С. В. Конявская-Счастная

НАЧАЛА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Москва
Типография «Вишневый пирог»
2025

УДК 004.056.5

ББК 30ф

Рецензенты:

Анатолий Александрович Стрельцов, Заслуженный деятель науки Российской Федерации, доктор юридических наук, доктор технических наук, профессор.

Андрей Юрьевич Щербаков, доктор технических наук, профессор, академик РАЕН.

Конявская-Счастная С. В.

Начала технической защиты информации. М.: Типография «Вишневый пирог», 2025. – 326 с.

ISBN 978-5-6053673-0-7

Книга представляет собой учебное пособие для тех, кто планирует быть разработчиком средств защиты информации. Пособие создано для поддержки вводных курсов на кафедре защиты информации ФРКТ МФТИ, но не связано ни с каким конкретным курсом или учебным планом. Может использоваться для самостоятельного ознакомления со спецификой специальности разработчика средств защиты информации и примерки на себя ракурса взгляда на информационные технологии «с точки зрения безопасника».

ISBN 978-5-6053673-0-7

© Конявская-Счастная С. В.

Оглавление

НАЧАЛО НАЧАЛ 6
ГЛАВА 1. СРЕДА ЗАЕЛА 25
1.1. Среда влияет на систему: следствия для защиты информации 26
1.2. Доверенная среда – это какая? 34
1.3. Средства организации доверенной среды 37
1.3.1. Аккорд-АМДЗ 39
1.3.2. m-TrusT и другие микрокомпьютеры Новой гарвардской архитектуры 44
1.3.3. Средства обеспечения доверенного сеанса связи 46
СПИСОК ЛИТЕРАТУРЫ: 58
ГЛАВА 2. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ 60
2.1. Общие вопросы: что, где, когда 60
2.2. «Факторы аутентификации» 67
2.2.1. Понятие «фактор» 69
2.2.2. Классификация «факторов» 75
2.3. Как обойтись без факторов 82
2.3.1. Предпосылки классификации аутентифицирующих данных 83
2.3.2. Субъектно-объектная классификация аутентифицирующих данных 97
2.4. Механизмы принятия решения о результатах аутентификации 105
2.5. Авторизация 120
2.6. И\А в открытых системах: новая биометрия и «оплати мой кофе своим взглядом» 123
2.6.1. Идентификация в открытых системах 126
2.6.2. Криминалистика и экономика 129
2.6.3. Новая биометрия. Замысел защиты 131
СПИСОК ЛИТЕРАТУРЫ: 135
ГЛАВА 3: РАЗГРАНИЧЕНИЕ ДОСТУПА 137
Защита неравенства 137
3.1. Разграничение доступа к ресурсам в доверенной среде 141
3.1.1. Разграничение доступа в ОС 141
3.1.2. Разграничения доступа к элементам управления 155
3.2. Разграничение доступа к ресурсу в зависимости от среды 187

3.2.1. USB-накопители и похожие на них устройства ... 188
3.2.2. Разграничение доступа к ресурсам ИС при доступе к ним с разных устройств 202
СПИСОК ЛИТЕРАТУРЫ: ... 206
ГЛАВА 4: ПЕРЕОСМЫСЛЕНИЕ ГРАНИЦ ЗАЩИЩЕННОЙ СИСТЕМЫ: ТЕХНИЧЕСКИЕ СРЕДСТВА ДЛЯ РАБОТЫ В ОТКРЫТОМ МИРЕ ... 207
4.1. Удаленка ... 212
4.2. Объекты критических информационных инфраструктур «в полях» ... 224
4.2.1. Среда функционирования криптографии ... 227
4.2.2. Неизвлекаемый ключ ... 228
4.2.3. Коммутация с СВТ ... 229
4.2.4. Криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации fin-TrusT ... 235
4.2.5. Направления разработки других СЗИ на платформе m-TrusT ... 238
4.3. Функции защиты, связанные с перемещениями в пространстве ... 245
СПИСОК ЛИТЕРАТУРЫ: ... 252
ГЛАВА 5. СОБЫТИЯ БЕЗОПАСНОСТИ ... 255
5.1. Системы удаленного централизованного мониторинга событий безопасности ... 257
5.1.1. Общая характеристика систем мониторинга и управления информационной безопасностью ... 257
5.1.2. Система централизованного управления и мониторинга средствами защиты информации от несанкционированного доступа ... 261
5.2. Хранение и архивирование журналов событий ... 268
СПИСОК ЛИТЕРАТУРЫ: ... 275
ГЛАВА 6. ВОПЛОЩЕНИЕ РАЗЛИЧНЫХ ИДЕЙ, ПОДСКАЗАННЫХ ЖИЗНЬЮ, ИЛИ ХОД МЫСЛЕЙ РАЗРАБОТЧИКА ... 277
6.1. Идеи и решения на основе технологии «Секрет» и устройств «Секрет» ... 278
6.1.1. Как возник сам «Секрет» ... 278
6.1.2. Программно-аппаратный неперезаписываемый журнал ... 280
6.1.3. «Идеальный токен» ... 282
6.1.4. «Система Ниппель» ... 283
6.1.5. «Секрет Администратора» ... 286
6.1.6. Случаи, когда второстепенная функция становится главной ... 292
6.2. Продукты и решения, возникшие на основе ПСКЗИ ШИПКА ... 299
6.2.1. Физический датчик случайных чисел с USB-интерфейсом ... 300

6.2.2. KeyMaker – Мастер ключей 301
6.2.3. Центр-Т: централизованная работа с терминальными образами 304
6.3. Продукты и решения сложного генезиса 307
6.3.1. Очень маленький универсальный хаб «Рассвет» (МКТ-card long) 307
6.3.2. Решение «два экрана» 310
6.3.3. USB Guard 318
СПИСОК ЛИТЕРАТУРЫ: 321
ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ 323
ВОПРОСЫ 323
ПРАКТИЧЕСКИЕ ЗАДАЧИ 324

НАЧАЛО НАЧАЛ

К моменту выбора специальности Вы уже, как правило, представляете себе, что «компьютерная безопасность» – это не про шапочки из фольги, защищающие от компьютерного излучения наш мозг, «компьютерная преступность» – это не когда кого-то стукнули компьютером по голове, а «защита информации» – это не защита массового сознания граждан от разрушающего воздействия мемов. Все это тоже существует, но в других местах, на кафедре защиты информации ФРКТ МФТИ акцент со всей определенностью поставлен на то, каким образом обеспечить и поддерживать безопасность информации в информационных (компьютерных) системах.

Определение:

Безопасность объекта – способность объекта сохранять свои номинальные параметры в заданных условиях окружающей среды [1].

Сразу обратим внимание на то, что следует из этой формулировки: эта самая способность объекта явно необязательно является результатом его защиты. Если заданные условия окружающей среды таковы, что объекту ничего не угрожает, то он в безопасности, даже если не защищен. Отсюда вытекает очень важное знание: безопасность и защищенность – это разное.

Определение:

Защищенность объекта – характеристика объекта, определяющая его способность противостоять атакам [1].

Это определение тянет за собой цепочку из еще двух важных с самого начала понятий.

Определения:

Атака – реализация угрозы безопасности вычислительной системы [1].

Угроза безопасности – возможное воздействие, которое прямо или косвенно может нарушить состояние безопасности информации, содержащейся и обрабатывающейся в вычислительной системе [1].

Зачем нам нужны эти понятия становится ясно при формулировании самых первых вводных тезисов о предмете защиты.

Казалось бы, тут все предельно ясно – защита информации, значит, предмет защиты – информация, что же еще.

Что такое «информация» – кажется интуитивно понятным. И это оказывается той самой не застегнутой пуговицей, из-за которой все неприятности. В свое время был страшно популярен офицерский афоризм «все ваши неприятности из-за того, что верхняя пуговица не застегнута». Это, конечно, ирония. Однако в самом деле масса неприятностей во всех областях человеческой деятельности связана именно с этим – с какой-то совсем небольшой небрежностью где-то в самом начале построения (рассуждения ли, процесса ли). Оказывается, что под словом «информация» понимаются самые разнообразные вещи и большинство из них решительно непригодны для того, чтобы на их основе выстраивать понятийную систему защиты информации.

Остановлюсь в двух словах на том, почему это так важно. Это важно потому, что влияет на критерии оценки эффективности защиты. Ведь если в технологию работы с криптографическим ключом входит операция его уничтожения *в памяти пользователя* (это реальная цитата из документа!) очевидно, что оценить эффективность такой технологии невозможно. Если принять в качестве определения

информации как объекта защиты чего-то вроде «вечной категории, содержащейся во всех без исключения элементах и системах материального мира, проникающей во все “поры” жизни людей и общества», то будет невозможно оценить, защищено ли это в итоге. И для недобросовестных безопасников это удобно.

С перечнями определений информации вы еще будете иметь дело в книгах из обязательного списка для чтения, здесь ограничимся только самыми полезными для формирования понятийной базы.

В первую очередь, это определение, приведенное в статье Н. А. Кузнецова как одно из классических. Оно относится к алгоритмическому подходу к информации, в частности, А. Н. Колмогорова, и уже давно используется как народное, без ссылки на автора.

Определение:

Информация есть сущность, сохраняющаяся при вычислимом изоморфизме [2].

Это определение звучит сейчас, скорее всего, совершенно не понятно, в первую очередь из-за слова «сущность», которое, как кажется на первый взгляд, ничего не проясняет, а только запутывает.

На самом деле это определение крайне продуктивно именно для целей защиты информации и чуть позже станет ясно, почему.

А прежде попробуем внести ясность в эту самую «сущность». Кратко пересказанное ниже рассуждение носит название «органическая концепция информации», оно приведено в книге А. А. Стрельцова [3. С. 14–27]. В книге эта концепция подкреплена анализом и критическим разбором других концепций и определений понятия «информация», вы сможете при желании ознакомиться с этой аргументацией самостоятельно.

Большинство подходов к определению информации объединяет то, что они выделяют у информации следующее ключевое свойство: отражать движение объектов материального мира в некоторой системе, которой это необходимо для адаптации к изменениям окружающей действительности.

Здесь ключевыми моментами является, во-первых, *отражение* (отражение движения, а не само движение, является информацией), а во-вторых, необходимость этого отражения, его целесообразность для системы (бесполезный шум, даже членораздельный (понятный), информацией не является).

Это звучит сложно, но на примере понять очень легко: для волка след зайца (отпечатки его лап на земле или запах) является информацией, так как он заинтересован в зайце. Для ящерицы заяц никакого интереса не представляет, и его след не является информацией, даже если она его тоже способна зафиксировать органами чувств. Если заяц проследовал, не оставив решительно никакого следа – ни отпечатков лап, ни запаха, и т. п. – то *информации* о том, что заяц тут был, у волка нет при всей его заинтересованности. То есть, во-первых, след зайца – это информация в системе волка, но не ящерицы. А во-вторых, если следа не осталось (какое-то изменение в действительности было, но не оказалось отражено никаким образом, или оказалось отражено так, как волк не может воспринять (например, заяц оставил письменное сообщение, а не отпечаток лап и не запах), то в системе волка новой информации не появилось).

Основой органической концепции служит положение о том, что информация – это категория, присущая только живой природе. В первую очередь потому, что для нас на сегодняшний день не очевидно, каким образом в неживой природе осуществляется целеполагание (если исходить из презумпции, что оно там вообще осуществляется). Иными словами, вряд ли системы неживой природы целенаправленно адаптируются к изменениям окружающей среды, а вот системы живой

природы к изменениям окружающей среды адаптируются, и поэтому нуждаются в том, чтобы как-то эти изменения отслеживать и желательно – прогнозировать.

Таким образом, получаем, что

Определение:

Информация – это отражение движения объектов материального мира в системах живой природы [3. С. 15].

Нужно учитывать, что «движение» здесь понимается предельно широко – не только в физическом, но и химическом, биологическом и социальном смысле. Вне философского контекста, возможно, было бы точнее слово «изменение». В материалистической философии «движением» называют любые виды изменчивости, наблюдаемые в объективном (то есть существующем независимо от наблюдателя) мире. Именно в этом смысле слово «движение» используется в этом определении.

Слово «отражение» тоже используется как категория диалектического материализма. Это приобретение материальным объектом некоторых свойств под воздействием свойств объекта, который с ним взаимодействует. Как бы приобретение «следа» свойств этого взаимодействующего объекта.

Последнее, что требуется для понимания определения – категория «взаимодействие» (так как без этого не до конца прояснен смысл понятия «отражение»). Взаимодействие – это взаимное изменение объектов материального мира.

Отражение в живой природе имеет особенности, связанные с тем, что она живая, то есть все ее системы являются организмами или состоят из организмов. С этим связана физическая сущность отражения движения материальных объектов в системах живой природы. Она

состоит в изменении происходящих в этих организмах биохимических преобразований. Результаты этих изменений используются организмами, чтобы выбрать вариант поведения, наилучшим образом отвечающий цели поддержания жизни (или иной цели, если она у организма есть). Эти результаты являются формой существования информации в организме и называются «сведения».

Определение:

Сведения – это запечатленные в организме результаты отражения движения объектов материального мира [3. С. 16].

Обратим внимание, что сведения не равны информации, их, согласно приведенным определениям того и другого, отличает «запечатление» и «результат».

Сведениями становятся только те результаты отражения движения объектов материального мира, которые запечатлелись в организме, то, из чего «не вынесен урок», не становится сведениями, «в одно ухо влетело, в другое вылетело».

Смысл компонента «результат» просто понять на примере: одна и та же «входная» информация, воспринятая разными организмами (например, двумя разными взрослыми людьми, ребенком, собакой и рыбкой) породит в этих субъектах разные сведения. И дело не только в том, кто кого «умнее», но также в том, что различаются цели этих субъектов (организмов), окружающая среда, к которой они адаптируются, текущая их адаптированность и т. д., поэтому и запечатлеется в них разное.

Возьмем такой пример движения-изменения: мальчик подошел к аквариуму и насыпал корм. Это зафиксировали органы чувств рыбки, его самого, его собаки, его мамы и его папы. Какие сведения во всех этих организмах запечатлелись? Рыбка: появилась еда, надо плыть, пока не съели. Мальчик: рыбка меня увидела и бросилась ко мне, мне это приятно. Собака: запах говорит о том, что это корм, и дали его не мне. Мама: Вася

покормил рыбок, надо не забыть об этом и не покормить их снова. Папа: Вася что-то бросил в воду, пойду посмотрю, не мои ли часы.

Все сведения, которые есть в распоряжении организма, формируют так называемую «информационную модель мира», которая постоянно корректируется при поступлении новых сведений (в зависимости от особенностей организма, таких как большее или меньшее разнообразие вариантов адаптации к изменениям окружающей среды, и тому подобных). Организмы с высокоразвитой нервной системой и психикой способны при этом вырабатывать «знания».

Определение:

Знание – это производные сведения о закономерностях изменения состояния отражаемых объектов материального мира [3. С. 17].

Ключевые пункты определения – «производные» и «о закономерностях». Сведения эти «производные» в том смысле, что это сведения не об объектах и не об их изменении, а о закономерностях их изменений. Они являются результатом не отражения чего-либо, а операций с другими сведениями (обобщения, вывода). А то, что они касаются закономерностей, обеспечивает их целевую функцию – прогнозирования на основе поступающих сведений дальнейших изменений состояния окружающей среды.

Так, знания, которые могли возникнуть в приведенных в примере выше организмах в процессе обработки сведений, запечатлевшихся в них при кормлении мальчиком рыбки, могут быть такими: рыбка – когда *этот* подходит ко мне, появляется еда; мальчик – если почаще кормить рыбку, она будет рада мне сильнее; собака – мальчик любит рыбку больше, чем меня; мама – одним делом меньше, я могу пойти почитать; папа – лучше класть часы повыше.

Сейчас важно остановиться в следовании за рассуждением А. А. Стрельцова и отдать себе отчет в том, что ни сведения, ни знания – не могут быть предметом технической защиты информации, так как они находятся внутри организма. Это нужно запомнить.

Социальные организмы – люди – обладают способностью обмениваться сведениями. И осуществляется этот обмен через «сообщения».

Определение:

Сообщение – это набор знаков, с помощью которого сведения могут быть переданы другому организму и восприняты им [3. С. 18].

Из этого определения очевидно, что сообщение – это форма существования сведений вне организма, при их передаче.

Можно ли упростить цепочку, в которой сведения – это форма существования информации в организме, а сообщение – это форма существования сведений вне организма?

Равно ли сообщение информации? Очевидно, нет, так как на пути к сообщению информация интерпретируется дважды

1) при трансформации в сведение в конкретном организме,
2) при выражении в знаках.

Связь означаемого и означающего в знаке любой природы (акустическом ли, графическом ли, или любом другом) – условна, в ее основе не объективные закономерности, а того или иного рода общественный договор. Выбор знака, как правило, вариативен (зачастую одно и то же означаемое может быть выражено разными знаками). Как мы уже говорили, обусловлено множеством факторов и

то, как именно запечатлеется в сведениях в конкретном организме та или иная информация.

То есть между сообщением и тем движением объектов материального мира, которое отражается в организме, порождающем затем сообщение, конечно есть связь, но эта связь явно не «тождество».

Сообщение порождает сведения в том организме, который его получил, в этом смысле можно утверждать, что оно «содержит» сведения. Однако очевидно, что одно и то же сообщение порождает разные сведения в разных организмах (аналогично порождению разных сведений при получении одной и той же информации).

Порождение сообщений – это своего рода кодирование, а восприятие сообщений – декодирование. И это уже заметно приближает нас к технической защите информации.

Для следующего шага от работы А. А. Стрельцова перейдем к работе В. А. Конявского [1. С. 179–191]. В своей работе он не опирается на выкладки А. А. Стрельцова, так как она написана раньше, чем [3], однако также выделяет именно точку отображения в сообщение – в материальную форму (все, что до этого происходит с информацией – не материально) как отправную точку для начала рассмотрения в качестве объекта защиты.

Объединив терминологию двух авторов, можно сформулировать, что сведения могут «материализоваться» в предмет или в процесс. Предмет – это то, что зафиксировано в пространстве, процесс же – это то, что зафиксировано во времени.

Так, речь – не фиксируется в пространстве, но фиксируется во времени. Напечатанный текст фиксируется в пространстве, но не фиксируется во времени.

Предмет и процесс – это две формы существования сообщения. Сообщение в форме предмета В. А. Конявский называет *данными*, а в форме процесса – так и называет, *процессами*.

Еще одно свойство материализации сведений, не рассмотренное А. А. Стрельцовым, заключается в упорядоченности знаков в сообщении (будь оно в форме данных или процесса). Буквы, звуки, точки, насечки – любые знаки, с помощью которых субъект порождает сообщение, содержат сведения до тех пор, пока, они сохраняются в заданном порядке. Чтобы проверить это, достаточно переставить буквы в тексте или прокрутить аудиозапись от конца к началу.

Таким образом, определение сообщения целесообразно скорректировать следующим образом:

Определение:

Сообщение – это упорядоченный набор знаков, с помощью которого сведения могут быть переданы другому субъекту и проинтерпретированы им.

Здесь не случайно заменен также организм на субъект (и восприятие на интерпретацию). Так как в технических системах способностью порождать сообщения обладают не только организмы. Датчики могут отображать в форме упорядоченной последовательности знаков результаты измерений, процессы – результаты выполнения преобразований, все это передается в виде сообщений в той или иной знаковой системе. Аналогично «воспринимать» – интерпретировать – сообщения, использовать их как входные данные могут тоже не только организмы, но и процессы, средства обработки, вывода и т. д.

Еще одним важным феноменом понятийной системы, связанной с информационным взаимодействием, является среда, для существования в которой формируется сообщение. От нее зависит знаковая система сообщения и его форма (процесс или данные), а в случае, если эта форма – данные, то и носитель. Очевидно, что для применения в одной среде

нам понадобится сообщение на листе бумаги, а для применения в другой – сообщение в памяти флеш-накопителя, и крайне редко сложится ситуация, когда эти сообщения будут взаимозаменяемы.

Более того, одно и то же сообщение может существовать на определенном отрезке своего жизненного цикла в виде данных, а на другом – в виде процесса, может «перекодироваться» из одной знаковой системы в другую. Залогом сохранения тождества в этом случае будет именно сохранение заданного порядка знаков различной природы (сигналов) – вычислимый изоморфизм, о котором мы читали выше в определении.

Вот это – сообщения (данные и процессы) как упорядоченный набор знаков, предназначенный для применения в определенной среде, и есть предмет защиты в технической защите информации. Именно это называется «информацией» в соответствующих контекстах. Помимо уже названных это влечет за собой еще одно важное следствие: защита информации – это всегда защита *информационного взаимодействия*. Так как сообщения формируются всегда и только с целью взаимодействия.

Информационное взаимодействие называется защищенным, если обеспечивается вычислимый изоморфизм – сохраняется отношение упорядоченности множества сигналов, маркированных как «информация» [1. С. 181]. Далее слово «информация» будет использоваться именно в этом смысле, а не в значении знаний, сведений или иных нематериальных сущностей.

Информация в компьютерных системах *хранится* и *обрабатывается*. Когда она хранится – она пребывает в статической форме – это *данные*. Когда она обрабатывается – пребывает в

динамической форме – это *процессы*[1]. Кроме обработки и хранения выделяется еще *передача* информации. Однако очевидно, что это тоже своего рода обработка – данные оказываются в другом месте. При этом хорошо понятно, что они не исчезают там, откуда они передаются (если исчезают, то это отдельный процесс их удаления). Нет сомнений в том, что это процесс, динамическая форма существования информации. Поэтому запомним, что вполне логично относить передачу данных к одному из видов их обработки, в дальнейшем это пригодится.

Сделать все эти довольно абстрактно звучащие вещи (данные, процессы) безопасными решительно невозможно без понимания основ защиты информации. Поэтому в самом начале пути необходимо разобраться в том, что может угрожать данным и процессам – и безопасности информации в информационной системе в целом.

Все, что делается с данными в цифровой форме осуществляется некоторыми *информационными технологиями*, выполняющимися в некоторых *информационных системах*.

Определение:

Информационная технология — заданная последовательность информационных операций преобразования входных данных в выходные.

Казалось бы, так можно описать вообще любое изменение. Однако это заблуждение, которое провоцируется неточным пониманием понятий «входные и выходные данные». Если проводить аналогию с технологиями в аналоговом мире, то входные данные – это материалы, сырье, а выходные – продукт. Если подать не тот материал – продукт не получится, если произвести над материалом не те операции,

[1] Пока возьмем на заметку, что если у информации есть форма – то явно должно быть и содержание, и где-то его важно не упустить из виду. Эта памятка понадобится несколько позже.

или не в той последовательности – продукт не получится, хотя и в том, и в другом случае будет иметь место некоторое преобразование.

Добавим в качестве «входных данных» соль, а не сахар, и «выходные данные» – торт – не получатся.

Если смешать желтый и синий, получится зеленый, мы это знаем с детства. Однако, если смешать желтую и синюю *краски*, действительно, получится зеленая *краска*, а если смешать желтые и синие *носки*, то *зеленые носки* не получатся. Здесь нам пригодилась сделанная выше заметка о том, что содержание информации не менее значимо, чем ее форма.

Если попытаться совершить неподходящую операцию, результат, скорее всего будет бессмысленным – сложить 5 яиц и 2 помидора, чтобы получить 7, а не яичницу – это не технология, а ерунда.

Если совершить подходящие операции в измененном порядке, результат получится неверным (это легко проверить, поменяв местами операции математического выражения).

Таким образом, информационная (или любая другая) технология всегда создается и должна рассматриваться относительно заранее определенных типов входных и выходных данных, и представлять собою определенные операции в определенном составе. Именно на это указывает в определении слово «заданная». Операции в машине Тьюринга – в любом множестве операций – всегда будут производиться в какой-то последовательности. Преобразование является технологией тогда, когда последовательность заданная (целенаправленно определенная).

Информационные технологии реализуются разнообразным *программным обеспечением* с использованием некоторых *входных данных*, поставляемых в информационную систему *снаружи, из аналогового мира* (пользователями или датчиками (результаты объективных измерений))[2].

---

[2] Тут необходимо сделать еще одну заметку на будущее, поскольку входными данными в тех или иных преобразованиях очень часто являются данные, не

Этого весьма абстрактного описания уже достаточно для того, чтобы наметить направления защиты информации для некоторой информационной системы (поскольку на начальном этапе конкретные примеры, позволяющие мысленно визуализировать то, о чем идет речь, желательны почти до необходимости, будем говорить о финансовой организации (банке), хотя с тем же успехом это может быть любая другая).

Вам встретится в различных источниках разной степени авторитетности масса определений информационной безопасности, безопасности информации и защиты информации в контексте их связи с такими признаками как «доступность», «конфиденциальность» и «целостность», и как правило они будут противоречивыми или недостаточно конкретными. Поэтому представляется целесообразным задать ту понятийную систему, в рамках которой будет формулироваться содержание этой книги.

Определения:

Безопасность компьютерной системы – это состояние компьютерной системы, в котором она сохраняет свои номинальные параметры (целостность, конфиденциальность, доступность данных и информационных технологий) в заданных условиях окружающей среды.

Защищенность компьютерной системы – это состояние компьютерной системы, в котором она способна противостоять атакам.

Целостность данных и/или информационных технологий – это отсутствие в данных и/или информационных технологиях изменений относительно эталонного состояния.

введенные пользователем или поступившие с датчика, а порожденные другими программами или процессами (то есть их *выходные* данные). В то же время где-то «в самом начале» все же, как правило, есть данные, поступившие снаружи системы. В любом случае, на текущем уровне абстракции это не принципиально.

Доступность данных и/или информационных технологий – возможность доступа к данным и/или информационным технологиям в рамках установленных прав доступа.

Конфиденциальность данных и/или информационных технологий – невозможность доступа к данным и/или информационным технологиям с нарушением установленных прав доступа.

Важно, что мы используем понятие «компьютерная система» (КС), а не «объект информатизации», «информационная система» или «автоматизированная система». Именно компьютерная система включает в себя только технические и программные средства и данные, и не включает в себя помещения, персонал, финансовые ресурсы и все прочее, что включают в себя остальные перечисленные системы. Техническая защита информации – это защита компьютерных систем и данных. Информационные системы, автоматизированные системы и объекты информатизации будут оказываться в поле нашего зрения при разработке моделей угроз и нарушителя, подготовке организационно-распорядительной документации для аттестации и в других аналогичных случаях, а также тогда, когда речь будет идти о предъявляемых кем-либо требованиях, если в них используется именно это понятие. При этом всегда нужно обращать внимание на то, какое определение дается этому понятию в каждом конкретном случае, так как они могут существенно различаться. Для получения представления об этом достаточно обратиться к любому общедоступному энциклопедическому источнику.

Итак, компьютерная система в безопасности, если она способна сохранять свои номинальные параметры в заданных условиях среды.

То есть пока не изменяется то, что оказывает на систему влияние (среда), система функционирует так, как предусмотрено при ее создании, не меняясь под влиянием среды (напомним, если среда сама не меняется).

Из этого логически не вытекает, что для того, чтобы быть в безопасности, система должна быть защищенной. Напротив, из этого логически вытекает, что возможна такая среда, при которой система будет в безопасности. Эмпирически же из этого достаточно очевидно следует, что такая среда для реальной компьютерной системы является крайне маловероятным и весьма недолговременным обстоятельством.

Не менее очевидно и то, что глобально можно двигаться в двух направлениях – создавать (менять, поддерживать – в общем, так или иначе приспосабливать под свои задачи) среду, то есть то, что снаружи нашей системы, либо управлять свойствами самой системы. Возможны оба пути, но и логика, и опыт подсказывают, что влиять на систему эффективнее, так как она заведомо более контролируема и меньше по объему, чем среда, границы которой могут и вовсе не определяться[3].

А значит, исходим из того, что в среде точно есть злоумышленник, и повлиять на него мы не можем. Значит, нужно сделать компьютерную систему способной противостоять его атакам, то есть – защищенной.

Заметим на будущее еще одно следствие из приведенного рассуждения – когда мы говорим о «границах системы» – в случае с компьютерной, а тем более – информационной системой во многом это выражение метафорическое. Поэтому несмотря на то, что влияние на систему так или иначе всегда оказывается через среду, защиты только «границ» – периферийной защиты – недостаточно. Она обязательно должна быть, но должна быть и «иммунная» защита системы, защита, пронизывающая ее внутреннюю структуру, аналогично тому, что для поддержания здоровья недостаточно укреплять кожу, необходим иммунитет. Традиционные средства защиты – антивирусы, VPN, межсетевые экраны, СДЗ и т. п. – это периферийная защита, защита от

[3] Еще одна необходимая заметка о том, что изменения настоящего времени делают тезис о замкнутости и контролируемости КС сомнительным – возвращаясь к избранному в качестве примера финансовому сектору, вспомним об оплате покупок путем приближения мобильного телефона к платежному терминалу (не говоря уж об оплате путем взгляда в видеокамеру). Однако об этом пойдет речь позже, пока ограничим предмет рассмотрения замкнутыми КС.

попадания чего-то нежелательного внутрь (внутрь чего – зависит от конкретного средства), иммунная же еще только разрабатывается, ее необходимость осознана.

Злоумышленник может реализовать преступные намерения,

- *изменив в свою пользу данные* – путем выполнения некоторых несанкционированных действий с ними в свою пользу от лица легального пользователя (от имени сотрудника банка, или от имени владельца счета), вплоть до нарушения работоспособности системы (например, обнулив данные о невозвращенных кредитах).

- *изменив в свою пользу технологию* – путем модификации программного обеспечения (например, так, чтобы при каждой подаче любой пластиковой карты в приемник банкомата, компьютер отправлял на определенный счет определенную сумму, почему бы нет?)

Следовательно, нужно обеспечить состояние системы, при котором

1) только легальные пользователи, аутентифицированные доверенными защитными механизмами

2) могут выполнять операции только из состава легальных технологий и

3) только в рамках назначенных им полномочий,

4) все программы работают корректно,

5) все события фиксируются.

В этом случае успешные атаки становятся возможными только при сговоре легальных пользователей. А это уже, как говорится, совсем другая статья. И за счет правильно организованной системы регистрации событий, ощутимо повышающей шансы на применение необходимой статьи, это может стать весьма существенным сдерживающим фактором.

Для того чтобы обеспечить такое состояние системы, принимаемые меры должны быть направлены на:

1) создание и поддержание вычислительной среды, в которой программы исполняются корректно (доверенная вычислительная среда),

2) доверенную идентификацию, аутентификацию и авторизацию пользователя (в случае с банком, который мы приняли примером, это должно касаться как «внутреннего» пользователя – сотрудников, так и «внешнего» – владельцев счетов),

3) разграничение доступа пользователей к ресурсам системы,

4) реализацию тех участков информационной технологии, которые не могут контролироваться эксплуатирующим персоналом информационной системы, с использованием технических средств, предназначенных для работы вне доверенной среды,

5) надежную фиксацию событий в системе.

Далее рассмотрим, какие именно меры, принимаемые по перечисленным направлениям, эффективны и действительно позволят блокировать атаки злоумышленников.

Начнем по порядку – с создания и поддержания доверенной вычислительной среды.

Определение:

Доверенная вычислительная среда – это система, все узлы которой аутентифицированы и целостность их установлена [8. С. 11].

Шире можно сказать, что в этом же смысле применяется слово «доверенный» и в качестве определения других объектов – канала, ОС, технологии. Подробнее об этом можно прочитать в [8 С. 10–17].

В этой главе, и в целом в развертывании сюжета книги так или иначе постоянно будут встречаться упоминания технических и программных средств, еще не описанных подробно прежде, более того, иногда знакомство с ними будет существенно отстоять от первого упоминания. Чтобы не нарушать логику изложения, объяснения и отступления в этих случаях вводиться не будут, рекомендуется получать общее представление о неизвестных предметах, обращаясь по ходу чтения к информационным источникам типа Википедии, этого будет достаточно для понимания текста.

ГЛАВА 1. СРЕДА ЗАЕЛА

Сегодня многие отрасли экономики, и банки в числе первых – заслуженно (по большей части) гордятся программным обеспечением, выполняющим целевые для деятельности финансовых организаций функции. Оно спроектировано и разработано продуманно и качественно, его функциональность позволяет обслуживать клиентов максимально эффективно и комфортно. Те же чувства испытывает владелец хорошей машины, способной мгновенно развивать бешенную скорость, обладающую великолепной маневренностью и прочими прекрасными свойствами.

Однако даже на такой замечательной машине, находящейся в абсолютно исправном состоянии, владелец может опоздать на встречу, например, потому что будет пробка, или на пути к цели не будет дороги, а будет океан.

Мы зависим от среды, в которой нам приходится действовать, больше, чем хотелось бы.

Это означает, что действия, корректность выполнения которых должна быть гарантирована, должны выполняться в «правильной» среде, которая надежно *изолирована* от среды внешней, незащищенной, потенциально опасной. Если изоляция не обеспечена, свойства среды могут измениться под влиянием внешней незащищенной среды.

Что вытекает из этих очевидных посылок?

1.1. Среда влияет на систему: следствия для защиты информации

В первую очередь, необходимость определения, какой же должна быть «правильная» среда. Ответ следует из постановки задачи – она должна исключать влияние на корректность информационных технологий, программ, которые в ней исполняются. Влияние исключено в том случае, если процессы в ней изолированы один от другого. Все в строгом соответствии с определением безопасности объекта: объектом в данном случае будет процесс (технология, программа). Процесс в безопасности, если сохраняются его номинальные параметры в заданных условиях окружающей среды, то есть среда не заставляет его меняться, не влияет на него. Это может быть, если среда в принципе не способна влиять, или если объект (процесс) защищен и способен противостоять атакам из среды. Значит, доверенная вычислительная среда – это такая вычислительная среда, в которой на исполнение процессов не влияет ничего постороннего, в том числе и другие процессы, легально исполняющиеся в этой же среде.

Известно несколько вариантов реализации такой среды – функционально замкнутая среда (ФЗС), изолированная программная среда (ИПС), доверенная вычислительная среда (ДВС), и феномен на стыке ФЗС и ДВС – доверенный сеанс связи (ДСС).

Для перечисленных сред разработаны и научно обоснованы модели и доказательства их защищенности, прочитать о первых трех можно в [1. С. 38–752; 4. С. 26–60], о четвертой – в [5, 6].

Какой именно должна быть среда в каждом конкретном случае, зависит от того, что представляет собой защищаемая технология, дать единственно правильный ответ тут нельзя. Самым высоким потенциалом защиты обладает ДВС, однако и стоимость ее создания и поддержания в системе – самая высокая. ИПС наиболее сложна с точки зрения доказательства корректности изоляции, ФЗС подходит только для однозадачных систем, а ДСС – обходится дешевле всего, но создает защищенную среду только для кратковременных сеансов работы.

Второе, что мы понимаем на следующем шаге – это необходимость не только создать, но и *поддерживать* среду, которой мы доверяем. Действительно, если информационная система в принципе меняется – а она меняется, — то она может измениться и из-за вредоносного воздействия. Значит, доверенную среду нужно не только создать, но и поддерживать.

Для этого как минимум необходимо обеспечить:

1. контроль запуска задач и процессов;
2. взаимное невлияние задач;
3. защиту от перехвата управления;
4. защиту информационных технологий как последовательности операций.

Нарушение доверенности среды возникает при ошибках реализации пунктов 1-4.

Далее необходимо понять границы, *в которых* требуется обеспечить доверенную среду, а *за которыми* – не требуется.

Информационное взаимодействие в большинстве случаев можно представить как взаимодействие клиентов через сервис. Например, рассмотрим то, с чем на практике сталкивается всякий – дистанционное банковское обслуживание (ДБО).

Если посмотреть на этот процесс как на взаимодействие хозяйствующих субъектов, то взаимодействует банк (финансовая организация) и человек (клиент банка), как на рис. 1.1.

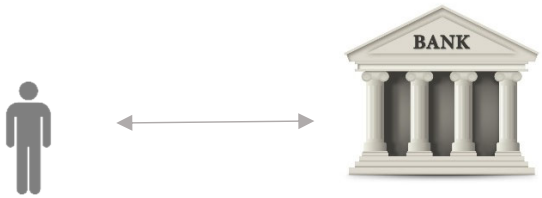


Рис. 1.1. Информационное взаимодействие клиента с банком при дистанционном банковском обслуживании

Если посмотреть на процесс как на информационное взаимодействие, то сервис предоставляет банк (это система «Клиент-Банк»), а взаимодействующие через сервис клиенты – информационная система, например, «Операционный день» со стороны банка и ПО он-лайн банкинга (обобщенно назовем его «Клиент ДБО») со стороны клиента банка. Графически это представлено на рисунке 1.2.

Внимание, нельзя путать «клиент ДБО» (это ПО) с клиентом банка – это человек!

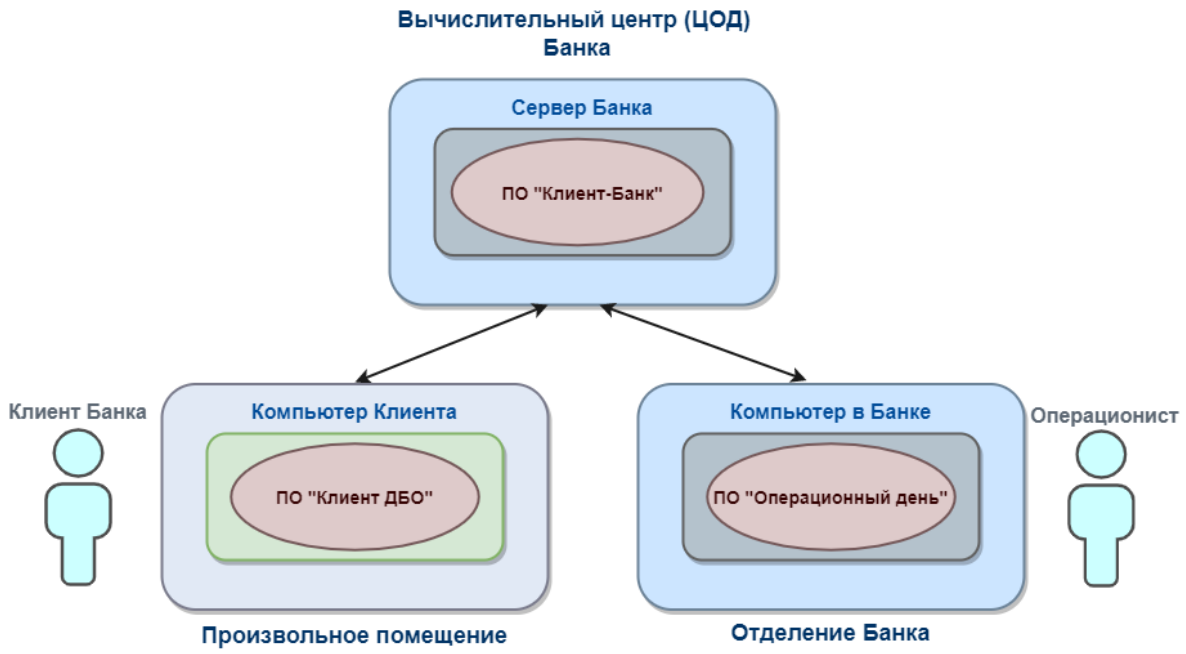


Рис. 1.2. Информационное взаимодействие клиента с банком при дистанционном банковском обслуживании

Посмотрим, что нам дает это понимание.

1. Информационная система банка (ПО «Операционный день» на картинке) должна функционировать в доверенной среде постоянно («Компьютер в Банке» в ЦОДе Банка на картинке).

2. Подсистема, которая предоставляет сервисы (ПО «Клиент-Банк» на картинке), должна функционировать в доверенной среде постоянно («Сервер Банка» в Отделении Банка на картинке).

3. Клиент как ПО («Клиент ДБО») – является частью той же системы, а защищенность системы равна защищенности самого слабого звена.

- ⇨ Следовательно, это ПО должно тоже всегда исполняться в доверенной среде («Компьютер клиента» в Произвольном помещении на картинке).

А всегда ли клиент какого-либо доверенного сервиса (человек) должен работать в доверенной среде? Вряд ли. Это будет слишком высокая цена за удобство осуществления безналичных расчетов, которые происходят не так уж часто и занимают не такое уж продолжительное время. Основную же часть времени работы на ПК человеку (клиенту банка) требуется свободный доступ в Интернет, мессенджеры и прочие небезопасные сервисы, из использования которых состоит большая часть нашего дня. Скорее, клиенту банка (человеку) нужно *часто* работать в недоверенной среде, и лишь *иногда* организовывать доверенный сеанс связи с доверенным сервисом.

Получается, что работа пользователя в доверенном режиме может быть необходима все время (именно так обстоит дело для операциониста, в информационной системе банка), а может лишь иногда, в относительно небольшие интервалы времени (так обстоит дело на домашнем компьютере клиента банка). В первом случае необходимо создать доверенную вычислительную среду (ДВС), во втором — достаточно организовать доверенный сеанс связи (ДСС).

В большинстве случаев корпоративные системы защищаются созданием ДВС, а частные, личные устройства защищаются таким образом, наоборот, редко.

ДВС создается однократно, но стоимость ее создания относительно велика. Действительно, однажды созданная, ДВС должна

поддерживаться долго, в отдельных случаях — годы[4]. За это время суммарное количество атак может стать огромным, и все эти атаки должны быть отражены защитными механизмами средства защиты информации (СЗИ), обеспечивающего ДВС. Конечно, такие СЗИ стоят дорого, так как они сложны и технически, и логически (ниже рассмотрим их на примере СЗИ НСД «Аккорд»).

ДСС создается каждый раз заново, и это в ряде случаев может быть неудобно – загрузка и проверочные мероприятия продолжаются 30–50 секунд, но средства ДСС стоят гораздо дешевле, так как длительность ДСС не всегда достигает и 20 минут (ниже рассмотрим их на примере средства обеспечения доверенного сеанса связи «МАРШ!»).

Графически перечисленные различия представлены на рисунке 1.3.

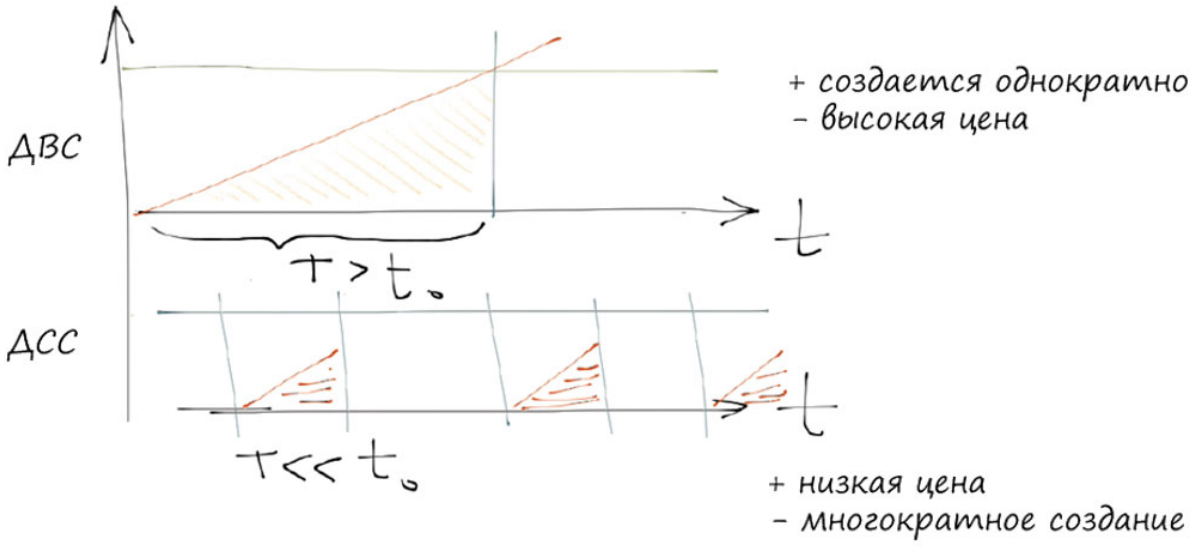


Рис. 1.3. Графическое представление различий между ДСС и ДВС

В двух словах необходимо прояснить связь между продолжительностью периода непрерывной защиты и ее сложностью

[4] Например, в платежных сегментах не редкость сервера и автоматизированные рабочие места (АРМ), которые должны работать в непрерывной сессии постоянно, в отличие от их эксплуатирующего персонала, работающего посменно.

(и стоимостью). Метафизическая связь времени и денег не подлежит сомнению, однако в данном случае связь между ними вполне физическая.

Изменяемость вычислительной среды определяет универсальность средств вычислительной техники, с одной стороны, а с другой, сама определяется архитектурой большинства современных средств вычислительной техники (СВТ), являющихся реализацией «машины Тьюринга» [7]. Проще говоря, наши компьютеры универсальны потому, что изменяемы, а изменяемы они потому, что такова их архитектура. Именно это свойство используют вирусы и другое вредоносное ПО (ВрПО), перехватывающее управление компьютером, ворующее пароли и выполняющее любые другие угодные хакеру действия. И для поддержания доверенной среды нам необходимо эту изменяемость блокировать.

Средства обеспечения ДСС блокируют ее, если сильно упрощать, путем запрета записи в долговременную память, то есть все, что случилось во время сеанса, обнуляется по его завершении. Поэтому сеанс не должен быть продолжительным, иначе теоретически, даже без записи в долговременную память, хакер сможет накопить изменения так, чтобы создать условия для реализации атаки (пример такой поэтапно подготовленной атаки – на схематическом уровне – можно прочитать в [8. С. 224–225] в разделе «Борьба с вирусами»). Это похоже на определение места, откуда звонит преступник в детективах – чтобы определить место, надо продержать преступника «на трубке» N секунд, а преступник старается успеть повесить ее на N-1, и при следующем звонке вся работа начинается сначала, результат не накапливается, специалист начинает не с того места, где закончил, а с нуля. Так же (только с обратными знаками – преступник с другой стороны) обстоит дело с и доверенным сеансом связи.

СЗИ, способные обеспечить создание и поддержание ДВС – меняют архитектуру компьютера, поэтому они сложны – в разработке,

в настройке и эксплуатации [9], они должны включать в себя резидентный компонент безопасности (РКБ), это понятие станет ключевым в целом ряде базовых дисциплин, и лучше всего получить о нем представление по [1] или [4].

Как именно это делается – создается доверенная среда исполнения задачи – постоянная, в случае с ДВС, или на сеанс, в случае с ДСС, разберем ниже.

Пока зафиксируем, что с продолжительностью периода работы связана и методика выбора средства обеспечения доверенной среды — там, где все операции должны выполняться в доверенной среде, создавайте и поддерживайте ДВС. Если доверенность нужна лишь иногда — достаточно (и удобнее) применять ДСС.

Сюда примыкает **еще одно следствие** из того факта, что система финансовой организации неизбежно включает в себя и сторону клиентов банка – они тоже являются пользователями системы, и те средства вычислительной техники, которые они используют, способны оказывать влияние на всю информационную систему банка. Следствие это состоит в том, что банку неизбежно приходится иметь дело с неквалифицированными пользователями, работающими потенциально на любом попавшемся устройстве. Такая особенность характеризует пока не все информационные системы, но именно таких со временем становится все больше, а «классических» корпоративных систем, состав пользователей которых постоянен, ограничен сотрудниками организации, да еще и работают они постоянно на одних и тех же физических рабочих местах – становится все меньше, и это надо иметь в виду.

Если со стороны сервиса (допустим, банка) всегда можно обеспечить достаточный уровень квалификации персонала, и, соответственно, достаточный уровень информационной безопасности, то обучить всех клиентов всех сервисов (или хотя бы всех клиентов всех банков) приемлемому уровню знаний об информационной

безопасности решительно невозможно. Пока не удается даже научить всех грамотно писать и говорить.

При организации защиты неквалифицированные действия обязательно создадут «дыру» в защищенности. А делать забор все выше и выше бессмысленно, пока в заборе остаются дыры. Оказывается, поскольку достаточный уровень квалификации со стороны клиента недостижим в принципе, бессмысленно все лучше и лучше защищать сервисы, пока «дыра» у клиента.

Что же делать?

Ответ очевиден — средства клиента должны быть ненастраиваемые (тогда он не настроит их неправильно), а все действия по управлению безопасностью должны быть переданы профессионалам.

Важно понимать, что такими же «клиентами» зачастую является и значительная часть пользователей внутри организации – системные администраторы и администраторы информационной безопасности (АИБ) называют таких пользователей «бабушками». Не всякий из них может различить телефонную и Ethernet розетку. Однако стационарно, на территории организации, такие пользователи как правило окружены вниманием упомянутых администраторов. Если же по тем или иным причинам они оказываются «на удаленке» и администратора рядом нет, их следует рассматривать так же, как клиентов банка – как потенциально неквалифицированных пользователей.

1.2. Доверенная среда – это какая?

Осталось **последнее**, что нужно прояснить перед рассмотрением конкретных средств и способов организации защищенной среды. Это то, как определить, действительно ли среда доверенная, чем это определяется, помимо наличия средства защиты, поставщик которого уверяет в том, что оно хорошее.

Одно из свойств уже было выведено выше – средство, контролирующее среду, должно быть не подвержено влиянию этой среды, то есть изолированным, автономным. Защита неминуемо связана с индикацией состояния защищаемого объекта, а это влечет за собой и общеизвестный принцип независимости средств контроля от контролируемого объекта. В реальной жизни это именно так. Центральный банк страны, контролирующий и защищающий денежную систему государства, должен быть отделен от исполнительной власти, распоряжающейся финансами. Налоговые органы действуют независимо от налогоплательщика. Если происходит иначе – возникают проблемы.

Обратим внимание на следующий факт – чтобы выполнить свою функцию, вредоносное ПО, как и любая другая программа, должно быть:

1) установлено на компьютер;
2) запущено на исполнение.

Для того чтобы ***установить*** программу, нужно получить доступ к операционной системе. Если в принципе существует момент времени, когда операционная система уже загружена, а защитные механизмы еще не включены – злоумышленник сумеет установить нужные ему программы. Не важно, сколько длится этот момент – час или микросекунду. Достаточно одного даже самого малого момента незащищенности.

Это означает, что защитные процедуры должны проводиться *до загрузки ОС*.

Это фундаментальный вывод. Его правильность давно доказана с применением точного математического аппарата [4], а следует из этого вывода также и то, что средство защиты должно быть аппаратным (так как программные средства работают в ОС, после ее загрузки). Обеспечить надежную защиту без применения специализированных аппаратных средств невозможно.

Любые попытки защитить компьютер и информацию в нем только за счет программных средств – абсолютно несостоятельны. Не знать этого сейчас просто нельзя, это знание давно доступно всем и подтверждено практикой, и те, кто утверждает иначе – просто кривят душой.

Чтобы исключить ***запуск на исполнение*** измененной программы, проводится контроль целостности. Правильно выполненный контроль целостности позволяет своевременно обнаружить несанкционированные модификации программ и данных и предотвратить использование таких модифицированных, а значит, недоверенных программ и данных.

Если для того, чтобы контролировать целостность программы «А» мы используем программу «В», то кто нам даст гарантию, что программа «В» осталась неизменной? Значит, нужна программа «С», которая проконтролирует целостность программы «В»! Нужна программа, контролирующая целостность программы, контролирующей целостность программы … и т.д., и т.п. Вера в то, что с помощью одной программы можно проверить целостность другой – то тяжелое техническое заболевание, состоящее в имитации мероприятий по защите без повышения уровня защищенности, получило название «Синдром Мюнгхаузена[5]».

---

[5] Барон Мюнгхаузен – литературный персонаж, ставший главным героем множества произведений различных авторов, которые объединяются общей сюжетной

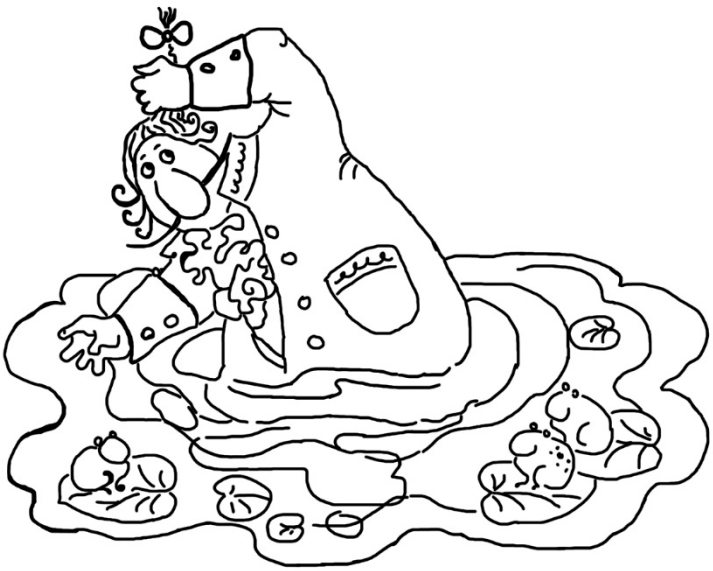


Рис. 1.4. Барон Мюнгхаузен достает себя из болота за косичку.

Для того чтобы разорвать порочный круг, нам нужен инструмент снаружи от нашего «болота», инструмент, который не мог быть изменен, поэтому остался точно доверенным. То есть снова – автономный и аппаратный. Автономность обеспечивает независимость решения от потенциально модифицированного окружения, а сама она – автономность – обеспечивается в свою очередь аппаратной реализацией.

Заручившись этими выводами, мы можем перейти к рассмотрению характеристик и примеров уже только тех средств защиты, которые могут обеспечить доверенную среду в вычислительной системе, не останавливаясь больше на аргументации неприемлемости программных решений или решений, включающих в свой состав аппаратную часть чисто формально, для галочки. А вот как отличить такие решения – необходимо ясно понимать.

доминантой: неправдоподобные рассказы героя о своих невероятных приключениях. Один из наиболее известных сюжетов, воплощенный в том числе и в мультфильме, – о том, как, провалившись в болото, барон вытащил себя из него за косичку парика (см. рис. 1.4) [10].

1.3. Средства организации доверенной среды

В этом разделе рассмотрим варианты обеспечения доверенной среды исполнения функционального программного обеспечения и криптографии, а также конкретные средства, позволяющие реализовать эти варианты.

Раз универсальность компьютера, которую нам необходимо ограничить, как мы выяснили выше, обеспечивается архитектурно, самой «конструкцией» машины Тьюринга, а архитектуру нельзя изменить программным путем, то никакие программные средства не помогут нам защититься от хакеров надежно.

А, собственно, от чего защититься?

Схема атаки хакера наиболее распространенного типа – атака с целью перехвата управления – выглядит так:

s1) внедряется и размещается в оперативной памяти вредоносное ПО (ВрПО);

s2) внедряется и размещается в оперативной памяти вредоносный обработчик прерываний;

s3) ВрПО и обработчик прерываний записываются в долговременную память;

s4) с помощью любого доступного механизма вызывается прерывание (например, с помощью DDOS-атаки, или злоумышленник может просто дождаться перезапуска СВТ);

s5) внедренный ранее обработчик прерываний срабатывает, и передает управление ВрПО;

s6) ВрПО выполняет свою функцию (например, реализует разрушающее программное воздействие).

Здесь s1 – s3 – это шаги по подготовке атаки, s4 – инициирование атаки, s5 и s6 – собственно использование архитектурной уязвимости.

Если уязвимость в архитектуре – то и совершенствовать нужно архитектуру.

Мы можем делать это одним из двух способов:

1. Усовершенствовать архитектуру уже существующих технических средств – то есть, приобретая новую технику, устанавливать на нее те или иные средства защиты.

2. Использовать новые технические средства на базе новой, более совершенной архитектуры.

В первом случае мы блокируем выполнение шагов s5 и s6 (не даем сработать вредоносному ПО), а во втором – шаг s3 (не даем записать в долговременную память изменения среды).

Рассмотрим на конкретных примерах.

1. Средство доверенной загрузки «Аккорд-АМДЗ» [11]. Оно реализует изменение архитектуры уже готового уязвимого компьютера фон-Неймановской архитектуры так, чтобы обеспечить его правильный старт (блокирование шагов s5 и s6), а также создает предпосылки к блокированию шага s3 (записи вредоносного ПО в долговременную память). Для этого его нужно устанавливать в любой компьютер фон-Неймановской архитектуры.

2. Специализированные компьютеры с аппаратной защитой данных Новой гарвардской архитектуры m-TrusT [12], обладающие сразу архитектурой, лишенной описанной уязвимости – они блокируют шаг s3, то есть не дают возможности записывать изменения в долговременную память никогда, кроме как в специальных режимах, перевод в которые программно невозможен (а значит, хакер этого сделать не сможет). Такой компьютер нужно использовать вместо уязвимого компьютера там, где это возможно и удобно.

3. Средство обеспечения доверенного сеанса связи (СОДС) «МАРШ!» [13]. Оно позволяет использовать незащищенный компьютер с уязвимой архитектурой в таком режиме, в котором архитектура не может повлиять на вычислительную среду пользователя в течение

непродолжительного периода защищенной работы. Его нужно подключать к компьютеру на время конкретного сеанса.

Последнее решение является промежуточным между первым и вторым подходом к обеспечению доверенной среды, однако и для него есть область применения, где оно может быть наилучшим.

1.3.1. Аккорд-АМДЗ

Итак, когда мы используем компьютеры с принципиально уязвимой архитектурой, у нас должно быть средство управления этой архитектурой.

На практике это означает, что на время загрузки и проведения контрольных процедур компьютер должен утрачивать свойства машины Тьюринга (универсального исполнителя), а затем, после успешного завершения контрольных процедур – снова приобретать эти свойства.

Выше мы уже определили, что изменить таким образом архитектуру уже готового компьютера может только аппаратное активное автономное устройство, начинающее контрольные процедуры до загрузки ОС.

Первым, с чего началась практическая реализация парадигмы аппаратной защиты в нашей стране и в мире, стало СЗИ НСД «Аккорд-АМДЗ», положившее начало линейке «Аккорд».

«Аккорд-АМДЗ» – это аппаратный модуль доверенной загрузки, обеспечивающий тот самый «правильный старт» компьютерной системы, доверенную загрузку операционной системы.

Определение:

«Доверенная загрузка» – это загрузка доверенной операционной системы из доверенного источника по доверенному каналу с сохранением заданного порядка операций загрузки.

Понятие доверенной загрузки операционной системы было введено в научный оборот давно, еще в 1999 году – в рамках парадигмы ДВС. А теперь это понятие вошло в понятийный ряд ФСТЭК России как целевая функция отдельного типа средств защиты информации: средства доверенной загрузки, СДЗ. Аккорд-АМДЗ во всех его вариантах исполнения согласно терминологии ФСТЭК России является СДЗ уровня платы расширения.

Аккорд-АМДЗ может быть реализован на различных контроллерах (см. рис. 1.5), различающихся принципиально только шинными интерфейсами: PCI или PCI-X; PCI-express; Mini PCI-express; Mini PCI-express half card; m.2.

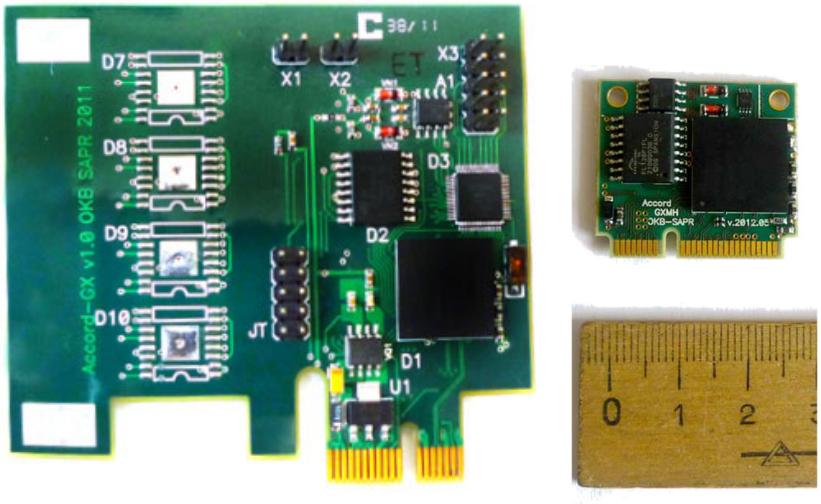


Рис. 1.5. СЗИ НСД «Аккорд»

Существует также вариант исполнения «Аккорд-АМДЗ» на базе USB-устройства, которое называется «Инаф» (от английского enough – достаточно). Этот вариант имеет определенные ограничения, которые должны восполняться орг. мерами или применением дополнительных механизмов, однако в ряде случаев этого вполне достаточно, отсюда и название.

Отдельного упоминания в связи с СДЗ требует вопрос применения криптографии.

Нормативная методическая база [14, 15] предписывает большинству финансовых организаций использовать СКЗИ не ниже класса КС2[6]. Эти требования основаны на требованиях ФСБ России и профильных стандартов [16-18]. Использование на СВТ СКЗИ класса КС2 возможно исключительно при совместном использовании с СДЗ уровня платы расширения (АПМДЗ), сертифицированного ФСБ России – это требование к среде функционирования криптографии (СФК).

Сегодня нет проблем в том, чтобы выбрать АПМДЗ (в терминологии ФСБ России) / СДЗ (в терминологии ФСТЭК России) для создания СФК на большинстве моделей настольных компьютеров и серверов. Хуже, но решаемо – с ноутбуками. Совсем сложно – с планшетами. На то есть технические причины, которые коротко сводятся к двум основным:

1) Мало на каких планшетах есть свободный разъем m.2 «с ключами A-E». M.2 (или NGFF) – это не просто разъем, а семейство разъемов, визуально различающихся ключами. Ключ – это перемычка, которая не позволит вставить неподходящую плату. Ключи определяют, какие интерфейсы будут использованы в разъеме. «С ключами A-E» означает m.2 с интерфейсом PCI-express[7], который необходим для работы СДЗ уровня платы расширения (АПМДЗ) в форм-факторе m.2 (о том, чтобы поместить в планшет какой-то еще вариант – трудно даже вести речь). Обычно имеющийся в планшете разъем m.2 имеет ключи B-M. В таком разъеме нет интерфейса PCI-express, но есть SATA, то есть он предназначен для работы с диском, а СДЗ уровня BIOS, подключить

---

[6] Если эти понятия – СКЗИ, классы СКЗИ – вас пока не знакомы, получите самые общие представления в Интернет, в дальнейшем вы будете проходить этот материал в рамках целого ряда курсов.

[7] PCI-express'ом называется и форм-фактор, и логическая шина, которая используется в большинстве СДЗ уровня платы расширения, в каком бы форм-факторе они не исполнялись. Исключениями являются немногочисленные примеры СДЗ на шинах USB и SATA, еще только входящие в оборот. Так, в контроллерах в форм-факторе PCI-express, в форм-факторе Mini PCI-express half size и в форм-факторе m.2 – одна и та же логическая шина – PCI-express.

в такой разъем нельзя. Если же «нужный» m.2 есть в наличии, как правило, он занят wi-fi модулем, а вынимать из планшета wi-fi, разумеется, неприемлемо в абсолютном большинстве случаев.

2) У планшетов совершенно иначе, чем у стационарных машин реализовано управление питанием – в частности, режим «сна». И это делает неприменимым на планшетах существующие в АПМДЗ механизмы реализации «сторожевого таймера» (строго говоря, в планшетах вообще нет той цепи, разрыв которой осуществляет стандартная схема сторожевого таймера), а также требует изменения механизмов идентификации/аутентификации пользователя, и так далее.

Как правило задача создания среды исполнения криптографии решается тем, что используется СДЗ уровня BIOS. Однако такое СДЗ не подходит для создания СФК в соответствии с требованиями ФСБ России. Таким образом, для того чтобы на планшете можно было использовать криптографию приличного класса (КС2 и выше), необходимо и особенное СДЗ (учитывающее особенности управления питанием в планшетах), и особенный планшет (со свободным разъемом нужного типа).

Подобрать эту пару самостоятельно – задача непростая и нелогичная для эксплуатирующей организации, поэтому ОКБ САПР поставляет планшет, в котором реализована СФК на класс СКЗИ КС3 (то есть установлен Аккорд-АМДЗ, сертифицированный ФСБ России) целиком, как единое решение. Он называется «ПКЗ 2020».

Характеристики планшета соответствуют всем нормальным современным требованиям, извлечение wi-fi модуля и отключение LTE не требуется.

Аналоги решения на сегодняшний день неизвестны – как целиком, так и АПМДЗ в формате m.2, которое соответствовало бы требованиям ФСБ России в части управления питанием для планшетов.

«Аккорд-АМДЗ» контролирует только старт компьютера и не работает в операционной системе, это означает, что на его

ответственности блокирование шагов s5 и s6 описанной выше атаки «на перехват управления», но не блокирование шага s3. Помешать записи в долговременную память чего-либо, попавшего в оперативную память во время работы компьютера, «Аккорд-АМДЗ» сам по себе не может. Однако выше упоминалось, что его использование создает предпосылки для блокировки и этого шага. Для того чтобы это сделать, необходимо применять не один «Аккорд-АМДЗ», а программно-аппаратные комплексы на его основе – ПАК «Аккорд-Win32», «Аккорд-Win64» или «Аккорд-Х». Они являются уже не СДЗ, а СЗИ НСД, то есть включают в себя, кроме СДЗ, еще подсистему разграничения доступа и предназначены, соответственно, для разграничения доступа в 32-х и 64-х разрядных ОС Windows и в ОС Linux.

Функциональность комплексов одинакова – в них реализованы дискреционный (с использованием 13 атрибутов) и мандатный механизмы разграничения доступа, в том числе – контроль запуска задач и контроль печати из любых приложений на принтеры любых типов (сетевые, локальные, виртуальные). Подробнее на этом остановимся в главе про разграничение доступа к ресурсам системы.

Несколько слов необходимо сказать об инфраструктурах виртуализации как о специфической среде, которую тоже необходимо делать доверенной. Специфика ее состоит в том, что между загрузкой физических машин, на которых работает инфраструктура, и ОС виртуальных машин (ВМ), в которые устанавливаются средства разграничения доступа, есть существенный разрыв, и в отличие от «физических» компьютеров и серверов, при использовании комплекта из СДЗ + ПО разграничения доступа непрерывной сквозной защиты не получится.

СЗИ НСД, если они корректно разработаны, разумеется, представляют собой не «комплект» (то есть СДЗ и СЗИ в одной коробке), а комплекс, то есть между этими компонентами есть взаимодействие, они используют данные друг друга и их решения взаимоувязаны. В случае со средой виртуализации сделать так же «в лоб» не получится,

нужен дополнительный компонент, контролирующий «прослойку». Именно с учетом этого обстоятельства реализованы комплексы, обеспечивающие сквозной контроль целостности при загрузке ВМ «Аккорд-В.» (для платформы виртуализации VMware vSphere) и «Аккорд-KVM» (для платформы виртуализации KVM). Подробнее о том, как это сделано, можно узнать из описания этих продуктов.

За счет совокупности своих функций, включающих аппаратный контроль целостности среды и контроль запуска задач в программной части комплекса, ПАК СЗИ НСД Аккорд позволяет закрыть уязвимость фон-Неймановской архитектуры компьютера, блокируя атаку на «перехват управления» на всех 6 ее шагах. При этом архитектура этого защищаемого компьютера, как и в случае с Новой гарвардской архитектурой (о ней речь пойдет ниже), но значительно бóльшими усилиями – становится динамически изменяемой: сохраняя необходимые для решения функциональных задач свойства «машины Тьюринга» во время работы, во время старта компьютер ею не является, работая скорее как «конечный автомат».

1.3.2. m-TrusT и другие микрокомпьютеры Новой гарвардской архитектуры

При всей своей эффективности и значительной распространённости «Аккорд-АМДЗ» и решения на его основе не всегда подходят, потому что они довольно дороги и сложны в настройке и использовании.

Для защиты ЦОДов и компьютеров x86, выполняющих задачи, требующие постоянного поддержания доверенной среды, этот вариант в наибольшей степени отвечает духу и букве требований регуляторов и здравого смысла.

Однако в некоторых других случаях он неудобен или даже неприемлем.

В первую очередь, это объекты критических информационных инфраструктур (КИИ), представляющие собой не офисы или ЦОДы, а включающие в себя некоторое специфическое оборудование. В финансовых системах это, например, банкоматы, терминалы оплаты, машины инкассации и многое другое. На транспорте это подвижные составы, корабли и самолеты, в энергетике – электроподстанции, «умные» приборы учеты, и т.д., и т. п.

Особенности таких объектов связаны, с одной стороны, со спецификой условий работы средства защиты, а с другой – с необходимостью работы в автоматическом режиме (в том числе, автоматический старт), с минимальным администрированием и обслуживанием. Решение для таких объектов – конкретно на примере банкомата – рассмотрено в [19], а спектр решений для КИИ, описанный в [20] еще будет рассмотрен в другом разделе.

Эти решения базируются на применении специализированных компьютеров с аппаратной защитой данных, или «вирусным иммунитетом» – микрокомпьютеров Новой гарвардской архитектуры. Про эту архитектуру можно прочитать в [8. С. 49–65; 105–135].

СВТ с Новой гарвардской архитектурой, не имеющей базовой уязвимости традиционных архитектур, не требуют установки средств защиты, способных менять архитектуру компьютера. Это существенно удешевляет и упрощает систему, так как дорогие и сложные в эксплуатации СЗИ не надо ни покупать, ни администрировать. Если предельно упростить, то защитные свойства компьютеров Новой гарвардской архитектуры основаны на том, что ничего (а значит, и вредоносное программное обеспечение или изменения, внесенные этим ПО) не записываются в долговременную память компьютера. Это и означает, что они не заражаются вирусами, имеют иммунитет к ним.

Место для таких компьютеров в информационной системе, кроме объектов КИИ, упомянутых выше, – это типовые рабочие места фронт- и бэк-офиса банка или любого «офисного» подразделения практически любой организации. «Офисное» – это такое, которое не решает

специфических в технологическом смысле задач, требующих каких-то особенных средств вычислительной техники или особенного, требовательного к СВТ программного обеспечения.

Подробно применение на таком участке микрокомпьютеров МКТ-card long описано, например, в [21]. Работа во фронт- и бэк-офисах, как правило, производится в рамках удаленного доступа в централизованной информационной системе, то есть сохранять файлы локально в долговременной памяти своего СВТ – не требуется. А те файлы, что все-таки необходимо сохранять или обрабатывать локально, могут храниться на защищенных служебных носителях «Секрет» [22], речь о которых пойдет в другом разделе.

1.3.3. Средства обеспечения доверенного сеанса связи

Случай, когда требования к простоте настройки усиливаются до «не должно быть никакой настройки», а низкая стоимость становится обязательным условием применимости – это ДБО, особенно тогда, когда клиентом ДБО является «физическое лицо». Сегодня практически нет банков, клиенты которых не пострадали бы от действий хакеров, атакующих системы ДБО, хотя это не какие-то качественно новые атаки, защититься от которых на современном этапе развития науки и техники было бы невозможно. Нет, атаки самые обычные, защищаться от них мы умеем. Более того, информационные системы банка зачастую защищены вполне надежно – это хорошо регулируется и тщательно контролируется.

Однако в ДБО участвует две стороны – банк и клиент. А это означает, что те компьютеры, с которых клиент взаимодействует с банком, тоже являются частью информационной системы, которую нужно защищать. Большинство успешных атак – это атаки на компьютер (в широком смысле – терминал – ноутбук, планшет, смартфон) клиента.

Не находя возможности повлиять на то, чтобы эти компьютеры были защищены, банки решают задачу минимизации своих потерь от таких атак, перекладывая ответственность на клиента. Это давно уже стало притчей во языцех [23], не станем останавливаться на этом подробно, сосредоточимся лучше на альтернативном подходе, который возможен: использование клиентом защищенной технологии взаимодействия с банком может быть *условием его обслуживания*. При этом возможно выстраивание гибкой логики, удобной и клиентам, и банкам – если клиент банка готов использовать защищенные способы доступа к своему счету, у него будут лучшие условия, страхование и прочие плюсы, если же он хочет использовать дешевые, но незащищенные технологии – то он сам отвечает за свои риски.

Однако это уже бизнес банков, вернемся к тому, какие должны быть созданы технические предпосылки для реализации этих возможностей.

Во-первых, необходимо, чтобы серверная часть компьютерной системы, реализующей функциональность ДБО, *была способна различать*[8], из доверенной или нет среды подключается в данный момент клиент. Декларируется, что это обеспечивается подключением, защищенным каким-либо VPN. Но, собственно, как? Ведь если ключи VPN у клиента находятся на отчуждаемом носителе (что является условием эксплуатации большинства VPN), то гарантировать, что пользователь подключается с защищенного компьютера, а не с какого попало, наличие VPN не может. В этом случае все манипуляции с ключом лежат на совести пользователя (это оговаривается и в технической документации, и в договорах клиентов с банками), а пользователь, в свою

[8] Здесь необходимо снова сделать заметку – способность различения чего-либо – это свойство, которое нам будет требоваться в защищенных системах очень часто. По сути именно это требуется от любого защищенного объекта – машина должна пускать владельца, а не угонщика, значит, должна их различать; дверь в квартиру должна различать легальных жильцов и воров; компьютер – легального пользователя и злоумышленника; банк – владельца счета и мошенника, и так далее. «Различать» – в дальнейшем будем использовать в смысле «идентифицировать» – среду, устройство, клиента.

очередь, может обладать низкой социальной ответственностью. В любом случае, тот факт, что наличие нужного ключа ничего не сообщает нам о том, из какой среды производится попытка доступа, нужно помнить при проектировании системы идентификации/аутентификации, и в свое время мы к этому вопросу вернемся.

Однако и тогда, когда такая функциональность системой поддержана, установка на компьютеры клиентов комплекса средств защиты за 35–60 тысяч, да еще и ограничение возможности связи с банком единственным компьютером – условия выполнимые для корпоративных клиентов, но совершенно безумные для частных лиц.

Зато работа в доверенном сеансе связи (ДСС) здесь видится идеальным выходом.

Мы в семье используем для работы с он-лайн банкингом СОДС «МАРШ!» с того момента, как у одного из наших разработчиков прямо на его глазах через эту систему (того же банка, услугами которого мы пользуемся!), ушло в неизвестном направлении 450 тысяч рублей. Есть люди, пострадавшие намного больше, но никакой пример так не впечатляет, как тот, который наблюдаешь лично.

Использование «МАРШ!» для ДБО предельно просто.

1. Подключаем устройство в USB-порт произвольного недоверенного компьютера, например, в гостинице (это предельный случай неконтролируемости среды – кто что мог установить или просто «подцепить» на такой компьютер – не может быть известно никому).

2. С «МАРШ!а» загружается эталонная вычислительная среда, в которой автоматически запускается браузер (и более ничего запуститься не может – это наше решение, а по желанию заказчика там может быть, например, офис или еще что-то полезное; на нашем «МАРШ!е» есть еще только набор драйверов для принтеров, так как часто требуется распечатанное подтверждение оплаты).

3. В строке браузера можно вводить что-угодно, но встроенный межсетевой экран не даст открыть никакой сайт, кроме он-лайн банкинга того банка, услугами которого мы пользуемся (это значит,

что в оперативную память не загрузятся вирусы со случайных сайтов).

4. После завершения работы с банком, мы отключаем «МАРШ!» и перезагружаем компьютер, чтобы использовать все возможности интернет-серфинга без ограничений.

Таким образом, мы изолируем от возможного негативного влияния только среду взаимодействия с банком, но изолируем надежно.

Как это достигается.

Конструктивно «МАРШ!» выполнен в виде USB-устройства, и выглядит точно так же, как обычная «флешка». Такой конструктив позволяет использовать «МАРШ!» практически со всеми компьютерами, так как почти все компьютеры имеют достаточное количество портов USB.

Тем не менее, «МАРШ!» похож на флешку только внешне. На самом деле это активное микропроцессорное устройство, с многоконтурной криптографической подсистемой, проверенной защищенной операционной системой Linux, браузером, специальной подсистемой управления доступом к памяти и многим другим.

Основная задача «МАРШ!а» — создание доверенной среды функционирования криптографии. Для этого в специальном разделе его памяти размещается все необходимое для этого программное обеспечение.

При начале доверенного сеанса связи пользователь загружается с «МАРШ!а», обеспечивая тем самым доверенную среду. Далее стартует браузер и все сопутствующее программное обеспечение, необходимое для работы. В браузере в доверенном сеансе обеспечивается защищенный обмен информацией, с соблюдением всех требований 63-ФЗ [24].

Загрузка производится из защищённой от записи памяти «МАРШ!а», жёсткий диск компьютера не используется, он отключен вместе со всеми размещенными на нем вирусами и ВрПО. Конфигурация загруженной операционной системы максимально ограничивает свободу пользователя: ему недоступны органы управления операционной системы, рабочая среда полностью

изолирована от посторонних сетевых соединений, открытый трафик отсутствует, после завершения работы в браузере сеанс связи автоматически завершается, не позволяя пользователю делать лишнего.

После загрузки ОС на компьютер клиента и старта браузера устанавливается защищённое соединение на основе криптографических алгоритмов с сервером центральной ИС(VPN-шлюзом). При этом закрытые ключи и сертификаты хранятся в защищённой памяти «МАРШ!», и доступ к ним возможен только из ОС «МАРШ!а», поэтому подключиться к банку с какого-то случайного компьютера, загруженного неизвестно откуда, а не с «МАРШ!а», но используя ключи VPN с «МАРШ!а», пользователь не сможет: либо ОС загружена с «МАРШ!а», либо нет доступа к ключам. Таким образом, исчезает «привязанность» пользователя и средств обеспечения информационной безопасности к конкретной рабочей станции, но при этом появляется уверенность в том, что если пользователь вообще подключился, то точно из доверенной среды.

С точки зрения управления доступом «МАРШ!» представляет собой память, разделенную на несколько разделов (см. рис. 1.6). Как правило, это не менее одного раздела ReadOnly (RO), не менее одного раздела ReadWriteHidden (RWH), используются также разделы AddOnly (AO) и разделы с общим доступом RW. Разделение на разделы осуществляется при производстве, и пользователем изменено быть не может.

Рис. 1.6. МАРШ! как память, разбитая на разделы

Обычно в RO разделе размещается операционная система и другое ПО, которое является неизменяемым достаточно длительное

время, обновления и дополнения ФПО размещаются в одном из разделов RWH, в другом размещается ключевая информация VPN, а раздел АО используется для ведения аппаратных журналов событий безопасности.

Взаимодействие клиента с банком в случае применения обыкновенного «МАРШ!» осуществляется через сетевые подключения компьютера (см. рис. 1.7).

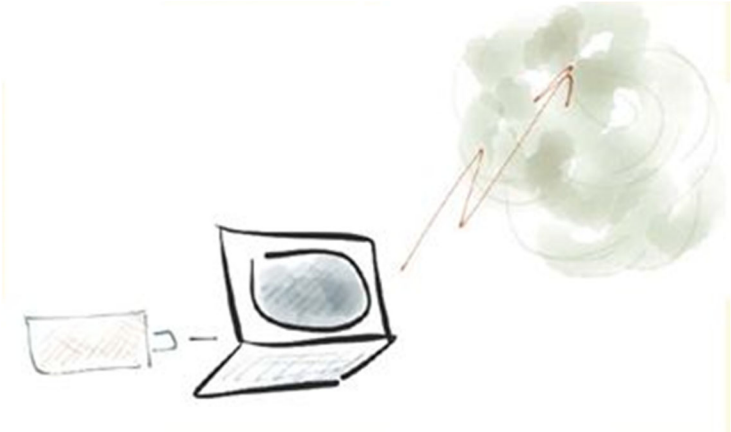


Рис. 1.7. Обыкновенный «МАРШ!» взаимодействует с сервером, используя сетевые интерфейсы компьютера

Это совершенно нормально для компаний, но у обычного пользователя может вызвать трудности в настройках, так как на территории страны услуги связи представляют сотни различных провайдеров, зачастую с проприетарными механизмами.

Пользователю, не владеющему навыками работы с сетевыми подключениями, лучше предоставить ненастраиваемое устройство, избавив его от множества проблем. В этом случае взаимодействие может осуществляться не через компьютер, а непосредственно через «МАРШ!», как показано на следующем рисунке 1.8.

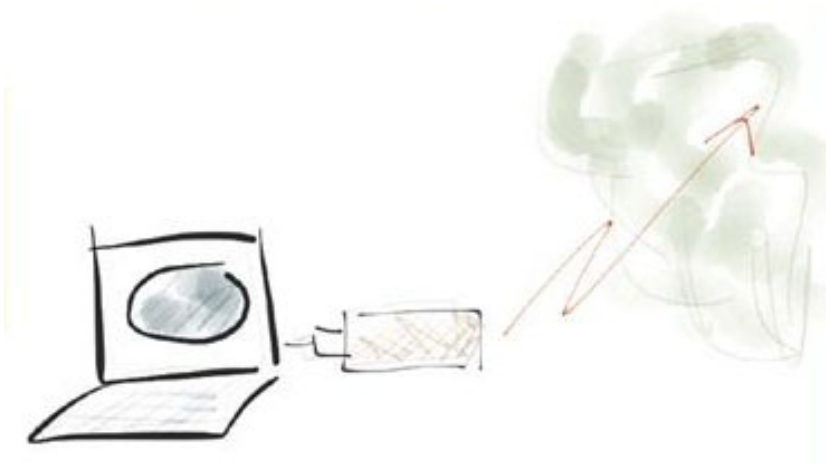


Рис. 1.8. «МАРШ!» с модемом взаимодействует с сервером, используя собственный сетевой интерфейс

В этом случае обеспечивается и простота эксплуатации, и высокий уровень защищенности. Достигается такой режим путем встраивания в «МАРШ!» беспроводного модема. Настройка на провайдера обеспечивается только SIM-картой. Такое решение называется «M!&M», или «МАРШ!-Модем» [25].

Такой подход позволяет использовать одно устройство как идентификатор, как носитель неизвлекаемых ключей, как модем, и как устройство обеспечения доверенного сеанса связи. Остается только одно – освободить пользователя от необходимости иметь под рукой какой-либо компьютер, к которому можно было бы подключить «МАРШ!». Такое решение тоже существует – в линейке микрокомпьютеров Новой гарвардской архитектуры.

Цена самого экономичного из микрокомпьютеров Новой гарвардской архитектуры – МКТ – в 10–15 раз ниже традиционного компьютера на базе x86, а подключается он к любому монитору или телевизору, имеющему интерфейс HDMI. В остальном все принципиально так же, как в случае с «МАРШ!ем». Очевидно, что это как раз то, что требуется для клиентов ДБО [26].

Если средство обеспечения ДСС (будь то «МАРШ!» или МКТ) будет позиционироваться аналогично банковской карточке – как собственность банка, предоставляемая клиенту на тех или иных

условиях для получения услуги, ситуация будет выглядеть крайне привлекательно как для клиента, так и для банка. Клиент банка получает ненастраиваемое устройство, которое обеспечивает загрузку неизменяемой проверенной операционной системы, устанавливает защищенное с использованием криптографических алгоритмов соединение с защищенным центром обработки данных, в котором установлено программное обеспечение (клиент ДБО) для доступа к автоматизированной банковской системе (АБС) банка. Риски клиентов и банка сведены к минимуму. При этом для клиента это еще и эффектный бизнес-аксессуар (см. рис. 1.9).

Рис. 1.9. Микрокомпьютер МКТ

Клиент ДБО (программное обеспечение) размещается в ЦОДе, отвечающем всем требованиям по защите информации, соответственно, доступ к АБС выполняется из одной, достоверно известной точки — из ЦОД, по защищенному каналу.

Технология доверенного сеанса связи гарантирует безопасность доступа клиента банка к своему клиенту ДБО (и, соответственно, к банку) из любой точки мира.

То есть клиент банка (человек) с помощью «МАРШ!» и компьютера в Интернет-кафе или микрокомпьютера МКТ из любого гостиничного номера, где есть телевизор, защищенно соединяется с клиентом ДБО (программным обеспечением), размещенным в защищенном ЦОДе и по защищенному каналу взаимодействующим с защищенной АБС

банка. Данные клиента обрабатываются в защищенной вычислительной среде, а хранятся на устройстве.

Финансовая сфера используется тут лишь в качестве примера для повышения наглядности. То, что все эти вопросы гораздо шире той или иной области деятельности, хорошо видно на примере ситуации, когда из-за введения режима самоизоляции в связи с эпидемией короновируса COVID-19 на удаленную работу переводились целые организации, в которых до тех пор такая работа не предусматривалась вообще, или предусматривалась лишь для крайне ограниченного круга сотрудников. Разумеется, большинство организаций положилось на «авось». Однако те из них, в которых защите информации уделяется существенное внимание, не ограничились активно рекламировавшимися для этих целей VPN и токенами для двухфакторной аутентификации, а обратились именно к средствам обеспечения доверенного сеанса связи.

Подводя итоги главы, необходимо явно сформулировать то, что внимательный читатель, скорее всего, обнаружил самостоятельно: говоря об обеспечении и поддержании доверенной среды, мы говорим так или иначе о ее целостности, ни о чем другом. Доверенная среда – это такая, которую никто посторонний *не изменил* в свою пользу.

Поэтому именно здесь нужно обратить внимание на разницу между *обеспечением целостности* и *контролем целостности*. Эти понятия часто смешиваются, что порождает массу ошибок не только в рассуждениях, но и в практике построения систем защиты.

Задача *создания и поддержания* доверенной среды не решается механизмами *контроля* целостности.

Они – эти механизмы – позволяют только *обнаружить нарушение* целостности или убедиться в его отсутствии. Предотвратить изменения – *обеспечить* целостность – средство *контроля* целостности не может.

Обеспечивается же целостность созданием режима, при котором исключены воздействия, которые могут ее нарушить. В разобранных примерах мы это хорошо видели.

В средствах создания и поддержания ДВС – это средства доверенной загрузки (не позволяют загружать ОС с нарушением установленных условий) и средства разграничения доступа (контроль запуска задач, контроль процессов и механизмы разграничения доступа не позволяют изменять то, что не должно быть изменено).

В средствах обеспечения ДСС – это минимизация состава среды и ее зафиксированность (нет задач – нет нужды контролировать их запуск, нет возможности записать изменения – нет нужды их запрещать).

В Новой гарвардской архитектуре сочетаются эти способы, что дает возможность установить разумный баланс между жесткой минимизацией среды и сложностью средств разграничения доступа (чем среда объемнее и универсальнее, тем более сложными должны быть средства ее контроля, и наоборот).

Так или иначе, в основе всех описанных подходов – *обеспечение* целостности, а не исключительно ее контроль. Контроля целостности – недостаточно, если нам необходимо, чтобы система *работала*, а не просто была защищена. Это важно хорошо запомнить.

Механизмы контроля целостности зачастую необходимы, но в крайне редких случаях (для решения очень специфических задач) они достаточны. Однако такие задачи все-таки есть, например, инвентаризация ПО рабочих станций. Речь идет о случаях, когда состав (в том числе, версии) ПО на компьютерах должен контролироваться, но недопустима остановка работы этих компьютеров в случае выявления нарушения целостности. То есть средство защиты должно проверять нет ли изменений, и, если они есть – не мешать работать, а только сигнализировать администратору, который должен рассмотреть представленный ему средством защиты анализ и принять решение о том, что делать дальше. Ситуация специфическая, но она встречается, к таким инструментам даже есть требования регуляторов, и средства с такой

функциональностью представлены на рынке. Среди продуктов ОКБ САПР – это «Паспорт ПО», о нем можно прочитать на сайте или в статьях.

Заметим, что только вскользь в этой главе упоминались информационные технологии. Это связано с тем, что основной акцент был сделан на создании и поддержании доверенной среды работы *пользователя*, а собственно информационные технологии – феномен, относящийся к *компьютерной системе*. Акцент таким образом был сделан просто для упрощения понимания материала, ведь пользователь всегда работает именно в КС, никак иначе быть не может.

Между понятиями «компьютер» (в любом его проявлении – СВТ, АРМ, ПК – неважно) и «компьютерная система» нет противоречия. Компьютерная система не всегда «больше» одного компьютера. Это просто другой аспект рассмотрения. КС может вся полностью состоять из одного компьютера, а может включать в себя нефиксированный список компьютеров, такие системы упоминались в примерах с ДБО. Просто для начала погружения в проблематику взгляд со стороны пользователя – удобнее.

Получив эти начальные сведения, для того чтобы не упустить из виду защиту информационных технологий как необходимую часть создания и поддержания доверенной среды, рассмотрим еще один мировоззренчески важный нюанс.

Если нам необходимо обеспечить, чтобы в КС исполнялась *вполне определенная* информационная технология (а, вообще говоря, нам всегда надо обеспечить именно это), то отсутствия каких-либо внешних влияний на программы недостаточно. Одна и та же программа при различных настройках, может работать по-разному – реализовывать разные ИТ, собственно, в этом и заключается смысл изменения этих настроек. Обобщенно это называется конфигурацией КС. Одни конфигурации обеспечивают выполнение желаемых информационных технологий, другие – тоже нормальные, допустимые с точки зрения ПО, могут быть опасными или совершенно неприемлемыми для данной информационной системы. Самый простой пример – установите

направление набора текста справа налево (а не слева направо) – и эффективность работы литературного редактора снизится в разы.

Вопрос контроля конфигурации компьютерной системы можно рассматривать с нескольких точек зрения:

1) *кто может влиять* на её изменение (задача разграничения доступа к настройкам КС, например, для виртуальных инфраструктур, это будет рассмотрено в главе про разграничение доступа);

2) *какие изменения* являются допустимыми и разрешенными, а какие должны блокироваться (задача контроля целостности конфигурации ИС [27, 28]).

Как выше уже упоминалось, не лишним будет повторить, решение одной или другой задачи – не альтернатива, они не взаимозаменяемы и должны решаться обе. Разграничение доступа позволяет не допустить изменения, а контроль целостности позволяет зафиксировать нарушение, если оно все же произошло. Даже при обеспечении доступа только доверенных пользователей только к разрешённым им функциям изменения конфигурации КС, необходимо проверять, что производимые настройки допустимы.

В заключение напомним об одной существенной детали. Доверенная вычислительная среда обеспечивает корректность выполнения программ в том смысле, что они исполняются так, как написаны, как эталонная версия, без искажений. Однако она не защищает от ошибок программного обеспечения, ошибок проектирования системы, неверного выбора или неверного применения технологий. В том числе, от неверного выбора или применения технологий и средств защиты информации. Поэтому раздел о доверенной среде – первый, но не единственный раздел этой книги.

СПИСОК ЛИТЕРАТУРЫ:

1. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. Минск: Серия «Библиотека журнала "УЗИ"», 2004. – 327 с.

2. *Кузнецов Н. А.* Информационное взаимодействие в технических и живых системах [Электронный ресурс] // Информационные процессы. 2001. Том 1. № 1. С. 1–9. URL: http://www.jip.ru/2001/1-1-2201.htm (дата обращения: 30.12.2021).

3. *Стрельцов А. А.* Правовое обеспечения информационной безопасности России: теоретические и методологические основы. Минск, 2005.

4. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД «Аккорд». Москва: «Радио и связь», 1999. – 325 с.

5. *Конявский В. А.* Серебряная пуля для хакера // Защита информации. INSIDE. СПб., 2013. № 4. С. 54–56.

6. *Конявский В. А.* Серебряная пуля для хакера (Окончание) // Защита информации. INSIDE. СПб., 2013. № 5. С. 69–73.

7. Машина Тьюринга // Википедия [электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%B0_%D0%A2%D1%8C%D1%8E%D1%80%D0%B8%D0%BD%D0%B3%D0%B0 (дата обращения 12.03.2020).

8. *Конявский В. А., Конявская С. В.* Доверенные информационные технологии: от архитектуры к системам и средствам. М.: URSS. 2019. – 264 с.

9. *Конявский В. А.* Иммунитет как результат эволюции ЭВМ // Инсайд. Защита информации. Спб., 2017. № 4. С. 46–52.

10. *Распе Р. Э.* За волосы // Приключения барона Мюнхаузена. Пересказ Корнея Чуковского. М.: Качели, 2020. С. 36–37.

11. Аккорд-АМДЗ // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/accord/accord-amdz/ (дата обращения 12.03.2020).

12. Новая гарвардская архитектура // Официальный сайт ОКБ САПР [электронный ресурс]. https://www.okbsapr.ru/products/newharvard/ (дата обращения 16.03.2020).

13. СОДС // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/storage/compute/sods/ (дата обращения 16.03.2020).

14. Положение Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

15. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Базовый состав организационных и технических мер».

16. Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [электронный ресурс]. URL: http://base.garant.ru/70727118/ (дата обращения: 12.08.2019).

17. РС БР ИББС-2.9-2016 «ИББС-2.9-2016 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации"» [электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/46924/rs-29-16.pdf (дата обращения: 12.08.2019).

18. РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» [электронный ресурс]. URL: https://www.cbr.ru/Content/Document/File/46928/rs-25-14.pdf (дата обращения: 12.08.2019).

19. *Конявская С. В.* Защита банкомата согласно Закону о КИИ: как избежать уязвимости традиционной архитектуры // Расчеты и операционная работа в коммерческом банке. М., 2020. № 1 (155). С. 13–25.

20. *Конявская С. В.* «Эта железка умнее меня!...» // Information Security/Информационная безопасность. М., 2020. № 1. С. 4–5.

21. Применение защищенных микрокомпьютеров МКТ-card lond в системах удаленного доступа смешанного типа // Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ». М., 2016. Вып. 3. № 114. С. 23–30.

22. Секреты // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/storage/flash/secret/ (дата обращения 18.03.2020).

23. *Конявский В. А.* «Всегда прав» или «Сам виноват»? // Защита информации. Инсайд. 2011. N 5. С. 70–77 (То же в электронной библиотеке: Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/library/publications/konyavskiy_2011_1/ (дата обращения: 05.05.2020)).

24. Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ [электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 05.05.2020).

25. M!&M // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/storage/compute/sods/m-m/ (дата обращения 18.03.2020).

26. *Конявский В. А.* Защищенный микрокомпьютер MK-TRUST — новое решение для ДБО // Национальный банковский журнал. М., 2014. № 3 (март).

27. *Мозолина Н. В.* Решение задачи контроля целостности конфигурации, основанное на атрибутной модели контроля доступа. // Вопросы защиты информации, 2017. № 3. С. 23–25.

28. *Мозолина Н. В.* Контроль целостности виртуальной инфраструктуры и ее конфигурации // Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ». М., 2016. Вып. 3. № 114. С. 31–33.

ГЛАВА 2. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ

2.1. Общие вопросы: что, где, когда

Идентификация, аутентификация и авторизация – это те функции защиты информации, с которыми сталкивается без преувеличения каждый. Хотя бы для того, чтобы отключить их на своем телефоне, планшете или компьютере.

Как правило, когда называются эти функции, речь идет об идентификации, аутентификации и авторизации *пользователя*. Однако это совершенно «не само собой разумеется». Идентифицированы и аутентифицированы защитными механизмами должны быть и объекты вычислительной среды, ведь до того, как объект идентифицирован и аутентифицирован, совершенно невозможно проверить его целостность. И именно авторизация производится, когда подсистема разграничения доступа дает определенному процессу возможность получить доступ к тому или иному объекту.

Иными словами, идентификация, аутентификация и авторизация пронизывают так или иначе все функции защиты информации.

Определение:

Идентификация (Identification – отождествление) – это отнесение объекта к определенной категории.

При этом, заметим, категория, к которой мы относим объект, может представлять собой как множество (вижу какую-то штуку, идентифицирую ее как сороку), так и единицу (вижу собаку, идентифицирую ее как свою собаку Жучку).

Идентифицировать пользователя – это определить, кто из пользователей перед нами. Идентифицировать компьютер, программу – аналогично – выяснить, какой это именно из компьютеров, какая именно из программ.

Как производится идентификация? Ответ подсказывается жизнью – по «особым приметам» – это и есть *идентификатор*.

Я идентифицирую сороку или Жучку по внешнему виду, это их идентификатор. Из двух одинаковых собак (хотя как собаки могут быть одинаковые?!) я могу идентифицировать свою, например, по ошейнику, тогда идентификатор – ошейник.

Компьютер – по серийному номеру материнской платы, процесс – по контрольной сумме кода (это не единственно возможные идентификаторы, а просто примеры).

Однако, обратим внимание на довольно очевидную вещь – если ошейник (который идентификатор моей собаки из двух одинаковых) на ней не надет, то он мне ничем не поможет. А вот соотнесение ошейника с собакой – это аутентификация.

Строго говоря, если не производится аутентификация, то нельзя сказать, что идентификация в полной мере состоялась, потому что пока мы не обнаружили каких-то подтверждений тому, что это именно он (пользователь, компьютер, процесс, сорока), мы имеем лишь предположение. А вот подтверждение идентификации каким-то образом – привязка объекта к его идентификатору – и есть аутентификация.

Определение:

Аутентификация (authenticity – подлинность) – это подтверждение связи между субъектом и признаком (идентификатором).

И вот дальше начнется такое количество «а может быть, и не так, а иначе», что прежде хочется привести пример на чем-то не таком многообразном, как аутентификация в цифровой среде.

Есть понятие «аутентичный», которое характеризует объекты культуры, как принадлежащие к какой-то категории (например, перу Шекспира, или этрусской культуре). Очевидна явная связь с аутентификацией – речь идет об установленной подлинности, просто характер этой подлинности другой и определяется она другими признаками – но таки именно наличием некоторых имманентных (то есть неотделимых от объекта) признаков. Способы установления аутентичности объектов материальной и духовной культуры сложны и разнообразны, требуют огромного количества специальных знаний и инструментария. Более того, результаты такой аутентификации – установления аутентичности – могут подвергаться сомнению и опровергаться веками.

Понимание этого обстоятельства задает некоторый фон восприятия вопросов аутентификации и в цифровой среде. Вопросы принципиально те же – насколько наличие того или иного признака действительно доказывает аутентичность.

Далее остановимся на этом подробнее, пока зафиксируем, что, вводя логин и пароль, мы сообщаем свой идентификатор – логин, и подтверждаем, что этот идентификатор, действительно, наш, чем-то, что система может проверить (паролем). Уже сейчас звучит весьма сомнительно (и не зря), однако для продолжения темы необходимо рассмотреть еще третье понятие – авторизацию, без которой идентификация и аутентификация повисают в воздухе.

Определение:

Авторизация (authorization – уполномочивание) – это сообщение объекту назначенных ему прав. Авторизованный пользователь – это тот,

который прошел аутентификацию и теперь уполномочен делать то, что ему можно по назначенным ему правам.

Всегда ли аутентификация сопровождается последующей авторизацией? Здравый смысл подсказывает правильный ответ – авторизация производится только в отношении тех объектов, которых можно «уполномочить», то есть активных, субъектов каких-то процессов. Объекты, которые не могут каким-либо образом действовать, уполномочивать ни на что не надо. Например, текстовый файл. Это обстоятельство нужно взять на заметку, так как при рассуждении ниже о том, является ли идентификация-аутентификация-авторизация жесткой связкой, которая должна реализовываться одним и тем же инструментом и существовать в виде неразрывной цепочки операций, нам эта улика понадобится.

Теперь становится очевидным место этой тройки. Оно, очевидно, *в начале*. Скорее всего, в большинстве источников вы прочитаете, что идентификация, аутентификация и авторизация проводятся *при доступе* некоторого субъекта доступа к некоторому объекту доступа. В значительном числе случаев это так и есть – постольку, поскольку в начале многих процессов информационного взаимодействия производится доступ чего-то к чему-то. Однако далеко не всегда наши и/а/а сопровождают именно его, иногда доступ отдельно, а и/а/а – отдельно, и производятся вообще в отношении совершенно других объектов.

Например, уже рассмотренный в качестве примера старт системы и загрузка ДВС – доверенная загрузка. Действительно, старт компьютера инициирует пользователь и зачастую (но не всегда!) с целью получить в конечном счете доступ к какому-то ресурсу. Но это не так, если пользователь просто запускает (или перезапускает) сервер. Или не сервер, а компьютер в банкомате или на каком-то еще объекте информатизации, где он – тот, кто запускает СВТ – вовсе не является пользователем какого-то ресурса.

Но рассмотрим более традиционный вариант – компьютер включает легальный пользователь, который собирается работать в ОС.

Проведение в отношении его идентификации, аутентификации и авторизации вполне выписывается в идеологию «при доступе» – он собирается получить доступ, в отношении него проводятся контрольные процедуры средством доверенной загрузки. Однако то же СДЗ проверяет при старте компьютера оборудование, реестр, файлы – все, что поставлено на контроль, и для этого, разумеется, все это идентифицирует и аутентифицирует. Даже если учитывать, что часть этих объектов активны и в процессе работы компьютера будут к чему-то получать доступ, лишь некоторая часть из них получает его именно сразу после прохождения и/а, большая же часть идентифицируется и аутентифицируется средством доверенной загрузки только с целью контроля их целостности, так как, напомню, невозможно убедиться в целостности объекта до того, как установишь, какой конкретно этот объект.

Связывать и/а с доступом – можно, но с известными ограничениями. Действительно, в значительном числе случае для получения доступа надо пройти какую-то и/а. Иногда этот процесс не очевиден для пользователя, например, при входе в ОС у пользователя может не запрашиваться ни логин, ни пароль, однако тем, с какой учетной записью загружается ОС (пользователя или администратора) определяется, какими правами будет располагать тот, кто будет работать в ОС. Это и есть авторизация, хотя никаких привычных видимых признаков и/а, типа ввода логина и пароля – не было.

Связывание и/а с доступом произошло в сознании общественности потому, что доступ воспринимается как некоторое «начало». И/а объекта, действительно, должна производиться всегда при начале работы с ним (нельзя работать неизвестно с чем), а вот авторизация – может производиться совершенно в другой момент, единственное, что мы об этом моменте можем сказать без какой-либо конкретики – этот

момент точно *до тех действий*, *на выполнение которых объекту авторизации нужны права*.

Рассмотрим еще несколько примеров для большей наглядности.

Межсетевые экраны или криптомаршрутизаторы осуществляют и/а подсистем системы при начале их взаимодействия (взаимодействие разрешается или запрещается конкретным, *идентифицированным* системам).

При начале взаимодействия с почтовым сервером производится и/а как пользователя, так и почтового клиента, и почтового сервера. *Пользователь*, в зависимости от настроек клиента, может идентифицироваться и аутентифицироваться как явно, так и автоматически, незаметно для себя, а и/а *клиента* и *сервера* обычно скрыта от пользователя, кроме случаев неуспешного завершения – тогда мы видим ошибку (она может быть разной – смотря кто кого «не узнал»).

Система защиты от несанкционированного доступа может включать в себя механизмы и/а клиентских СВТ, а не только пользователей, и тогда устройства, поддерживающие эти механизмы, передают при старте сессии данные о себе и проверяют данные о сервере. Здесь пока не рассматриваем вопрос о том, в каком случае этим данные можно доверять, разберемся с этим дальше.

Наконец, есть устройства, которые позволяют компьютеру работать с собой только после того, как он (компьютер!) пройдет и/а и будет авторизован ими (подключенными устройствами). Например, служебные носители (проще говоря, защищенные флешки) «Секрет». Они проверяют компьютер на предмет его наличия в их списке разрешенных (например, «Секрет особого назначения» проверяет компьютер по 5 параметрам, в «Секрете Фирмы» это реализовано иначе, подробнее можно узнать из материалов о продуктах). И только если компьютер в списке есть, диски «Секретов» монтируются и устройства начинают процессы и/а пользователя, который пытается с ними работать.

От того, *какой именно* компьютер был идентифицирован устройством, оно может предоставить доступ к памяти с разными атрибутами. Есть продукты «Система Ниппель» и «Секрет Администратора», которые на одних компьютерах предоставляют доступ к своему диску типа «массторадж» на запись, а на других – на чтение. То есть на одних компьютерах можно что-то записать на флешку, а прочитать – нельзя, а на других – можно прочитать, но нельзя записать. А на тех, что вообще в списке отсутствуют, нельзя сделать вообще ничего. Для чего это нужно и как работает – можно прочитать в материалах об этих продуктах, а мы еще вернемся к этим продуктам в 6-й главе.

Далее рассмотрим некоторые важные для формирования начальных представлений о процессах идентификации, аутентификации и авторизации понятия.

Например, наверняка кажущиеся знакомыми, факторы аутентификации.

2.2. «Факторы аутентификации»

Как правило, одним из первых, что узнают люди о защите информации, становятся именно «факторы аутентификации» – заветные «знать/владеть». В то же время получить внятный ответ на вопрос, что же это такое – очень сложно. Как правило, ответ на этот вопрос (явный или имплицитный) дается в виде списка этих самых «факторов» (например, [1]), хотя, строго говоря, это, конечно, не может быть ответом на вопрос «что такое…?». В бытовом процессе узнавания, однако, легко вспомнить массу таких случаев – ребенку объясняют, что такое цвет, перечислением цветов, а не объяснением природы этого явления, и многое другое постигается таким же образом. Но что хорошо в детстве – не вполне уместно в защите информации.

Факторы вводятся для того, чтобы сформулировать на их основе понятие о двухфакторной (или многофакторной) аутентификации. Понятие «однофакторная аутентификация», кстати, заметного распространения не имеет.

«Общим местом» является список из трех факторов:

1) знание,
2) владение,
3) биометрия (обладание некоторой биологической особенностью).

Двухфакторная аутентификация (сейчас модно ее обозначать 2FA), как правило означает комбинацию из «знать» и «владеть».

Согласно стандарту NIST «Руководство по цифровой идентификации. Аутентификация и управление жизненным циклом» [2] биометрический фактор является дополнительным, способным подтвердить обладание субъекта тем предметом, который для него воплощает фактор «владения» (например, биометрическое подтверждение того, что данная смарт-карта – этого человека): «Биометрия ДОЛЖНА использоваться только как часть многофакторной

аутентификации с физическим аутентификатором (*то, что у вас есть*)» [2. Раздел 5.2.3][9]. То есть в многофакторной аутентификации этот «фактор» может быть только третьим. Если *заменить* ввод пароля к смарт-карте предъявлением отпечатка пальца, то аутентификация перестанет считаться многофакторной, допустимо только *добавить* предъявление биометрического признака[10].

Иногда к факторам также относят расположение в определенном месте [3. С. 13], но согласно ISO/IEC 29003 [4] – это не фактор, а только свидетельство, то есть данные, которые могут дополнительно привлекаться для усиления уверенности в положительном результате аутентификации или при первичной идентификации. В то же время, согласно ISO факторов все-таки 4, но 4й – это не расположение в пространстве, а то, что субъект «обычно делает» (например, какие-то поведенческие паттерны) [4. Раздел 3.6].

Пришло время признать, что использование системы понятий, сформировавшейся вокруг сленгового идиоматического выражения «факторы аутентификации» на современном этапе развитии науки и техники вредно и должно быть прекращено.

---

[9] В пункте 4.2.1 при этом есть примечание «Примечание. Если биометрическая аутентификация соответствует требованиям, изложенным в разделе 5.2.3, устройство должно быть аутентифицировано в дополнение к биометрической – биометрия признается как фактор, но сама по себе не распознается как аутентификатор. Поэтому при проведении аутентификации с использованием биометрии нет необходимости использовать два аутентификатора, поскольку связанное устройство служит “чем-то, что у вас есть”, в то время как биометрия служит “тем, чем вы являетесь”». Чтобы исключить искажение смысла некорректным переводом, приведем оригинал: «Note: When biometric authentication meets the requirements in Section 5.2.3, the device has to be authenticated in addition to the biometric — a biometric is recognized as a factor, but not recognized as an authenticator by itself. Therefore, when conducting authentication with a biometric, it is unnecessary to use two authenticators because the associated device serves as “something you have,” while the biometric serves as “something you are.”». Судя по всему, этот текст тоже указывает на некоторую несвободу биометрического признака, хотя и не говорит ничего о природе этой несвободы.

[10] Благодарю А. Г. Сабанова за это уточнение, данное в личной беседе.

Для того чтобы вы могли принять на этот счет собственное информированное решение, разберем классификацию «факторов аутентификации» в соответствии с научной методологией, это всегда дает наиболее наглядные результаты, потому что основа современной научной методологии – рациональность.

В отношении классификаций в научном исследовании возможна постановка нескольких принципиальных вопросов.

1. *Является ли рассматриваемое классификацией*, или имеет место результат какой-то другой операции над предметом изучения. Это важно постольку, поскольку именно к классификации применимы требования быть исчерпывающей, построенной на одном основании, причем на основании значимого для всего классифицируемого множества признака, и так далее. Если перед нами не классификация, то эти требования не могут считаться обязательными.
2. *Корректна ли классификация* – то есть соответствует ли она действительному наблюдаемому положению вещей.
3. *Целесообразна ли классификация* – то есть продуктивна ли она, позволяет ли она решить какие-либо задачи (прогнозирование, объяснение причин и др.), устанавливаются ли соответствие или связи иного рода между нею и другими фрагментами научного описания того же сегмента действительности. Это важно, так как всегда желательно минимизировать изменения в устоявшейся практике, поэтому если бы оказалось, что классификация аутентифицирующих данных, в настоящее время в научном обороте представленная перечнем «факторов аутентификации» построена с нарушениями, но при этом она целесообразна, то имело бы смысл постараться ее сохранить, устранив недостатки, а не создавать новую классификацию на других основаниях.

2.2.1. Понятие «фактор»

Понятие, лежащее в основе классификации, очевидно должно быть определено, так как этим определением задаются границы класса. Все, что попадает в область определения этого понятия – каждый

конкретный случай его проявления – должно быть возможно отнести к какой-то из выделяемых классификацией групп. Без такого определения проверить корректность и полноту классификации невозможно.

Определение фактора аутентификации дано в проекте ГОСТ Р 58833-2020 «Идентификация и аутентификация. Общие положения» [5. С. 7]: «фактор аутентификации: Вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа или объектом доступа при аутентификации».

Поскольку это определение является предметом критики, не выделяем его как определение для запоминания.

Похожее определение есть в [3. С. 13] и других работах, определение из проекта ГОСТ выбрано потому, что он разработан теми же авторами, что и другие работы, содержащие определение «факторов аутентификации», и при этом является последним по хронологии, то есть аккумулирует результаты развития их взглядов на предмет.

Рассмотрим, что удается почерпнуть из этого определения.

«Аутентификационная информация» и «информация, предъявляемая субъектом доступа или объектом доступа при аутентификации», – это в общем случае одно и то же, так что это уточнение ничего не добавляет к основной части: «вид (форма) существования аутентификационной информации».

Надо отметить, что «форма существования» – это формула, естественная для научного дискурса вообще, и к понятию информации она применяется достаточно часто. По системе определений, сформулированной А. А. Стрельцовым [6. С. 10–33], информация существует ***в форме сведений и сообщений***, при этом и та, и другая форма существования информации – определены и четко отделены одна от другой. По системе определений В. А. Конявского [7. С. 179–191], в цифровой среде следует говорить не об информации как таковой, а о ее отображении (если провести параллель с системой определений Стрельцова, то в ней сведения отображаются в сообщениях). Отображается информация или в статической форме – ***в форме данных***

(чисел, представляющих собой упорядоченное множество символов) или ***в форме процессов*** – динамической форме.

В обеих системах дефиниций понятна природа определяемых феноменов, понятны их взаимосвязи и следствия из них – «форма существования» информации в виде сведений и сообщений позволяет выделить и определить предмет правоотношений, форма существования в виде данных и процессов – построить модель электронного документа и его защиты.

Что позволяет прояснить «существование аутентифицирующей информации в форме факторов аутентификации»?

Анализируя введенный в научный оборот закрытый перечень «факторов аутентификации» (поскольку определение должно анализироваться не изолированно, а в совокупности с практикой применения термина), можно сделать вывод, что «вид» и «форма» здесь характеризуют парадоксальным образом как раз не форму, а содержание. На содержательном уровне «факторы» и «аутентификационные данные», действительно, некоторым образом связаны.

1) Фактор «знание» связан с паролями в том смысле, что пароль требуется *знать*.

2) Фактор «владеть» связан с аппаратным идентификатором в том смысле, что чтобы его предъявить, он у пользователя должен быть в наличии («владеть» тут не очень подходит, потому что обычно владельцем идентификаторов является организация, не пользователь, но если это личный идентификатор – то да, «владеть»).

3) Фактор «биометрия» связан с папиллярным узором на пальце тем, что это биометрический признак.

4) Фактор «расположение в пространстве» связан с геолокационными данными в том смысле, что они сообщают о том, где в пространстве расположен объект.

5) Фактор «обычное поведение» связан с поведенческими паттернами в том смысле, что они его описывают.

Однако, даже с учетом наличия этой смысловой связи, «расположение в пространстве» – это не форма и не вид существования геолокационных данных, даже метафорически вряд ли можно сказать, что геолокационные данные существуют в форме (или в виде) расположения в пространстве. Это высказывание просто не имеет никакого смысла. То же самое будет, если попытаться подставить в эту конструкцию другие факторы: пароль существует в форме знания, ТМ-идентификатор существует в форме владения и так далее.

Скорее можно говорить о разделении всех возможных для применения в процессе аутентификации данных на классы по тому, *чем* в реальном физическом мире является *их источник* – знанием, характеристикой какого-то предмета, физиологической особенностью, местом, образом действия. Но почему следует поступить именно так?

Заметим, что речь может вестись только именно о том, что является источником, а не о том, что представляют собой сами данные, это нужно хорошо понимать, ведь компьютерная система не может работать ни с предметом, ни со знанием, ни с расположением, ни с чем другим из реального мира, она может работать только с цифровыми данными, введенными через строго определенные интерфейсы (допустим, если пароль надо ввести на клавиатуре, то бесполезно его называть вслух или показывать на бумажке – хотя пароль будет и верный, пока он не будет введен с клавиатуры, аутентификация успешно не завершится)[11].

Содержание понятий раскрывается, помимо определений и прямых классификаций, контекстом их применения. В ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации» [8. С. 11] упоминается еще один процесс (помимо предъявления при аутентификации), в котором участвуют аутентифицирующие данные и факторы аутентификации: «для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При привязке должны использоваться следующие факторы…». Здесь снова, казалось бы, создается некоторый интуитивно понятный образ: данные

[11] Этот момент необходимо запомнить, в дальнейшем он пригодится – в разделе 2.4.

с помощью чего-то привязываются к субъекту, который будет затем их предъявлять. Но, вообще говоря, совершенно не понятно, что же именно за этим стоит, если пытаться рассмотреть какой-то конкретный пример. Например, цифровой профиль отпечатка пальца – идентификационные данные человека. Неужели он *привязывается* к субъекту *с использованием биометрического фактора*? Что это может означать? Не говоря уже о том, чтобы включить сюда «форму существования» – как можно привязать информацию к чему-либо с помощью формы ее же существования?

При обсуждении терминов часто высказывается позиция о том, что обсуждение употребления тех или иных выражений только отвлекает от сути вопроса, заставляя искать и запоминать новые формулировки для того, что и так понятно. Дескать, ведь все, кто использует слово «доступ» или «фактор», или иное обсуждаемое – прекрасно понимают, о чем идет речь, а давать красивые определения – дело гуманитариев. Разобранные выше примеры показывают, что это «понимание» – мнимое, оно исчезает сразу, как только задаешь себе вопрос «что конкретно?».

В то же время, действительно, когда сложился определенный *узус* (грубо – обычай использования того или иного слова в том или ином контексте), может быть целесообразно просто переопределить понятие «фактор» более удачно и оставить общественности привычное словоупотребление. Казалось бы, в случае номинального определения – то есть такого, когда некоторому явлению присваивается некоторое имя («солнцем будем называть звезду, которая…»), рассуждать о том, что «на самом деле – это не так», – не уместно. Условимся, и будет так. Речь тут может идти только о целесообразности или нецелесообразность определения, а не о его истинности или ложности.

Во многом это справедливо, но есть одно ограничение – полностью свободны мы в назначении определения словам, которые до сих пор не значили вообще ничего. Пока слово «слон» свободно от значения – мы можем определить его как мелкого грызуна с рыжей шерстью, но как только у слова «слон» уже появляется некоторое значение, вошедшее в

употребление и закрепленное словарями – эту свободу определения мы утрачиваем, и договориться называть грызуна слоном больше нельзя, даже по взаимному согласию (за исключением, конечно, каких-то игровых контекстов).

Так вот, у слова «фактор» уже есть значение. Это значение такое:

«ФАКТОР, -а; м. [от лат. factor – делающий, производящий] *Книжн.* Существенное обстоятельство, способствующее какому-л. процессу, явлению. *Учесть все факторы. Немаловажный ф. Постоянно действующий ф. Неизбежный ф. Ф. времени. Ф. успеха, победы. Ф. внезапности (воен.;* неожиданные для противника действия, способствующие его поражению). *Поражающие факторы ядерного взрыва* (совокупность причин, приводящих к разрушениям, смерти). *Человеческий ф.* (роль и значение человека в общественной жизни, в социальных процессах; всё то, что связано в этих процессах с человеком как субъектом деятельности)» [9].

То есть словосочетание «фактор аутентификации» может означать или обстоятельство, влияющее на аутентификацию, или саму аутентификацию, как явление, влияющее на что-то еще. Назначить этому выражению смысл «вид (форма) существования информации» нельзя, ни на русском, ни на английском языке, где слово factor тоже, разумеется, имеет латинское происхождение.

К слову, при словарной трактовке слова «фактор» и знание чего-то, и владение чем-то, и биологические признаки чего-то – действительно являются факторами аутентификации – то есть тем существенным обстоятельством, которое оказывает на аутентификацию влияние, способствует ей, должно учитываться. Но надо признать, что эта (словарная) трактовка разрушает всю систему терминов, построенную в западных стандартах (и распространившуюся в сфере защиты информации повсеместно) вокруг «факторов аутентификации». Ее принятие, фактически, равносильно отказу от «факторов аутентификации» как основы всех дальнейших построений. Например, если попытаться подставить это значение в «многофакторную аутентификацию», получается очевидный тупик. Важнее, однако, другое

– в этом «словарном» значении понятие «фактор аутентификации», скорее всего, вообще не может быть положено в основу классификации, так как исчерпывающий перечень факторов, влияющих на аутентификацию, едва ли возможно сформировать и привести к единому основанию. В этот список, например, необходимо будет включить фактор времени аутентификации (причем, в обоих смыслах – и продолжительность процедуры, и время (время суток, время года, день недели), в которое она может завершаться по-разному) дееспособности субъекта (или исправности, если субъект не является человеком), фактор намерения (субъект может иметь целью пройти аутентификацию успешно или наоборот – неуспешно, подтвердить, что он «тот» или подтвердить, что он как раз «не тот», причем, и в том, и в другом случае, он может быть заинтересован как в правде, так и в ошибке) и многое-многое другое. Вероятно, можно составить классификацию типов факторов, но сама эта классификация и ее задачи будут далеки от того, как используются «факторы аутентификации» сейчас. Это не говорит о том, что такая работа не нужна (например, она может быть полезной при составлении Модели угроз и при выборе способа и реализации системы аутентификации), но ее целесообразность нуждается в оценке и обосновании.

Таким образом, очевидно, что ни термин «фактор аутентификации», ни его определение в том виде, в котором они существуют сегодня в сфере защиты информации, не могут быть признаны хоть сколько-нибудь приемлемыми.

Однако, даже если неприемлемы и сам термин, и его определение, имеет смысл все же рассмотреть саму классификацию.

Если она сама по себе жизнеспособна, то, вероятно, замена термина на более удачный может дать возможность оставить ее в целом неизменной.

2.2.2. Классификация «факторов»

Основания считать, что перечень факторов аутентификации позиционируется как классификация, – есть. Перечень классов всегда

представляется как закрытый, несмотря на то, что факторов от 2 до 4 (при этом самих пунктов 5 (знать, владеть, биометрия, расположение, поведение), но все 5 одновременно в одном перечне никогда не встречаются, и более того, в построениях, в которых факторы используются вне перечней, эксперты ISO склонны даже сужать перечень «факторов в чистом виде» до 2, а остальные называть – дополнительным фактором, свидетельством и так далее).

Однако в классификации должен быть ясно выраженный классификационный признак, все классы должны быть выделены на одном основании и, наконец, классификация должна быть исчерпывающей и желательно постоянной в своем составе (или по крайней мере разные представления о составе классификации должны быть соотнесены между собой в какой-то дискуссии, а не существовать просто параллельно).

Классификационный признак

Классификационный признак должен быть связан с целью, для которой проводится классификация, он должен быть объясним.

Не удается обнаружить явных причин тому, что классифицировать аутентифицирующие данные целесообразно именно *по источнику*. Более того, если на основании «факторов» аутентификации строятся дальнейшие рассуждения, то оценивается не то, откуда данные берутся, а признаки, характеризующие степень их связанности с субъектом. Чаще всего – *насколько необходимо* вступать в контакт с субъектом, и *насколько тесным* должен контакт для того, чтобы злоумышленник смог получить эти данные в свое распоряжение. То есть разделяются феномены на группы по одному признаку, а используются далее – другие признаки, свойственные этим же группам (возможно, эти группы признаков связаны, но эта связь не описана).

Единое основание

О едином основании в перечислении «знать, владеть, биометрия» говорить невозможно. Именно поэтому, видимо, биометрию зачастую назначают «дополнительным» признаком.

Полнота классификации

1. *Охвачены не все типы субъектов*

Первое, что необходимо отметить в связи с полнотой классификации, это то, что классификация «знать-владеть-биометрия» оставляет полностью не закрытым один из двух (!) типов субъектов аутентификации.

Не универсальность подхода становится очевидной при попытке применения «факторов» для создания общего описания процессов идентификации и аутентификации *любых субъектов*, не только пользователей в смысле людей, но и сущностей цифровой природы. Именно это наблюдаем в разрабатываемом ГОСТе [8. С. 11], в частично уже приведенном фрагменте:

«Для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При привязке должны использоваться следующие факторы[12]:

- фактор знания. Привязка устанавливается с использованием информации, которая известна (свойственна) субъекту (объекту) доступа;
- фактор владения. Привязка устанавливается с использованием идентификационных данных, которые имеет (обладает) субъект (объект) доступа. При этом идентификационные данные свойственны (присущи) субъекту (объекту) доступа или содержатся в его свидетельствах, представляющих собой документальное подтверждение. Субъект (объект) доступа должен правомочно обладать данными свидетельствами;

[12] Общая характеристика факторов – по ГОСТ Р Идентификация и аутентификация. Общие положения.

- фактор биометрический. Привязка устанавливается по результатам верификации биометрических характеристик, которые свойственны субъекту доступа – физическому лицу. При этом принимается, что эталонные характеристики субъекта доступа действительно принадлежат ему.

Примечания

1 Условно считается, что при привязке для субъектов доступа и объектов доступа, которые являются информационными и вычислительными ресурсами [средствами вычислительной техники, автоматизированными (информационными) системами и т.п.], используется один фактор. По решению оператора и при выполнении условий, определенных требованиями к первичной идентификации, может считаться, что при привязке субъектов доступа и объектов доступа, которые являются информационными ресурсами, используется более одного фактора».

Приведенный текст очень наглядно показывает искусственность этого построения. Очевидно, что не просто «не все», а ни один из «факторов» (кроме относительно нового и не совсем фактора, который коротко назовем «расположение») не может быть *без оговорок* отнесен ни к процессу, ни техническому или программному средству, ни к информационной системе в целом (ни что из перечисленного не может ни знать, ни владеть, ни иметь биологические особенности). Что именно сообщается в примечании – совершенно не понятно: используется один фактор – а какой? Может использоваться более одного – а какие?

Терминологическая система, подходящая без оговорок только одной из двух глобальных групп субъектов, очевидно, несовершенна.

2. *Охвачены не все фактически применяемые для аутентификации виды данных*

«Формы существования» аутентифицирующих данных, которые без оговорок не укладываются в «знать» и «владеть», зачастую называются

«свидетельствами». Например, паспорт – это официальное свидетельство. Действительно, в парадигме «знать-владеть-биометрия» классификация паспорта как того, с помощью чего человек аутентифицируется, затруднительна хотя бы потому, что некоторые из паспортов – биометрические, а некоторые – нет. А главное, в отношении паспорта каким-то сомнительным представляется установление связи «владение». Вместе с тем, кроме этого затруднения, нет никаких причин отказывать паспорту в том, что он является носителем аутентифицирующих данных.

Но свидетельства в парадигме понятий ГОСТов [5, 8] могут применяться только в процессах идентификации, а не аутентификации, а значит, паспорт не может применяться для аутентификации, а может применяться только для идентификации[13]. Хотя наблюдение над практикой аутентификации показывает обратное: как правило мы показываем паспорт именно для того, чтобы подтвердить декларацию «я такой-то».

Разумеется, не охвачены классификацией те виды данных, которые предъявляются субъектами цифровой природы – контрольные суммы, серийные номера, UID'ы и аналогичные (отнесение их к фактору «владеть» из приведенной выше цитаты более чем сомнительно).

Отступление о влиянии точки зрения на реальность

Любопытно, что между примером с серийными номерами и паспортом гораздо больше общего, чем представлялось сначала. В обсуждении представленных в этой главе выкладок от некоторых специалистов-практиков звучали возражения, что серийные номера и UID'ы – это идентификаторы, а отнюдь не носители аутентифицирующих данных. Легко заметить, что это возражение абсолютно симметрично

[13] Этот вывод не является вымыслом автора, он получен от А. Г. Сабанова, который является в нашей стране главным апологетом теории факторов, в личной беседе о том, к какому фактору аутентификации относить паспорт.

утверждению А. Г. Сабанова о том, что идентификатором, а не носителем аутентифицирующих данных является паспорт человека.

В 1984 году был снят гениальный болгарский мультфильм «Фигури и форми»[14] (это на болгарском языке, поэтому название выглядит странно). В нем высокий и низкий человек смотрят на один и тот же объект и спорят о том, круг это или квадрат (см. рис. 2.1).

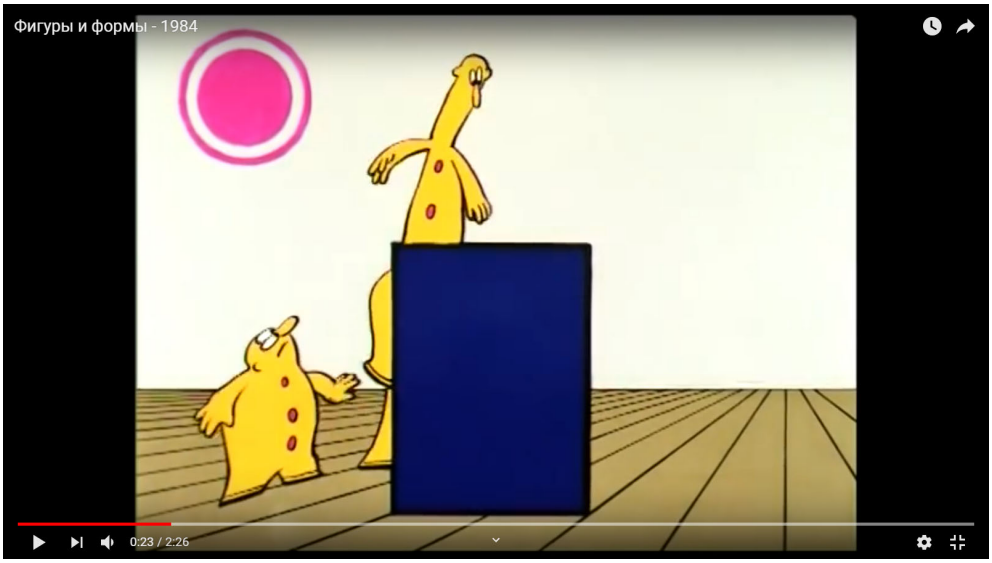


Рис. 2.1. Кадр из начала мультфильма «Фигури и форми»

В конце мультфильма объект падает и выясняется, что это цилиндр (см. рис. 2.2), однако герои продолжают спорить, так как теперь высокий видит квадрат, а низкий – круг. И только тот, кто, как выяснилось, был внутри объекта, сообщает героям, что это – цилиндр.

[14] https://www.youtube.com/watch?v=tMpkcpTSN_s

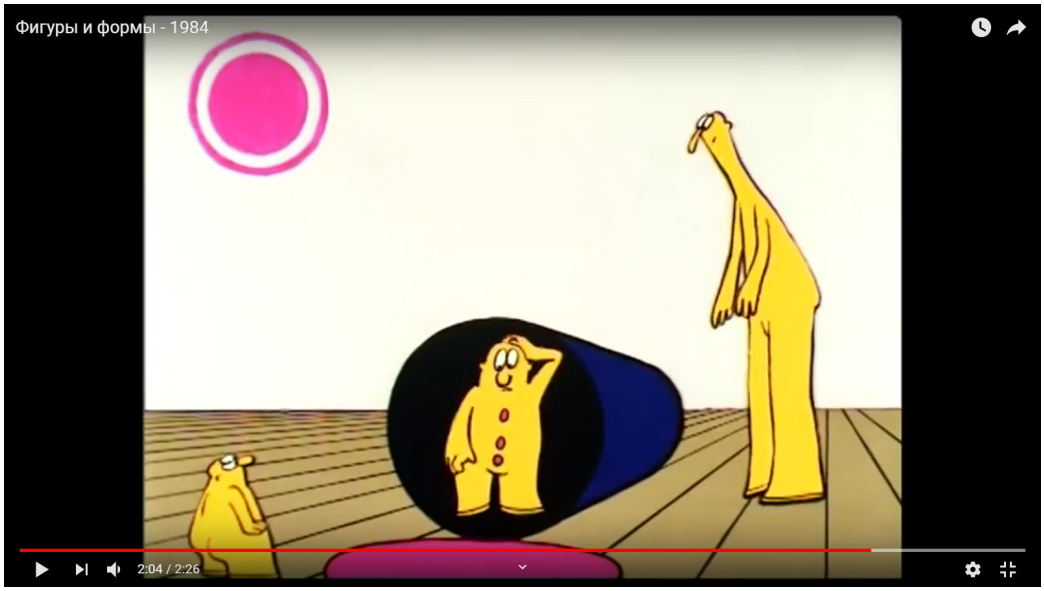


Рис. 2.2. Кадр из окончания мультфильма «Фигури и форми»

Разумеется, правы оба героя, так как они ясно определяют то, что видят. Однако видят они только то, что видно с их точки зрения.

Что такое нож – кухонная утварь или орудие преступления? Ответ зависит от того, что им в данный момент делают (или уже сделали).

Если я труп и рядом со мной обнаружен мой паспорт, то он (паспорт) – идентификатор. Если я пришла в присутственное место и представилась, а подтвердила свою самопрезентацию демонстрацией паспорта на такие же ФИО, то это носитель аутентифицирующих данных. Если мы ищем устройство с серийным номером 1765390, то номер – идентификатор, если же мы проверяем серийный номер устройства, чтобы дать или не дать разрешение на его использование – то это аутентифицирующие данные (а устройство – их носитель).

Признак может быть идентификационным или аутентификационным в зависимости от того, что сейчас выполняется – идентификация или аутентификация, в каком смысле признак предъявляется.

Это не означает, что один и тот же признак будет (или должен быть) непременно принят в любом качестве. Но это совершенно другой вопрос.

2.3. Как обойтись без факторов

Представляется вполне возможным устранить все приведенные выше недостатки системного описания аутентифицирующих данных таким образом, чтобы его можно было распространить на всю область определения субъектов аутентификации, причем без коренного разрушения привычной понятийной системы и без слова «фактор».

Коренные изменения нецелесообразны в первую очередь потому, что сама предметная область характеризуется высокой степенью стабильности: если что-то начинает использоваться для аутентификации, то остается в этом качестве как минимум надолго, несмотря на все недостатки способов аутентификации с помощью данных этого типа, как происходит с паролями, например. Их практически все и всегда только критикуют, но они продолжают использоваться и в старых, и в новых системах.

Если перечень возможных данных достаточно стабилен, и нет оснований считать, что он должен быть радикально изменен, то задача сводится к изменению *описания* сегмента действительности как он есть, то есть к фиксации результатов наблюдения над практикой.

Классификация, полученная таким – эмпирическим – способом, может быть принята к рассмотрению, если она будет:

полной,

на едином основании,

целесообразной, и

совместимой с другими объектами этого же семантического поля.

Например, будет без противоречий накладываться на перечень способов аутентификации, фактически применяемых на практике. При этом из классификации могут следовать возможности применения других, до сих пор не используемых способов или механизмов – и это

следует рассматривать как подтверждение эффективности предлагаемой классификации.

2.3.1. Предпосылки классификации аутентифицирующих данных

Предмет классификации

В первую очередь, необходимо зафиксировать, что в информационную систему мы в любом случае представляем только *данные*, а не знания, не собственность или что-то еще из аналогового или духовного мира. Поэтому речь должна идти о *данных*, характеризуемых какими-то *признаками* или наборами признаков.

Таким образом, предмет классификации – аутентифицирующие данные.

Способы аутентификации и *аутентифицирующие данные* – это разные вещи, и они не должны смешиваться. Является общим местом, что важно не только и не столько то, какие данные используются для аутентификации, сколько то, *каким образом реализован механизм аутентификации* в системе. Например, реализация парольной защиты может быть признана слабой в двух совершенно разных случаях:

1) если она не включает в себя проверку на слабые пароли (или какие-то механизмы блокировки угроз, связанных с их применением),
2) если слабые пароли в ней исключены, но сильные хорошие пароли – хранятся и передаются в открытом виде и в форме, делающей их доступными для нелегального применения.

То есть так или иначе, слабость пароля и слабость реализации – это две разные слабости.

Ниже речь пойдет не о способах и не о механизмах аутентификации, а именно об аутентифицирующих данных и их признаках.

Классификационные признаки

Первое, что необходимо проговорить явно – это то, что «аутентифицирующие» – это не более и не менее, чем «использующиеся для аутентификации». Аутентифицирующими данными могут любые, об использовании которых договорились стороны, участвующие в аутентификации. А как договорятся стороны – зависит от того, для чего им аутентификация нужна, что именно нужно подтвердить. Например, если кататься на карусели можно всем, кто уже выше 120 см, то в качестве подкрепления утверждения «мне уже можно», на входе на карусель предъявить нужно только рост[15].

То есть цель классификации аутентифицирующих данных – не в том, чтобы определить, какие данные могут быть аутентифицирующими, и ничего не пропустить, а в том, чтобы получить предпосылки для их анализа. В частности, определить, какие данные целесообразно использовать в качестве аутентифицирующих, а какие нет. А для тех, которые использовать в принципе целесообразно, выявить ограничения: какие условия требуется создать и поддерживать для доверия результатам аутентификации.

У аутентифицирующих данных можно выделять множество особенностей, и значительная часть описывающих эти особенности признаков будет важна с точки зрения защиты информации. Например, может требоваться точное совпадение сравниваемых данных с эталоном или совпадение в рамках некоторого диапазона: пример первого – пароль, второго – биометрический эталон.

Данные могут быть постоянными / условно постоянными / изменяющимися.

Постоянные – статические биометрические данные, они никогда не меняются. Однако, постоянным является так же и пароль, например, так как один и тот же пароль никогда не станет другим, его можно только поменять на другой – тоже постоянный.

---

[15] Заметим, что для авторизации понадобится еще оплата катания.

Условно постоянные – это данные, которые могут меняться, но не целенаправленно, а из-за каких-либо неконтролируемых обстоятельств. Таким признаком, например, является сосудистое русло ладони. Его принято считать неизменяемым биологическим признаком, но уже доказано, что приблизительно раз в полгода следует обновлять их эталон, так как рисунок сосудистого русла все же меняется.

Изменяющиеся данные – это данные, которые изменяются «сами по себе», независимо от воли человека, например, динамические биометрические данные[16] (они каждый раз разные, какие бы усилия ни приложил человек).

Другой признак – характеризующий не столько данные, сколько их применение – это кратность. Данные, использующиеся для аутентификации могут представлять собой «кортеж», содержащий кроме собственно представляемых в систему данных (например, пароля), еще данные о том, сколько раз можно использовать эти данные.

Эти – и многие другие – признаки важны, и они характеризуют именно те особенности аутентифицирующих данных, которые определяют их принципиальную применимость и ограничивают способы их применения в механизмах аутентификации. Но для классификации нужны такие признаки, которые характеризуют одновременно *все* возможные данные, причем характеризуют информативно, а не формально (так, наличие признака «частота» не дает оснований классифицировать звуки и цвета по длине волны в одну сплошную классификацию).

Признаки, по которым данные будут классифицированы, должны позволять строить на основе этой классификации рассуждения о защищенности механизмов аутентификации, использующих эти признаки аутентифицирующих данных. Значит, они *должны быть связаны с ключевыми элементами процесса аутентификации*.

---

[16] Например, слежение взглядом за перемещением по экрану случайного стимула [18, 19 и др.].

Рассмотрим, что это за элементы. Аутентификация – понятие относительное. Что-то одно можно аутентифицировать относительно чего-то другого, нельзя аутентифицировать что бы то ни было само по себе. Более того, даже объективно существующая связь между идентификатором и субъектом может в одном случае обеспечить успешную аутентификацию, а в другом случае решительно никак не повлиять на результат аутентификации. Например, совершенно бессмысленно показывать паспорт вместо предъявления карты СКУД или прикладывать палец к считывателю рисунка радужной оболочки глаза. И даже если технически предъявление возможно – это еще ничего не гарантирует, попробуйте предъявить не тот палец, который был зарегистрирован – несмотря на то, что он определенно ваш, аутентификация закончится неуспешно. Важно, что в процессе аутентификации производится подтверждение объективной связи субъекта именно с тем идентификатором, который является его признаком для второй участвующей в процессе аутентификации стороны.

В процессе аутентификации участвует не менее двух сторон. Если это стороны А и Б, то:

1. А можно аутентифицировать относительно Б;
2. Б можно аутентифицировать относительно А;
3. Стороны А и Б можно аутентифицировать одну относительно другой – взаимно аутентифицировать.

Назовем участвующие в аутентификации стороны субъектом и объектом аутентификации, так как даже при *взаимной* аутентификации все равно каждый конкретный случай аутентификации какая-то сторона инициирует, и в этом смысле разделение *субъекта* и *объекта* вполне уместно и, как кажется, не порождает никаких проблем.

Выше уже упоминалась разница между объектом доступа и объектом аутентификации, важно о ней не забывать. Когда администратор включает сервер, этот сервер может не быть объектом доступа, так как решительно никаких действий на нем администратор не выполняет, он может даже не иметь на нем учетной записи

пользователя ОС (а быть, например, только пользователем СДЗ). Однако объектом аутентификации сервер определенно будет. В зависимости от реализации подсистемы защиты информации объектом аутентификации при процедуре включения сервера может быть не сервер, а СДЗ на сервере, однако, общей картины это не меняет, так как объектом *доступа* он все равно не будет: пользователю не станет доступно выполнение никаких операций ни с сервером, ни с СДЗ.

Объектом доступа может быть некоторый целевой ресурс, а не информационная система целиком или даже СВТ. Аутентификацию в идентификации/аутентификации банкомата клиент банка проходит для того, чтобы получить доступ к своему счету, а не к банкомату. И *объектом аутентификации* будет банкомат как информационно-вычислительный ресурс, предоставляющий доступ к целевому *объекту доступа*[17].

Определения:

Объект доступа – объект, на выполнение операций над которым претендует субъект доступа. Успешный результат процедуры доступа – возможность выполнения операций субъектом над объектом (например, чтения, записи и так далее). Условием для успешности процедуры доступа может быть ***авторизация***.

Определение основано на ГОСТ Р «Защита информации. Формальное моделирование политики безопасности Часть 1. Формальная модель управления доступом» [10].

Объект аутентификации – объект, относительно которого аутентифицируется субъект. Успешный результат процедуры

[17] Необходимо заметить, что терминологическая система в отношении этих понятий далека от совершенства, поэтому ссылки на принятые определения не приводятся, они ничего не прояснят. Новые определения вводятся для выстраивания понятийного аппарата. В нормативных методических документах приняты другие.

аутентификации – подтверждение связи пользователя и предъявленных им идентификационных данных пользователя.

Это разделение существует и в аналоговом мире. Я аутентифицируюсь в ЗАГСе по паспорту, но чтобы получить доступ к услуге (регистрация вступления в брак или расторжения брака, например), мне надо оплатить гос.пошлину, то есть успешной аутентификации для доступа не всегда достаточно.

А в целом ряде других случаев – и в цифровом, и в аналоговом мире, наоборот, для доступа к чему-либо не понадобится вовсе никакая аутентификация.

Вывод – целесообразно разделять аутентификацию, авторизацию и доступ, это разные процессы, хотя и часто связанные в цепочки последовательных и взаимообусловленных шагов.

Говоря о типах аутентифицирующих данных, останемся в рамках процесса аутентификации.

Итак, аутентифицирующие данные используются для того, чтобы подтвердить для объекта аутентификации связь между субъектом аутентификации и его идентификатором.

Процесс этот состоит из предъявления данных субъектом и проверки данных объектом (см. рис. 2.3).

Рис. 2.3. Предъявление субъектом аутентификации аутентифицирующих данных для проверки объектом аутентификации

Различные аутентифицирующие данные могут быть охарактеризованы с точки зрения и других процессов – порождения этих данных, их хранения, обработки, передачи. В этих случаях могут рассматриваться такие параметры, как носитель и канал передачи данных объекту[18], источник и характер порождения данных, организация хранения и другие особенности, однако для того чтобы было возможно рассматривать эти аспекты системно, целесообразно классифицировать аутентифицирующие данные на самом высоком уровне – с точки зрения их ***связанности*** с субъектом и объектом аутентификации.

Связанность с объектом аутентификации

Не зависеть от объекта аутентификации совсем аутентифицирующие данные не могут, так как иначе они не смогут сыграть целевую для них роль – доказательства. Объект должен располагать какими-то данными для того, чтобы принять решение о корректности представленного подтверждения. Эти данные могут быть *именно теми*, которые субъект будет предъявлять, или какими-то *косвенными данными*, позволяющими определить корректность данных, не располагая ими «в лоб». Например, так производится проверка ключа подписи атрибутного сертификата – ключом подписи субъекта объект не располагает, но располагает возможностью проверить его корректность.

По этому признаку аутентифицирующие данные можно разделить на те, что требуют *простой* проверки (рис. 2.4), и те, что требуют проверки *функциональной* (рис. 2.5). В первом случае производится сравнение предъявленных данных с эталонными, во втором – вычисляется некоторая функция.

---

[18] Канал передачи данных от субъекта в подсистему аутентификации объекта зачастую определяется применяемым носителем данных (USB-токен не передаст данные через сканер отпечатка пальца и наоборот), поэтому их целесообразно рассматривать в связке как интерфейс передачи данных от субъекта объекту.

В системе:

Пользователь предъявляет:

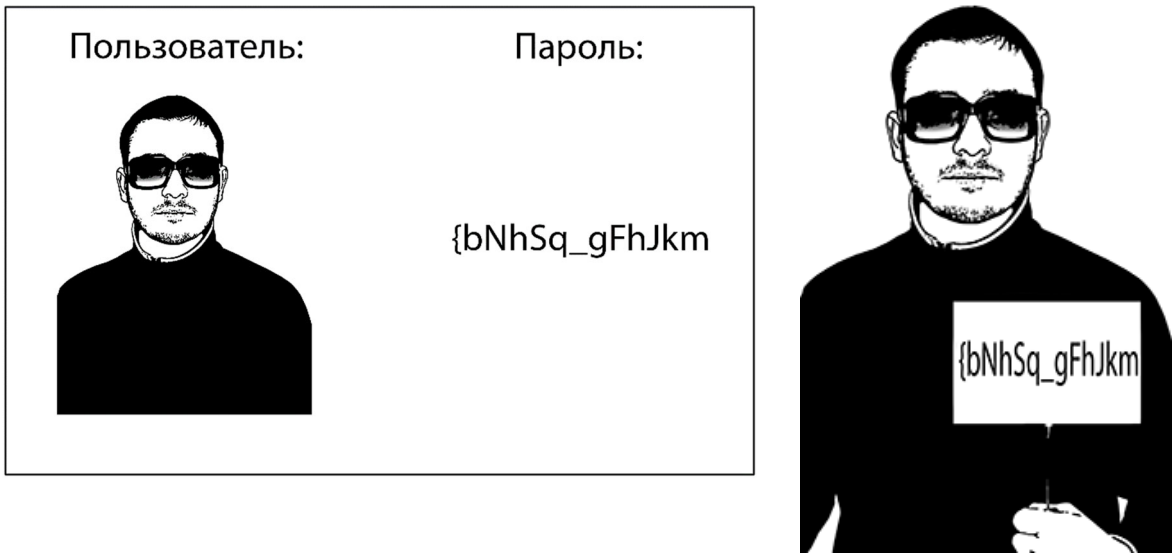


Рис. 2.4. В системе пользователю сопоставлен ***назначенный ему пароль****, пользователь при аутентификации должен предъявить* ***тот же самый*** *пароль*

В системе:

Пользователь предъявляет:

Рис. 2.5. В системе хранятся данные и реализованы механизмы для проверки предъявленных аутентифицирующих данных (в данном случае данные – это половинка разрезанной банкноты, а механизм – сложить имеющуюся половинку с предъявленной и оценить, от той же банкноты предъявленная половинка или нет). Пользователь предъявляет другие данные (другую половинку банкноты). В системе производится оценка корректности данных (сложилась ли банкнота из предъявленной и имеющейся половинок).

Проиллюстрируем свойства и различия таких данных таблицей 2.1.

Таблица 2.1. Свойства сравниваемых и проверяемых аутентифицирующих данных

	Сравниваемые	Проверяемые
Хранение аутентифицирующих данных на стороне объекта	да	нет
Что требуется для успешной аутентификации	совпадение	корректность
Контрольная процедура	сравнение	проверка
Предъявляемые данные и данные, используемые контрольной процедурой	одинаковые	разные
Зависимость от объекта аутентификации	прямая	косвенная
Примеры в аналоговом мире	Пароль, проверка собственноручной подписи	Узнавание по наличию подходящей ответной части (разделенный на части предмет, ключ от замка, способность вынуть меч из камня)
Примеры в информационном взаимодействии, в котором субъект – человек	Пароль, PIN- и PUK-код	Атрибутные сертификаты, криптографические ключи в процедуре «рукопожатия»
Примеры в информационном взаимодействии, в котором субъект – техническое средство или процесс	Имя компьютера	Контрольные суммы

Связанность с субъектом аутентификации

Охарактеризовать связанность аутентифицирующих данных с субъектом аутентификации можно по признаку ***отделимости*** от него.

Данные или присущи, имманентны субъекту – и тогда они от него неотделимы, или ассоциированы с ним (упрощенно можно сказать, что они ему выданы, назначены). Ассоциированные данные от субъекта отделимы. Примеры аутентифицирующих данных этого типа визуализированы на рисунке 2.6 и 2.7.

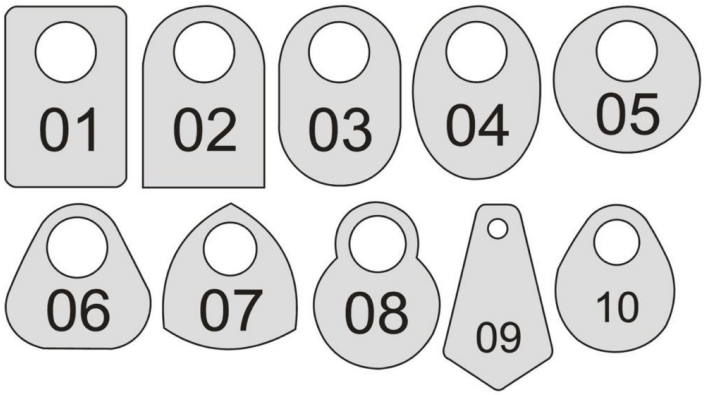


Рис. 2.6. Номерки в гардеробе не имеют никакого отношения ни к человеку, ни к его одежде, однако обеспечивают некоторую вероятность получить свою одежду назад.

Рис. 2.7. Комикс о том, что пароль должен быть сложным для подбора компьютером, а не для запоминания человеком (хотя как правило получается наоборот) с сайта https://xkcd.com/.

Не следует смешивать понятия неотделимости и неотчуждаемости. Неотчуждаемость – характеристика, означающая, что тот или иной объект нельзя штатными средствами извлечь из чего-либо (например, ключ из носителя) и, например, скопировать. С неотделимостью дело обстоит иначе – доминантой является не невозможность *доступа* к той или иной сущности и манипуляций с нею (аутентифицирующие данные должны быть непременно доступны для предъявления!), а скорее то, что субъект является целым, штатно функционирующим, или, проще говоря – является самим собой – только тогда, когда этот признак при нем, не отделен от него. Строго говоря, такие данные как папиллярный узор (или иная биометрия) являются в такой же степени условно

неотделимыми от субъекта, как условно некопируемым является аппаратный идентификатор. При желании и настойчивости от человека можно многое отделить – но он определенно потеряет свою целостность и будет уже не тем, что прежде. Ассоциированные же данные можно отделить от человека вполне безболезненно (прошу прощения за неуместный каламбур).

Определенная сложность с признаком неотделимости данных заключается в том, что этот признак может характеризовать только те данные, которые *в непреобразованном виде* в систему (и подсистему аутентификации, в частности) передаваться *не могут*. От чего бы неотделимыми ни были эти данные (от человека ли, от устройства ли), они неотделимы от чего-то, что находится за *рамками* системы, значит в систему *никогда не попадают*. Однако это влияет только на описание процесса порождения данных и не создает никакой проблемы для их классификации.

В то же время сам по себе признак неотделимости данных очень важен, это очевидно хотя бы по иррациональному доверию людей к биометрии. На рисунке 2.7 в качестве примера приведено изображение глаза человека. Радужная оболочка глаза – это неотделимый от человека признак.

Рис. 2.7. Глаз человека

Необходимо ответить только на один существенный вопрос – отделимость/неотделимость *от чего* мы будем считать классифицирующим признаком. Неотделимость биологических характеристик от человека – это одно, а неотделимость, допустим,

ключа от носителя – это несколько иное, хотя бы потому, что носитель от человека вполне легко отделяется.

Ответ получается довольно очевидным – мы характеризуем зависимость от *субъекта аутентификации*, стало быть отделимость или неотделимость мы должны установить именно от него. Если субъект аутентификации (напомню, это тот, кто аутентифицируется) – человек, то нас интересует отделимость от него, если аутентифицируется носитель каких-то данных или любое другое устройство (или программа) – то отделимость от носителя/устройства/программы соответственно.

Проиллюстрируем свойства и различия ассоциированных и неотделимых данных таблицей 2.2.

Таблица 2.2. Свойства ассоциированных и неотделимых аутентифицирующих данных

	Ассоциированные	Неотделимые
Связь с субъектом	нет	есть
Возможность передачи другому субъекту	+	-
Возможность утраты	+	- (с оговорками, которые в данном контексте значения не имеют)
Возможность замены в случае компрометации	+	-
Примеры в аналоговом мире	Номерок в гардеробе, билет на концерт, ключ от замка, разделенный на части предмет	Особые приметы, способность вынуть меч из камня
Примеры в информационном взаимодействии, где субъект – человек	Пароль, PIN- и PUK-код, аппаратный идентификатор, сертификат ключа подписи	Биометрические характеристики различного рода
Примеры в информационном взаимодействии, где субъект техническое средство или процесс	Имя компьютера, Электронная подпись	Серийный номер устройства, фрагмент кода программы

Второй важный признак аутентифицирующих данных – их ***тиражируемость***. На первый взгляд этот признак близок к ассоциированности/неотделимости до полного смешения – операция копирования является базовой в цифровой среде, значит, любые данные, попадающие в цифровую среду, могут быть скопированы сколько угодно раз.

Разумеется, такой подход непродуктивен. Тиражируемостью предлагается называть возможность параллельного использования данных разными субъектами или разными объектами аутентификации.

Тиражируемость между субъектами аутентификации

Так, аппаратный идентификатор мы условно считаем некопируемым, то есть одновременно он может находиться только у одного пользователя. Поэтому, хотя он может быть передан легальным субъектом постороннему лицу, он все же является ***нетиражируемым***, так как одновременно им может воспользоваться один субъект.

Пароль же может быть назначен любому числу субъектов (именно так обычно происходит с паролями user, student, admin и аналогичными) – поэтому он ***тиражируемый***.

Эти примеры иллюстрируют тиражируемость данных с точки зрения субъектов аутентификации: возможность использования данных разными субъектами в одно время.

Тиражируемость между объектами аутентификации

С точки зрения объекта аутентификации фактор тиражируемости аутентифицирующих данных тоже может быть значимым. И сводиться он будет, по всей видимости, к тому, в одном или нескольких объектах аутентификации этому субъекту сопоставлены эти данные.

Сразу приходит в голову старое, как мир, но бесконечно нарушаемое правило – не регистрировать в разных ресурсах один и тот же пароль. Однако, когда в разных ресурсах регистрируется одно и то же лицо (в прямом физическом смысле – face), принципиально – это то же самое. Причем ситуация даже хуже, чем с паролем – пароль поменять существенно легче, чем лицо.

Заметим, что ***тиражируемыми*** между объектами аутентификации могут быть данные, нетиражируемые между субъектами, и даже неотделимые от субъекта аутентификации. Надо заметить, что тиражируемые данные – это данные, которые *могут быть* растиражированы, а не обязательно заведомо растиражированные. Но как безопасники, мы, конечно, должны исходить из того, что то, что может быть растиражировано, будет растиражировано, если это хоть кому-нибудь нужно. Значит, для всех тиражируемых данных в системах должны приниматься какие-то меры, препятствующие их тиражированию.

Нетиражируемыми между объектами аутентификации могут быть, по-видимому, только динамические аутентифицирующие данные. В отношении любых статических данных должны применяться какие-то механизмы, ограничивающие возможность использования одних и тех же данных в разных системах. Так, ограничивая пользователя в праве зарегистрировать в той или иной системе свой личный идентификатор (или идентификатор из другой системы) – мы создаем ему определенные неудобства, но несколько снижаем вероятность компрометации аутентифицирующих данных. Но насколько это существенное снижение – нужно анализировать на основании Моделей угроз и нарушителя.

Может ли пользователь зарегистрироваться со своим идентификатором и паролем, или только получить специальные идентификатор и пароль именно для этой системы, будет зависеть от реализации системы аутентификации.

От реализации системы аутентификации будет зависеть еще много параметров. Например, постоянными или временными будут данные, ассоциированные с субъектом:

- система может использовать заводской номер идентификатора (он постоянный) или вычисление от каких-либо данных, записанное в память идентификатора, или даже им осуществляемое (и это будут временные данные);

- система может требовать или не требовать смены пароля по регламенту.

Однако разделение этих данных на «аппаратный идентификатор» и «пароль» все равно справедливо находится на уровень выше.

2.3.2. Субъектно-объектная классификация аутентифицирующих данных

Итак, получается, что по отношению к объекту аутентификации данные могут быть

1) сравниваемые / функционально проверяемые,
2) тиражирумые между объектами / нетиражируемые между объектами.

Наложением этих признаков, получаем следующие варианты пересечений:

1) сравниваемые тиражируемые,
2) проверяемые тиражируемые,
3) сравниваемые нетиражируемые,
4) проверяемые нетиражируемые.

Довольно очевидно, что «проверяемых тиражируемых между объектами» данных быть не может, так как если в системе не хранятся данные (проверяемые данные – значит, в системе хранится функция для проверки, а не сами данные), то они и не могут быть растиражированы между системами. Система не растиражирует данные, которых у нее нет.

Остальные классы не пустые, для них находятся примеры:

1) пароль,
2) -
3) одноразовый пароль, талончик в очереди[19],

[19] Очевидно, что система не хранит список номеров талончиков, из которых выдает по одному, а формирует номера по порядку с учетом каких-то дополнительных входных данных (например, за какой госуслугой пришел в МФЦ посетитель, или к какому врачу); также очевидно, что талончик не связан с субъектом, а ему назначается; о зависимости от носителя тут тоже говорить некорректно, так как то, что на талончике напечатано, от носителя не зависит, оно полностью формируется

4) атрибутный сертификат, интерактивная биометрия.

По отношению к субъекту аутентификации получаются следующие пары признаков:

1) ассоциированные / неотделимые,
2) тиражируемые между субъектами / нетиражируемые между субъектами.

Наложением признаков получаем следующие классы:

1) ассоциированные тиражируемые,
2) неотделимые тиражируемые,
3) ассоциированные нетиражируемые,
4) неотделимые нетиражируемые.

Проверим на предмет пустых классов:

1) пароль, имя компьютера;
2) биологические признаки, свойственные классу субъектов (такие как возраст, пол, цвет глаз или волос), ФИО, фрагмент кода программы;
3) аппаратные идентификаторы,
4) личные биометрические данные (как статические, так и динамические).

Здесь стоит лишний раз оговориться, что мы определяем аутентифицирующие данные, а не реализацию подсистем, поэтому

системой. Можно возразить, что такой же номерок, но напечатанный на чем-то другом, не будет принят как подтверждение очереди, однако тут опять же связь с системой, а не с носителем, ибо талончики именно в таком как есть виде целиком выпускаются системой, можно сказать, являются ее продуктом. При этом доступ дается на основании сравнения данных талончика с номером, который высветился над соответствующим окошком. Суммируя все это, можно утверждать, что это ни что иное, как вариант реализации одноразового пароля. Важной особенностью этого случая является то, что подтвердить с помощью таких аутентифицирующих данных субъект может только одно – «бронирование» права на взаимодействие с системой.

возможность кражи данных *после предъявления их в систему* к тиражированию не относим.

Представить себе данные, которые были бы неотделимы от субъекта, но в то же время тиражируемы между субъектами – на первый взгляд, довольно сложно, и ситуация с этим классом кажется аналогичной «проверяемым тиражируемым». Но через субъект – техническое средство или программу – это сделать возможно. Фрагмент кода программы является от нее явно неотделимым, без него, если его отделить – программа станет другой. Однако тот же кусок кода может встречаться в других программах, и тоже являться их неотъемлемой частью. Имя человека ему имманентно, но как правило, есть еще довольно много людей с таким же самым.

Любопытно, что с именем компьютера дело обстоит иначе, чем с именем человека – человеку имя назначается раз и навсегда (кроме исключительных случаев), компьютер же может быть переименован сколь угодно часто, поэтому имя компьютера целесообразно считать ассоциированным, а не неотделимым признаком.

Это рассуждение делает довольно очевидным, что использовать такие данные как аутентифицирующие целесообразно только тогда, когда требуется аутентификация на уровне отношения субъекта к некоторому классу. В аналоговом мире такая задача иногда встречается (проход в женскую раздевалку (женский пол) или на аттракцион (рост не менее 120 см) и тому подобные), но в области технической защиты информации это маловероятно[20].

В целом формулирование этих свойств и сопоставление им фактически используемых на практике аутентифицирующих данных позволяет лучше понять, в каких случаях какие данные адекватны целям аутентификации, и принятия каких защитных мер требует применение именно их в той или иной системе. Например, если Модели угроз и нарушителя допускают, что субъект аутентификации может быть недобросовестным (например, в сговоре с нарушителем, или просто

[20] Об эквивалентности задач аутентификации и классификации (установлении соответствия 1 к 1 или принадлежности к классу) см. специально посвященный этому раздел в [7. С. 282–287].

неблагонадежным в плане дисциплины), то использование для аутентификации данных, ассоциированных с субъектом, а в еще большей степени – тиражируемых между субъектами, должно сопровождаться комплексом мер, каким-то образом снижающих риск передачи другим лицам и/или тиражирования аутентифицирующих данных. Особенно это касается аутентификации при доступе к учитываемым или просто платным услугам – здесь передача и/или тиражирование открывает возможности личной наживы, что может быть сильным стимулом для нарушения политики безопасности.

Ассоциированные с субъектом аутентификации и тиражируемые между субъектами аутентификации данные должны считаться потенциально скомпрометированными во всех случаях, если субъект аутентификации признается потенциальным злоумышленником.

Разница между ассоциированными нетиражируемыми и тиражируемыми заключается только в том, что о компрометации тиражируемых данных субъект данных может и не знать. То есть строго говоря, ассоциированные данные следует считать потенциально скомпрометированными в любом случае.

Что же касается возможности тиражирования между объектами аутентификации – если важно, чтобы аутентифицирующие данные, использующиеся в той или иной системе, не использовались в других системах, то необходимо либо использовать данные, не тиражируемые между объектами аутентификации, либо разрабатывать какие-либо защитные меры, препятствующие тиражированию.

И наоборот, если субъект аутентификации имеет основания предполагать, что объект аутентификации передает аутентифицирующие данные в смежные системы или просто не чист на руку и, например, продает их, то ему целесообразно избегать предоставления таких данных, которые система может тиражировать. Хотя, надо признать, пользователь не всегда может влиять на то, какие данные предоставлять, если взаимодействовать с системой он вынужден в любом случае.

Тиражируемые между объектами аутентификации аутентифицирующие данные, которые мы предоставляем системе, следует считать уже потенциально скомпрометированными.

Классификация

Одновременно данные характеризуются какой-то зависимостью и от субъекта, и от объекта. Это можно визуализировать в виде таблицы (таблица 2.3) и попробовать сопоставить получившимся ячейкам фактически использующиеся данные. Так станет очевидно, каких классов быть не может, а далее будет возможно проанализировать, какие данные использовать решительно нецелесообразно.

Необходимо оговориться, что по данным, передаваемым объекту аутентификации как таковым, в отрыве от каких-либо сопутствующих условий или обстоятельств, определить, какого они типа – не представляется возможным. Как принято говорить – «это просто нули и единицы». Различия проступают наглядно тогда, когда мы смотрим на систему на уровне «аутентификаторов»[21] или сценариев использования данных. Поэтому выделенные типы аутентифицирующих данных ниже иллюстрируются именно через эти два проявления: аутентификаторы и сценарии использования. Предпосылкой, делающей возможным такое сведение друг к другу разных понятий, является их детерминированность. Одному типу данных может соответствовать (и, как правило, соответствует) несколько типов аутентификаторов и сценариев аутентификации, но не наоборот. Аутентификаторы и сценарии использования не могут работать сразу с разными типами аутентифицирующих данных.

---

[21] «Аутентификатор» – это понятие в русскоязычной практике терминологически не оформленное, и здесь хотелось бы воздержаться от его определения, ограничившись ссылкой на англоязычную Википедию [11]. Нестрого «аутентификатор» можно определить как инструмент аутентификации (то, с помощью чего субъект передает свои аутентифицирующие данные).

Таблица 2.3. Пересечение классов аутентифицирующих данных по отношению к объекту и к субъекту аутентификации: примеры данных

		Сравниваемые тиражируемые между О	Сравниваемые не тиражируемые между О	Проверяемые не тиражируемые между О
Ассоциированные тиражируемые между S	человек	Пароль, контрольные вопросы	Одноразовый пароль, талончик в очереди, гостевая карта СКУД	нет
	техническое средство	Имя файла, компьютера, пр.	лицензионный ключ на ПО, зависящий от данных лицензируемого ПО и системы, для которой оно лицензируется	нет
Ассоциированные не тиражируемые между S	человек	Аппаратный идентификатор, номерок в гардеробе,	токен аутентификации (Token-Based Authentication)	Атрибутный сертификат, ЭП, OTP (устройство, генерирующее одноразовые пароли)
	техническое средство	Серийный номер наложенного СЗИ (при условии, что S аутентификации является не СЗИ, а СВТ)	лицензионный ключ на ПО, зависящий от данных лицензируемого ПО и СВТ в рамках этой системы	Криптографическое рукопожатие
Неотделимые тиражируемые	человек	ФИО, биологические параметры, характеризующие класс, а не индивидуума (цвет кожи, рост, вес, пр.)	нет	нет
	Техн. средство	Фрагмент кода программы, сигнатура	нет	нет
Неотделимые не тиражируемые	человек	Статические биометрические данные	нет	Динамическая (интерактивная) биометрия
	техническое средство	заводской серийный номер устройства (того, которое является S аут-ции, или неотделимого от него), контрольные суммы	нет	ЭП поставщика

Необходимо оговорить ячейки, в которых стоят «нет».

Так, неотделимые от субъекта и в то же время тиражируемые между субъектами данные могут быть только сравниваемыми с эталоном и тиражируемыми между объектами аутентификации. Это логично, так как это самый простой в реализации системы тип связи аутентифицирующих данных и объекта аутентификации, и просто не имеет никакого смысла реализовывать более сложные варианты для использования данных, позволяющих аутентифицировать не конкретного субъекта, а лишь класс, к которому он относится. Трудно придумать какую-то конструктивную цель такой аутентификации в информационной системе, поэтому данные этого типа предлагается считать нецелесообразными к применению в защите информации.

Ассоциированные с субъектом тиражируемые между субъектами данные, как выше уже упоминалось, логично в любом случае считать потенциально скомпрометированными, поэтому строить более сложную систему их проверки (функциональная проверка – более сложная, чем простое сравнение) – явно нецелесообразно.

Если данные неотделимы от субъекта, но их эталоны для прямого сравнения хранятся в системе, нет никаких причин к тому, чтобы их было невозможно поместить и в другую систему, поэтому примеров неотделимых от субъекта сравниваемых и нетиражируемых между объектами данных – нет.

Обращает на себя внимание тот факт, что все ячейки заполнены только в строке ассоциированных с субъектом нетиражируемых между субъектами данных. Именно этот тип аутентифицирующих данных фактически наиболее популярен, так как в условиях защищенной корпоративной системы позволяет без значительных сложностей реализовать подсистему аутентификации, соответствующую всем распространенным моделям угроз.

И второе наблюдение, которое можно почерпнуть из полученной таблицы – единственный тип данных, которые нет причин заранее считать потенциально скомпрометированными без применения дополнительных защитных мер – это неотделимые от субъекта нетиражируемые между субъектами данные, функционально

проверяемые объектом аутентификации. Для аутентификации пользователя (человека) – это динамические биометрические данные.

Примера данных, которые бы не попадали ни в одну из получившихся категорий, пока не обнаружено, что, безусловно не говорит само по себе о том, что классификация верна, однако усиливает ее правдоподобность.

Классы данных расположены по возрастанию сложности нелегального получения данных этих классов в свое распоряжение.

В то же время нельзя не заметить, что так же возрастает и сложность реализации подсистемы идентификации\аутентификации, использующей данные разных типов.

Однако рост сложности реализации в некотором смысле компенсируется тем, что снижаются требования к обеспечению доверия тем или иным компонентам системы, которые могут в разных случаях быть легче или сложнее доступны для контроля. Иногда проще сделать доверенным клиентское устройство, а иногда – использовать намного более сложную систему аутентификации, но не контролировать клиентские устройства совсем. Очевидно, что в условиях, когда взаимодействие с системой производится с произвольных устройств – такие системы называются открытыми – контроль этих клиентских устройств обеспечить невозможно, а значит, в них должны использоваться проверяемые имманентные аутентифицирующие данные. Ниже рассмотрим это утверждение в отдельном разделе главы, поскольку оно крайне важное.

Понимание того, контроль какого компонента должен быть усилен, а какого – может быть ослаблен, тоже можно получить как следствие из предложенной классификации.

Это означает, что приведенная классификация аутентифицирущих данных обладает определенной продуктивностью, то есть целесообразна.

На этом пока можно остановиться и рассмотреть другие важные аспекты, связанные с идентификацией/аутентификацией. В частности, кто и как «принимает решения».

2.4. Механизмы принятия решения о результатах аутентификации

Одной из проблем, в основном, психологического толка, связанных с отказом от «факторов», является устоявшееся представление о том, что аутентификация тем лучше, чем более она «многофакторная».

Однако при ближайшем рассмотрении становится очевидно, что на «качество» аутентификации (насколько она «хорошая»[22]) влияет не то, *сколько типов* данных представлено в подтверждение связи субъекта аутентификации с его идентификатором, а то, *как* они представлены в систему. Именно то, как данные представляются в систему, определяет число ошибок первого и второго типа при фактическом функционировании системы, а не на математической модели механизма.

Рассмотрим на примерах.

«Многофакторность» возникает обычно в описании системы вместе с «аппаратным идентификатором».

Возьмем классический вариант — ТМ-идентификатор. Его использование основано на том, что у него есть память, и туда можно записать различные данные. И чем ТМ-идентификатор будет являться — идентификатором или аутентификатором — зависит от реализованного порядка его использования в системе.

Например, можно сделать так:

---

[22] Вообще говоря, для оценки аутентификации как «хорошей» или «плохой» нет принятого термина. Принято говорить о «надежной» аутентификации, но это употребление слова «надежность» ясно нарушает его терминологический смысл в технической сфере. Надежный – это работающий без отказов (с минимумом отказов). Очевидно, что это совершенно не то, что определяет качество выполнения целевой функции аутентификации, хотя и важно. Можно было бы предположить, что в области защиты информации свойству надежности приписывается другое значение, но согласно, например, ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [20], определение совершенно обычное: «свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования».

- в память устройства записать уникальный идентификатор,
- раздать пользователям,
- составить табличку вида {ФИО сотрудника; идентификатор},
- и потом потребовать, чтобы при входе в систему они предъявляли «таблетку».

Если хранящийся в ней номер (или даже — в простейшем случае — собственный ID ТМ-идентификатора) зарегистрирован в системе, то пользователю доступ разрешается, если нет — то нет. В этом случае есть только идентификация, а никакой аутентификации (тем более — двухфакторной) нет и в помине, хотя налицо «предмет», которым «владеет» пользователь. Фактор есть, а аутентификации нет.

Другая ситуация — если в ТМ-идентификатор записывать набор данных, связанный с именем пользователя, зарегистрированного в системе, а потом требовать ввода имени пользователя с последующим прикладыванием зарегистрированной «таблетки». В этом случае «таблетка» будет являться «фактором» аутентификации (двухфакторной, если помимо этого вводить пароль с клавиатуры или что-нибудь еще по еще какому-либо отдельному каналу, а в противном случае — однофакторной, несмотря на «владеть», которое зачастую вызывает ложную уверенность, что факторов уже в любом случае два).

Это только две из существенно большего количества совершенно разных схем с использованием устройства, которое называется «идентификатор», причем схем, крайне похожих «внешне» — по сценарию работы пользователя.

Действительно, из разобранных случаев наиболее защищенным при прочих равных является вариант с вводом идентификатора с клавиатуры, потом аутентифицирующих данных с ТМ-идентификатора и пароля с клавиатуры.

Но это усиление производится за счет того, что аутентифицирующие данные поступают по разным каналам, а не за счет того, что они имеют разные источники. Выше я просила взять на заметку связь между аутентифицирующими данными и интерфейсом их представления в ИС: невозможно передать голос через сканер

отпечатка пальцев, а ТМ-идентификатор бесполезно прислонять к микрофону. Именно (а часто и только) в этом смысле использование набора из разнообразных аутентифицирующих данных усиливает защищенность.

Количество каналов важно потому, что для компрометации данных, поступающих по разным каналам, требуется более сложная атака.

Если мы используем один канал, то для поддержания того же уровня доверия к технологии, он должен быть защищен существенно более надежно. Для поддержания непривлекательной для злоумышленника трудоемкости атаки мы либо более тщательно защищаем меньшее количество каналов, либо диверсифицируем точки приложения потенциальных усилий злоумышленника – используем независимые каналы.

Однако эта логика имеет определенное ограничение – она работает только в том случае, если процесс аутентификации будут атаковать *именно на этапе передачи данных в систему*.

Так ли это будет – зависит от того, как именно реализована подсистема идентификации/аутентификации.

Обобщенно процесс аутентификации выглядит всегда одинаково:
субъект аутентификации
- передает аутентифицирующие данные,
объект аутентификации
- получает предъявленные данные,
- проверяет полученные данные,
- передает результат проверки туда, куда предусмотрено инфраструктурой объекта доступа.

Визуализировать этот процесс, чтобы ясно увидеть возможные направления атак злоумышленника можно так, как на рис. 2.8.

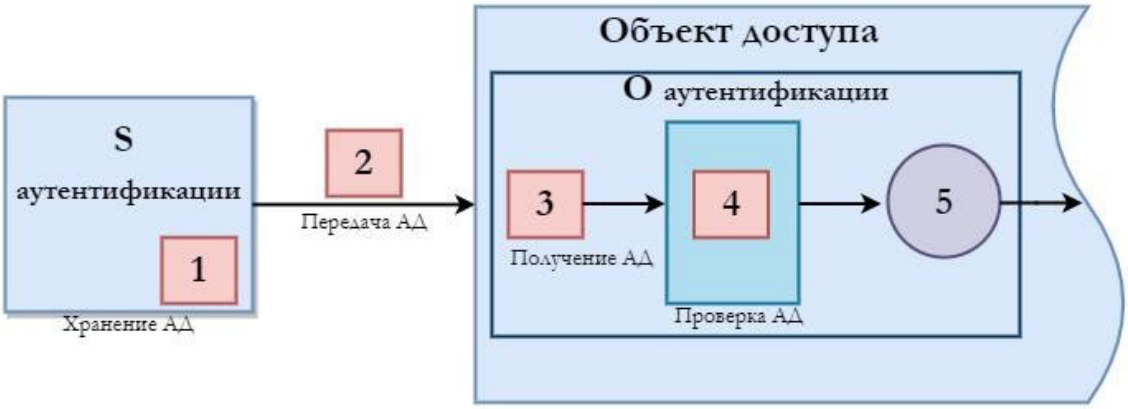


Рис. 2.8. На что могут быть направлены атаки злоумышленника. Цифрами 1–4 обозначены процессы, в рамках которых могут быть атакованы аутентифицирующие данные (АД). 1 – при хранении у субъекта аутентификации, 2 – при передаче объекту аутентификации, 3 – при получении объектом аутентификации, 4 – при проверке аутентифицирующих данных объектом аутентификации. Цифрой 5 обозначен результат аутентификации, который представляет собой выходные данные процесса проверки и передается в блок авторизации или куда-либо еще, в зависимости от особенностей реализации объекта доступа.

С точки зрения злоумышленника идеально (по эффективности) атаковать возвращаемый результат. Если есть возможность всегда, когда надо злоумышленнику, передавать результат «да», то нет никакого смысла ни перехватывать данные пользователей, ни подсовывать фальшивые эталоны или подменять механизмы проверки. По сути, ничего другого делать не надо. Передача результата «аутентифицировано» – это цель злоумышленника, и этого достаточно.

Более того, успешная атака на аутентифицирующие данные даст злоумышленнику возможность аутентифицироваться только как один определенный пользователь, а успешная атака на данные о результате аутентификации – даст ему возможность аутентифицироваться как любой из пользователей системы.

Атаковать для этого можно «верификатор» (тот механизм, который вырабатывает решение о результате проверки предъявленных данных), или канал передачи ответа верификатора дальше, то есть канал между подсистемами аутентификации и авторизации. Поэтому в действительно защищенных системах решение о результате

аутентификации принимается в доверенной вычислительной среде и передается средству авторизации, находящемуся либо в этой же доверенной среде, либо по защищенному каналу, либо в защищенном виде.

Например, в СДЗ уровня платы расширения «Аккорд-АМДЗ» процедура сравнения предъявленных данных с эталоном производится механизмами ПО СДЗ, которое исполняется в среде, независимой от вычислительной среды того компьютера, который защищен этим СДЗ. Авторизация в рамках этих функций заключается в том, что аутентифицированному пользователю либо разрешается продолжить загрузку ОС компьютера (если он пользователь СДЗ), либо разрешается войти в среду администрирования СДЗ (если он администратор СДЗ).

В этих условиях для обхода подсистемы аутентификации нужно либо подменить эталон, либо завладеть легальными аутентифицирующими данными.

Как именно осуществить атаку с целью подмены эталона, зависит от того, как реализована работа с ним в каждом конкретном случае. В общем случае есть некоторая база эталонов аутентифицирующих данных, связанных с идентификаторами. По идентификатору производится выбор нужного эталона, и он сравнивается с фактическими данными.

Разница обусловлена тем, где находится база по отношению к «верификатору». Если это не единый инструмент, и верификатор получает эталон «снаружи», то влияние на результат оказывает канал передачи эталона. Если злоумышленник может передать нужный эталон, он может получить нужный результат аутентификации.

В СДЗ «Аккорд-АМДЗ» база пользователей находится внутри устройства, поэтому передать другой эталон нельзя. Если база находится на жестком диске компьютера или на ином устройстве, то защищенность базы и защищенность канала – должны быть обеспечены и доказаны.

Другой случай – когда субъект аутентификации – не человек, рассмотрим на примере взаимной аутентификации Секретов из комплекса «Секрет фирмы». При подключении к компьютеру в своей сети «Секрет» пользователя инициирует процедуру

«криптографического рукопожатия» с Секретом сервера аутентификации (СНСА – Служебный Носитель Сервера Аутентификации). Ключи, с использованием которых производится рукопожатие, хранятся в «Секретах», вычисления производятся внутри «Секретов», не попадая в оперативную память компьютеров. Ни подменить ключи, ни завладеть легальными – невозможно.

Заметим, что аутентификация пользователей относительно «Секретов» тоже производится. Пользователь вводит свой ПИН-код, который проверяется процессором «Секрета». Этот ПИН-код записывается в память «Секрета» при регистрации пользователя. Для доступа к перезаписи ПИН-кода в «Секрете» надо ввести ПИН- или PUK-код, причем сделать это на легальном компьютере (на нелегальном до аутентификации пользователя дело не дойдет). Значит, подменить эталон нельзя, подобрать перебором правильный – нельзя благодаря защите от перебора (длинна ПИН-кода, блокировка после установленного количества неверных вводов). Получается, что единственный вектор атаки здесь как раз на передачу правильного ПИН-кода («подслушивание»). В то же время, аутентификация по нескольким каналам здесь все-таки не используется, поскольку аутентификация пользователя возможна только на разрешенных компьютерах, то есть предполагается, что на этих компьютерах в общем случае не может оказаться установлено средств перехвата паролей[23].

Тут представляется полезным привести для сравнения контурное описание того, как аутентификация пользователя бывает реализована в других «защищенных флешках». Например, флешках с доступом «по пальцу», или по паролю. «Палец» или пароль – совершенно не важно, и сейчас станет понятно, почему.

Распространено ошибочное убеждение, что отпечаток пальца «подобрать» сложнее, чем PIN-код. Но даже если бы это было так, стоило бы задуматься о том, как может быть реализована

[23] Возможность такую исключать совсем, разумеется, нельзя, однако, аутентификация пользователя – факультативный защитный механизм в «Секрете», ведь поскольку злоумышленник не может применить «Секрет» за пределами легальной информационной системы, мало вероятно, что завладение ПИН-кодом для него вообще целесообразно, он не станет тратить на это силы.

биометрическая аутентификация в обычной флешке. Предельно ясно, что эталон хранится на самой же флешке (флешке больше негде его хранить), а сравнение производится в оперативной памяти ПК (так как у флешки нет своих вычислительных ресурсов). То есть флешка передает эталон в оперативную память и получает оттуда ответ – да или нет.

Все следствия очевидны:

1. у системы есть доступ к эталону (можно его заменить на любой),
2. решение «сошлось» принимается в оперативной памяти компьютера (можно передать флешке любое нужное решение).

При этом флешка не различает компьютеры, и все это злоумышленник может проделывать на собственном компьютере, оборудованном всеми необходимыми ему инструментами. Это значит, что злоумышленник сможет открыть флешку, вне зависимости от того, что она запрашивает – пароль или отпечаток пальца.

Обратим внимание, что механизм верификации аутентифицирующих данных «один к одному» – это тоже сравнение с базой, но просто с такой, в которой есть только одна запись. Речь идет о механизме, например, такого рода: на аппаратный идентификатор (смарт-карта, ТМ-идентификатор) записан эталон аутентифицирующих данных (отпечаток пальца, пин-код и т. д.). Пользователь аутентифицируется относительно своего аппаратного идентификатора (производится сравнение предъявленных им данных с теми, что записаны в идентификатор) и при совпадении производятся определенные действия – например, идентификатор передает какие-то другие данные в систему. В системе при этом и/а производится уже без учета тех данных, что обеспечили аутентификацию в устройстве (см. рис. 2.9).

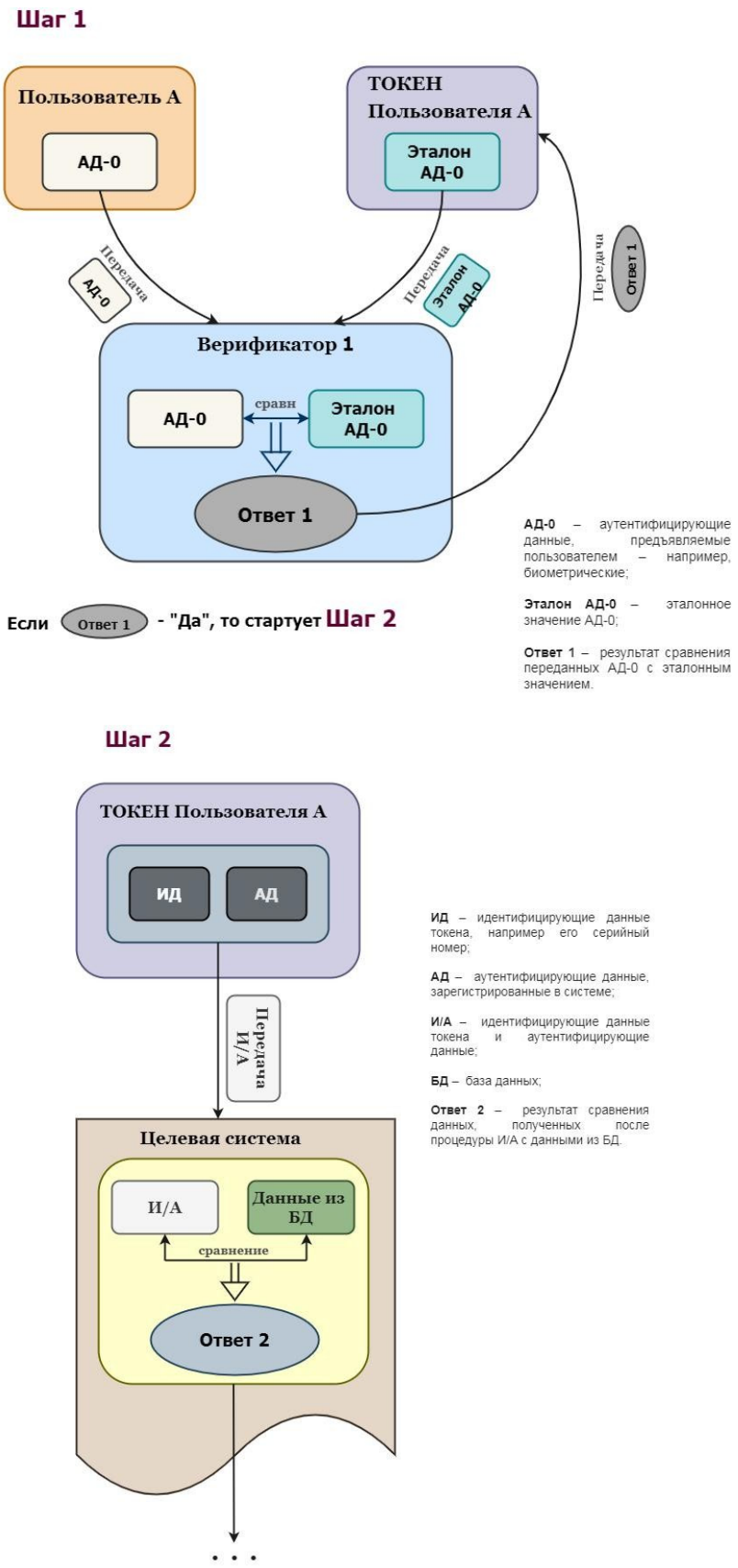


Рис. 2.9. Ход процесса аутентификации по биометрическому признаку с хранением эталона на персональном устройстве пользователя

Это может быть полезно как раз потому, что база эталонов должна быть защищена от несанкционированных изменений, и передача эталонов из базы в незащищенную среду крайне нежелательна.

А чем эта база меньше по объему, тем проще обеспечить необходимый уровень ее защищенности. Значит, базу желательно иметь маленького объема.

А эталоны, например, биометрических данных имеют довольно ощутимый объем (даже статических, а динамических – и того более). Защитить очень надежно можно и базу большого объема, но несравнимо бóльшими ресурсами. В описанном же примере база биометрических эталонов не создается. Один эталон поместится в память большинства устройств, использующихся как аппаратные идентификаторы. А нигде за пределами аутентификации пользователя относительно собственного идентификатора этот эталон не используется. В базе целевой системы (пускай это будет то же СДЗ «Аккорд-АМДЗ») хранятся эталоны данных, передаваемых идентификаторами (они обычно небольшие, фиксированного объема, так как представляют собой хеш от чего-либо).

Таким образом то, что для пользователя выглядит как единая процедура аутентификации, представляет собой цепочку процедур (это хорошо видно на рис. 2.9), и то, какие данные в конечном итоге аутентифицируют его при загрузке, например, ОС – пользователь зачастую себе плохо представляет, с его точки зрения он аутентифицировался «пальцем».

В этом смысле необходимо понимать, что использование статических биометрических признаков в и/а не ведет к повышению защищенности системы, оно имеет целью только повышение удобства ее эксплуатации. А это значит, при введении таких механизмов нужно оценивать, какие уязвимости они привносят, и эти уязвимости блокировать.

Разберем это на примерах ниже, а пока продолжим рассматривать, в каком же случае злоумышленник может атаковать именно процедуру

получения системой аутентифицирующих данных. Это имеет смысл, если планируемые действия – получить корректные данные и затем предъявить их. Это возможное, но не единственно возможное, как показано выше, направление. И только против атак такого рода может помочь предъявление аутентифицирующих данных нескольких типов.

Однако эти данные должны различаться не по источнику (знание, обладание и прочее), а по *каналу их передачи в систему*. Если в одном блоке, подключаемом, допустим, к USB-порту, находится, например, клавиатура для ввода пин-кода и считыватель для отпечатка пальцев, то несмотря на то, что отпечаток пальца – биологический признак, а пин-код – знание, передаваться они будут в систему по одному каналу, и атака на этот комплект данных не сложнее, чем если бы вводилось что-то одно (ниже еще проиллюстрируем это в рамках обещанных примеров с биометрией).

Если используется единственный канал, он должен быть лучше защищен от компрометации, или процедура должна быть организована так, чтобы не зависеть от канала, как, например, в разобранном выше примере взаимной аутентификации «Секретов». Перехватывать посылку от «Секрета» пользователя Служебному носителю СА, или от СНСА «Секрету» пользователя и пытаться использовать ее для аутентификации нелегального устройства – бессмысленно, так как в реализации алгоритма «рукопожатия» для защиты от имитации используются метки времени, а значит, данные, отправленные «из прошлого» не будут корректными.

Разберем положение о влиянии каналов передачи аутентификационных данных на реализацию процедуры аутентификации на примерах встраивания технологий работы со статическими биометрическими данными в системы защиты информации.

Главное, что объединяет встраивание в СЗИ любой биометрии – это необходимость наличия некоторого прибора, который соответствующий биометрический признак считывает. При этом данные разной природы, разумеется, считывают зачастую совершенно

разные приборы, и замена программного обеспечения вряд ли «научит» прибор, считывающий голос, считывать геометрию лица. Вместе с тем, с точки зрения принципа работы с данными, такие приборы можно объединить в три большие группы.

1. «все в одном» — в одном приборе объединены считыватель, верификатор, работа с эталоном;
2. «эталон передается снаружи» — прибор считывает биометрический параметр и верифицирует его с переданным в него эталоном;
3. «эталон в базе» — прибор считывает биометрический параметр и передает его в верификатор, функционирующий в ОС компьютера (или где-то еще снаружи от прибора – на удаленном сервере, внутри какого-то еще устройства, так или иначе, в какой-то внешней для прибора среде), для поиска соответствующего эталона в базе эталонов.

Все в одном

Выбирая ***первый из рассматриваемых вариантов*** («все в одном»), разработчик СЗИ должен понимать, что доверять можно данным, полученным только от идентифицированного и аутентифицированного прибора. Если злоумышленник подменит прибор, в котором содержится считыватель фактических данных, хранится эталон данных и который сам производит сравнение данных с эталоном, то он сможет получать можно любой желаемый результат.

Значит, должно быть точно установлено, что СЗИ взаимодействует именно с тем прибором, который был установлен администратором, причем взаимодействие осуществляется по доверенным каналам связи. Обеспечить выполнение этого условия можно либо организационными мерами, либо техническими. В простейшем случае необходимо провести идентификацию прибора и предусмотреть в протоколе его взаимодействия с СЗИ проверку этого идентификатора (например, серийного номера).

В этом варианте биометрический признак в общем случае не должен являться единственным, вводимым в систему пользователем (поскольку мы получим идентификацию и аутентификацию

пользователя не в системе, а в считывателе, а система получит только «да», которого недостаточно для дальнейшей авторизации). Исключениями будут:

1. системы, не предполагающие авторизации, то есть системы второй группы по классификации ФСТЭК России [21] — то есть такие, в которых пользователи характеризуются равными полномочиями, а задачи идентификации/аутентификации сводятся исключительно ко входу в систему, то есть в самой системе аутентифицирующие данные больше не понадобятся;

2. применение «интеллектуального» считывателя, в функции которого входит помимо считывания параметра и его верификации — также формирование некоего информационного набора, выполняющего в дальнейшем роль логического (а не физического) уникального идентификатора. В этом случае при дальнейшей авторизации этот информационный набор будет выполнять функцию аутентифицирующих данных.

Но и в перечисленных случаях необходимо отдавать себе отчет в том, что критичность канала «считыватель — СЗИ» (где под «СЗИ» понимается активная составляющая, принимающая решение) существенно возрастает по сравнению с ситуацией, когда по биометрии пользователь только аутентифицируется, а идентификатором пользователя является отдельный параметр, данные о котором поступают в СЗИ по другому, независимому каналу. Например, с того же ТМ-идентификатора.

Эталон передается снаружи

Во втором из рассматриваемых вариантов («эталон передается снаружи») помимо подмены прибора возможна и подмена эталона. То есть наряду с идентификацией прибора (она также актуальна, так как от прибора зависит корректность считывания и сравнения), СЗИ должно проводить проверку эталона и передавать в прибор для верификации только те эталоны, которые связаны именно с этим конкретным СЗИ и

для которых, возможно (опять же, в зависимости от модели угроз), подтверждена целостность.

Например, СЗИ передает свои собственные (хранимые им защищенно в своей базе) эталоны по доверенному каналу (предположим, прибор подключен прямо к плате СЗИ). Или эталон передается из ТМ-идентификатора или карточки пользователя, данные которой СЗИ проверяет на предмет легальности.

Поскольку на легальном носителе может оказаться подмененный эталон, СЗИ нужно проверять не просто ID карты или номер ТМ-идентификатора, но и информационный набор, связанный с содержимым памяти (например, подпись под эталоном).

Хотя объектов для контроля становится больше (что усложняет систему), есть и существенный плюс: реализация атаки на эти объекты становится менее привлекательной для злоумышленника, ведь атаковать их по отдельности становится менее эффективным.

Проблема диверсификации источников данных в этом варианте снимается автоматически, поскольку эталон поступает «снаружи», что и является независимым каналом.

Эталон, поступающий, например, из ТМ-идентификатора или из смарт-карты, является идентифицирующими данными, в отличие от аутентифицирующего предъявляемого параметра (самой руки, пальца, глаза).

Эталон в базе

Третий вариант, с эталоном в базе, наиболее распространен, но и наиболее сложен для интеграции с СЗИ, так как в нем больше сущностей, которые могут быть изменены, и соответственно, которые необходимо контролировать.

Наряду с идентификацией прибора необходимо контролировать целостность верификатора и целостность базы данных эталонов. Храниться в независимой памяти СЗИ база биометрических данных не может, так как они имеют большой объем (если это только не случай, когда база состоит из одного или буквально нескольких эталонов). Значит, эту базу потребуется размещать и защищать отдельно.

Также необходимо будет обеспечить защищенность доступа верификатора к базе данных.

А вот трудоемкость реализации атаки принципиального не вырастет, более того, при прочих равных атака на компонент, работающий в ОС — проще.

Эталон биометрического признака, хранящийся в базе, вполне может быть той самой уникальной информацией, которая пользователя идентифицирует. Однако этот вариант не очень приветствуется «безопасниками». Когда вместо «базы пользователей» используется «база идентификаторов», получается, что критичная информация хранится в открытом виде. В этом случае база становится ресурсом, атака на который крайне привлекательна и который, соответственно, нуждается в крайне строгой защите. Эта необходимость, заметим, в случае с биометрическими данными усиливается и требованиями нормативных документов.

Из изложенного хорошо понятно, что использование именно биометрических, а не каких-то иных данных никак не повышает защищенность системы. Повышается только удобство пользователя и управляющего персонала (и отчасти – удовольствие от процесса «как в кино»).

Более того, как выше уже упоминалось, риск дискредитации биологических данных существенно выше, так как их нельзя сменить при компрометации. Хуже того, скомпрометированное, например, изображение лица невозможно даже «отозвать», остается только дорогостоящая операция. Вопрос о том, действительно ли это адекватная цена за удобство «не выполнять лишних действий» для аутентификации, остается открытым.

Если с пользователем все ясно, то на удобстве управляющего персонала стоит в двух словах остановиться. Дело в том, что когда пользователь ввел неверный пароль больше разрешенного числа попыток ввода (а он обязательно это сделает, даже если установить число допустимых неверных вводов в 32, например), или просто забудет – случайно или нарочно – свой идентификатор, это становится проблемой управляющего персонала – администратора и администратора безопасности информации (АБИ). В значительном числе случаев просто отпустить пользователя с работы – нельзя. Приходится принимать различные меры, которые, даже если они заранее проработаны и не вызывают затруднений, негативно сказываются на продуктивности использования рабочего времени — уже не только АБИ, но и

пользователями. А в случае с недобросовестными пользователями возможен и осознанный саботаж. Именно в этом, собственно причина того факта, что по регламенту большинства организаций АБИ не могут просто сообщать пользователям PUK-коды для разблокировки их устройств и поручать разблокировать их самостоятельно, ведь в ходе «ошибок» при разблокировке можно заблокировать устройство безвозвратно и получить возможность для «вынужденного» безделья.

В качестве примера рассмотрим интеграцию биометрической аутентификации по сосудистому руслу ладони в ПАК «Аккорд».

Из описанных выше трех способов работы с данными был выбран второй — сравнение предъявленного пользователем рисунка сосудистого русла с предъявленным им же эталоном, который записан в персональный идентификатор пользователя (в зависимости от потребностей целевой информационной системы это может быть ТМ-идентификатор, токен, смарт-карта).

Пользователь подносит руку к сканеру и совмещает идентификатор со считывателем (прислоняет ТМ-идентификатор, подключает токен или устанавливает смарт-карту в считыватель). Из идентификатора система получает эталон, со сканера — биометрические данные, средством защиты производится верификация. Таким образом, идентификатором так и будет идентификатор, а аутентифицирующие данные – фактически предъявляемый пользователем на сканер рисунок вен.

Возможность компрометации этих данных – их подмена или считывание в канале между сканером и ПК. Реализация такой угрозы крайне маловероятна, так как для нее потребовалась бы атака с использованием не только глубоких и специфических знаний и навыков, но и сложной измерительной аппаратуры.

Перспективы, которые открывает применение описанной схемы, в первую очередь связаны с возможностью интеграции СЗИ НСД со СКУД (системами контроля и управления доступом). Если эталон биометрического признака будет записываться в карту СКУД, которая должна быть, в свою очередь, поддержана в СЗИ НСД в качестве идентификатора пользователя, то возможно логичное и целесообразное развитие системы безопасности, которое способно существенно повысить эффективность как СКУД, так и СЗИ НСД. Такую систему рассмотрим ниже – в 3 главе.

2.5. Авторизация

Отдельно, вплоть до вынесения в раздел, хочется остановиться на авторизации. Выше уже шла речь о том, что это отдельный процесс, который не следует путать или смешивать с идентификацией /аутентификацией, хотя зачастую они довольно тесно связаны.

Необходимо сразу заметить, так как это важно всегда держать в голове, что положительный результат аутентификации – это далеко не всегда гарантия авторизации именно с теми правами, на которые пользователь претендует.

Например, если легальный пользователь системы будет претендовать на работу вне рамок назначенного ему времени, или вне рамок своих полномочий, то успешная аутентификация ему ничем не поможет (или, если используется такая неудачная система защиты, которая уравнивает эти процессы, то аутентификация не поможет, наоборот, владельцу системы – легальные пользователи будут делать, что хотят, а не что должны).

Итак, авторизация учитывает результаты и/а. И/а – необходима для авторизации (если пользователи системы имеют разные права). Но авторизация – это отдельная процедура.

Чаще всего мы сталкиваемся с системами, где авторизация производится сразу после и/а, по ее результатам. В таких системах, как правило, решение об авторизации принимает тот же управляющий компонент, который принимает решение о результатах аутентификации.

Однако на деле все часто устроено затейливее, чем выглядит на первый взгляд, даже в таких системах. Как правило, разработчики систем ориентированы на то, чтобы минимизировать число процедур и/а для пользователей, и результаты одной и/а передаются от подсистемы аутентификации в самые разные подсистемы авторизации.

Разберем простейший пример: единый комплекс – ПАК СЗИ НСД «Аккорд» на автономном ПК. Комплекс состоит из СДЗ уровня платы расширения «Аккорд-АМДЗ» и СЗИ – монитора разграничения доступа – специального программного обеспечения (СПО) «Аккорд-хххх» (название после дефиса зависит от семейства ОС, для которой

предназначен комплекс и ее разрядности). В этом случае и/а пользователя производится соответствующей подсистемой Аккорда-АМДЗ из состава ПАК. Эта же подсистема производит авторизацию пользователя – на вход в систему администрирования Аккорда, если он администратор Аккорда, или на продолжение загрузки ОС, если он – пользователь (разумеется, с учетом ограничений на время, в которое они могут работать и всего остального – авторизация производится на основании не только положительного результата аутентификации, но и других признаков). Больше в отношении будущих действий пользователя Аккорд-АМДЗ ничего не предпринимает.

Дальше начинает работу программная часть комплекса – СПО «Аккорд». И уже оно разграничивает права пользователей в ОС, наряду с собственной подсистемой разграничения доступа самой ОС. И вот эти подсистемы авторизации в качестве входных данных могут запрашивать и/а пользователя, а могут – получать данные о пользователе от Аккорда-АМДЗ. В абсолютном большинстве случаев, конечно, ситуация развивается по второму сценарию, пользователь не проходит новую и/а. А вот авторизация на дальнейшую работу – производится.

К слову, в меньшем числе систем, но такие есть, наоборот, и/а проводится СПО «Аккорд», а не Аккордом-АМДЗ.

Итак, вернемся к базовой схеме: пользователь прошел и/а в Аккорд-АМДЗ, авторизовался им на продолжение загрузки ОС, ОС и СПО «Аккорд» получили данные о пользователе от Аккорда-АМДЗ (и/а прошла скрыто от пользователя) и авторизовали пользователя на положенные ему действия в ОС с учетом всех необходимых параметров.

Дальше пользователь может начать работу с приложениями, также требующими авторизации, например, с электронной почтой, или каким-то функциональным программным обеспечением, или инициировать соединение с каким-то удаленным ресурсом. В зависимости от того, насколько глубока проработка проекта системы, все эти действия могут требовать или не требовать от пользователя повторной и/а (повторной с его точки зрения, но первой – с точки зрения этих приложений), но процедура авторизации будет так или иначе иметь место. Очевидно, что успешность аутентификации не гарантирует пользователю авторизацию с желаемыми правами ни на

каком из этапов, но без этого условия авторизация вообще не будет осуществляться.

Есть и такие операции, для которых в общем случае недопустима «сквозная» аутентификация, например, доступ к криптографическим ключам, к операциям с использованием средств электронной подписи (СЭП).

За этим не скрывается никакой серьезной проблемы, это нужно просто себе представлять, чтобы отчетливо видеть процедуры, выполняемые подсистемой защиты информации, и чтобы адекватно проектировать сценарии действий пользователей.

2.6. И\А в открытых системах: новая биометрия и «оплати мой кофе своим взглядом»

Наконец, последнее, на чем необходимо остановиться в отношении идентификации и аутентификации.

Приемы идентификации существенно зависят от ее цели (это правило релевантно вообще для всех инструментов – они всегда зависят от цели, а если нет, то, скорее всего, они используются не по назначению и работают плохо).

Так вот, идентификация не всегда выполняется в целях безопасности, она выполняется также и в криминалистических целях.

Криминалистическая идентификация выполняется как правило на доверенном оборудовании, без сотрудничества с идентифицируемым объектом (потому что это обычно или труп, или подозреваемый (или даже и вовсе преступник)). Идентификация же в системах цифровой экономики выполняется в предположении, что субъект готов к сотрудничеству.

До сих пор задачи защиты информации ставились и решались для корпоративных систем, границы которых точно известны. В этих границах всегда можно обеспечить достаточный уровень защищенности, базирующийся на доверенности СВТ, включенных в состав системы.

Теперь же защита информации должна обеспечиваться в открытых системах, а в них ставить вопрос об обеспечении доверенности всех средств вычислительной техники просто невозможно. Так, мобильные средства доступа пользователей (смартфоны, планшеты) ни при каких условиях нельзя сделать доверенными, это личные устройства.

Очевидно, что все большее количество услуг граждане хотят получать именно по такой схеме – используя свои личные планшеты и телефоны. И никакие опасности их не остановят, о чем наилучшим образом свидетельствует длительный опыт использования ДБО. Потери клиентами денег сопровождают ДБО от самого его возникновения, но эти потери нисколько клиентов не останавливают. Наоборот, активно входят в нашу жизнь и более радикальные решения – класса «оплати взглядом».

Специалисты уже много писали о том, сколь мрачной видится перспектива оплаты взглядом в камеру [18 и др.]. Однако очевидно, что движение к тому, что так удобно, нельзя остановить, а можно только постараться ввести в разумное русло.

Можно развивать систему в двух направлениях – перенести всю тяжесть защиты на центр и отказаться от использования надежной криптографической защиты при доступе к сервисам (например, банка) с мобильных устройств пользователей, или/и строить распределенную, «иммунную» систему защиты, обеспечивающую приемлемый уровень защищенности клиентских транзакций даже при недоверенном оборудовании.

Первое направление очевидно, и многие идут по этому пути, полагая, что риски пока невелики и такими же останутся в дальнейшем. Очевидно, что это не так. Брешь в защите всегда находится и эксплуатируется преступниками. Брешей в защите следует избегать.

Второе направление еще ждет своих исследователей, оно совсем новое. Основой эффективных решений могут стать системы обнаружения вредоносной активности, построенные по принципу мультиагентных систем [22], а также системы мультимодальной биометрической идентификации с использованием динамики рефлекторных реакций.

Этот раздел – про рефлекторную идентификацию как метод и средство, которые позволят в ближайшее время применять недоверенные клиентские устройства в доверенных информационных системах цифрового общества.

Безопасность (и защищенность) всегда базируется на сложности и избыточности [9]. Так, электронный документ для фиксации волеизъявления автора дополняют электронной подписью (избыточность), а конфиденциальность обеспечивается криптографическими методами (сложность решения обратной задачи).

Операции идентификации и аутентификации занимают особое место в последовательности операций в открытых системах [23], так как еще до начала всех операций нужно понимать, с кем начинается взаимодействие – с партнером или хакером. И наоборот, результат информационного взаимодействия фиксируется применением электронной подписи, придающей взаимодействию статус волеизъявления.

Как быть в тех случаях, когда недоверенное личное устройство (планшет, телефон) гражданина – участника цифровой экономики – должно выступать его идентификатором при совершении того или иного волеизъявления? Пусть это будет вызов такси со смартфона с последующей оплатой услуг такси картой, привязанной к этому смартфону.

Очевидно, что для оплаты услуги кроме такси, смартфона и денег на счету необходимо также намерение пассажира оплатить услугу, иначе это уже не оплата услуги, а Бог знает, что. Кстати, на момент написания этой книги намерения пассажира для оплаты не требуется, деньги списываются вне зависимости от того, считаю ли я услугу оказанной.

Предполагается, что убедиться в том, что оплатить услугу – мое осознанное решение, должна помочь идентификация меня с помощью моего смартфона. Хорошо понятно, что далее возникает биометрическая идентификация, по целому ряду причин – она привычна в смартфонах, она кажется хорошо изученной и надежной, для нее не надо ничего запоминать или носить с собой, и так далее.

Однако, справедливости ради необходимо заметить, что хорошо изучена и поддержана длительным положительным опытом применения биометрическая идентификация исключительно в криминалистике. Которая, в свою очередь, имеет дело с совершенно другими инструментальными средствами, совершенно другими задачами идентификации и совершенно другими объектами идентификации. Диаметрально противоположные задачи и у злоумышленников, пытающихся влиять на процесс идентификации. Очевидно, что использовать биометрический методы, разработанные для совершенно другой области применения, в цифровой экономике невозможно. Но это не означает, что биометрию необходимо отклонить совсем – люди не откажутся от того, что так удобно. Об этом уже многое написано [18; 24. С. 65–83], разработаны подход и концепция [25], в лаборатории МФТИ ведутся исследования и разрабатываются

конкретные способы реализации этого подхода. Далее некоторые его детали.

2.6.1. Идентификация в открытых системах

Естественным механизмом идентификации (аутентификации) для открытых систем представляется биометрическая идентификация. Биометрические параметры неотъемлемы от человека, и поэтому соблазн использовать их объясним. Об эффективности биометрии свидетельствует огромный опыт применения для идентификации самых разных модальностей – радужной оболочки глаза, папиллярного узора, рисунка сосудистого русла, формы лица, ладони, голоса, состав генома и другие. Эти биометрические модальности хотя и избыточны, но предельно просты – они или статичны, или условно статичны. Более того – если снимаемые приборами характеристики не инвариантны, то исследователи зачастую пытаются свести их к инвариантам [26] в попытке упростить последующий анализ. Например, голос существенно зависит от состояния мягких тканей, это значит, что при насморке он может измениться (характеристика не инвариантна). И чтобы упростить работу с голосом как биометрической характеристикой, исследователи пытаются свести эту характеристику к зависимости только от твердых тканей. Это обеспечивает инвариантность, но уменьшает информативность за счет снижения сложности.

В силу простоты и статичности эти модальности легко воспроизводятся и моделируются, что не только не снижает риски ошибочной идентификации, но и позволяет влиять на ее результаты.

Традиционные (инвариантные) биометрические модальности не обеспечивают и не могут обеспечить достаточный уровень доверия к результатам идентификации на недоверенном устройстве.

Успешный же опыт применения биометрии связан не с визуальной и/или приборной идентификацией, а только с криминалистической, где в базах данных никто отпечатки не подменит, гражданин не наденет при регистрации отпечатков перчатку и не передаст ее потом злоумышленнику, а средства идентификации, используемые полицией – доверенные [27].

Таким образом:

- биометрические характеристики применяются для идентификации и аутентификации в силу своей инвариантности к внешним факторам, полной или частичной;
- исследования по применению биометрических механизмов явно или неявно основываются на предположении о доверенности технических средств обработки.

В нашем случае предположение во втором пункте явно неверно, и именно это требует изменения подхода к биометрическим характеристикам как к инвариантам.

Действительно, любые результаты идентификации, если они будут получены на недоверенных (обычных) устройствах (смартфонах, планшетах) легко подделать, что дискредитирует саму идею применения биометрии в юридически значимом информационном взаимодействии.

Работаем ли мы с измерениями, полученными непосредственно датчиками (микрофоном, камерой и т.д.), или это данные, уже подменённые злоумышленником? Пока мы не знаем, как это определить, мы не можем реализовать такую идентификацию, которую достаточно для обеспечения юридической значимости и доступа к удаленным криптографическим ключам при использовании недоверенных клиентских устройств.

Простота подделки статических биометрических модальностей сегодня осознана [28], и операторов идентификации на основе биометрических данных начинает интересовать вопрос: «А нельзя ли повысить достоверность идентификации за счет использования не одной, а нескольких биометрических характеристик»? – то есть за счет мультимодальности на этапе принятия решения.

Мультимодальность, однако, такая же мантра, как многофакторность. Для независимых модальностей вероятности ошибок (как первого, так и второго рода) перемножаются. Независимость при этом понимается как независимость источников и независимость каналов.

Предположительно, биометрические характеристики человека нельзя считать независимыми уже хотя бы потому, что они принадлежат одному человеку. Во всяком случае, независимость не доказана и, скорее всего, не изучалась. Уже в связи с этим гипотеза о повышении

уровня доверия при использовании мультимодальностей не очевидна и требует серьезного изучения.

Выше уже было разобрано, что для повышения защищенности каналы должны быть независимыми, а в нашем случае канал один – он формируется клиентским терминалом (смартфоном) и интернетом. Конечно, ни о какой независимости здесь даже не может идти речь.

Таким образом, использование статических параметров для повышения достоверности идентификации с использованием недоверенного устройства практически нецелесообразно.

Одним из решений проблемы подделки (или подмены) статических (инвариантных) биометрических параметров является проверка активности и разумности субъекта в дополнение к проверке биометрических показателей. Такая проверка могла бы отсечь случаи полностью автоматизированной подмены параметров. Традиционным способом проверки того, что субъект не является алгоритмом или компьютерной программой, является так называемый тест Тьюринга, или CAPTCHA. Пользователю предлагается распознать текст, звук, изображение, или решить арифметическую или логическую задачу. Работоспособность такой методики обосновывается тем, что указанные задачи для их решения требуют применения интеллекта человека. Однако последние успехи в области машинного обучения хоть и не позволяют построить «сильный» искусственный интеллект (подобный человеческому), но позволяют решить множество частных задач, которые, как ранее считалось, может решить только человек (то есть создать «слабый» искусственный интеллект). К таким задачам относятся распознавание речи и образов, перевод на разные языки, обработка запросов на естественном языке, текстовое описание изображений и видео. Поэтому такой подход не применим для описанной выше проблемы. Но даже если бы алгоритмы искусственного интеллекта не совершенствовались с каждым днём, то на недоверенном устройстве пройти тесты, контролирующие интеллект, может злоумышленник-человек, а биометрические характеристики – подменить.

Другие способы проверки активности субъекта – проверка подвижности зрачков глаз при сличении рисунка радужной оболочки, проверка температуры лица при идентификации по лицу, или проверка наличия пульса при анализе отпечатков пальцев – обладают

аналогичными недостатками: могут быть подделаны либо подменены на недоверенном считывающем устройстве.

2.6.2. Криминалистика и экономика

Сравним **задачи, средства** и **данные**, необходимые для решения задачи идентификации в криминалистике и в цифровой экономике.

Идентификация в рассматриваемом контексте может упрощенно трактоваться как установление личности. Это так и для криминалистики, и для процессов цифровой экономики. Видимо, такая упрощенная трактовка и привела к имеющейся путанице. Рассмотрим теперь понятия более глубоко.

Нулевая гипотеза идентификации может быть сформулирована субъектом так: «Идентифицируемый объект – тот, за кого он себя выдает (за кого его принимает субъект)».

Криминалистика, как правило, имеет дело с теми, кто ориентирован на сотрудничество. Ее обычный объект – это труп, подозреваемый или преступник. Цель анализа – доказать факт совершившегося доступа объекта – к орудию и/или месту преступления, установление личности потерпевшего и так далее. И, конечно, объект редко заинтересован в правильной идентификации.

Активное противодействие здесь, если оно есть, направлено на нарушение идентификации – доказать, что там не был, не участвовал, не нарушал.

Другими словами, противодействие (со стороны объекта, или сообщников, или трудности, связанные с недостатком данных) направлено для достижения ошибки «*false positive*» – ошибки первого рода (отвергнута верная нулевая гипотеза).

Цель противодействия (бездействия) – отклонить нулевую гипотезу при том, что она верна.

Используемые технические средства при этом – доверенные. Они специально разрабатываются, защищаются сертифицированными средствами, проходят регламентные процедуры контроля и так далее.

В цифровой экономике – объект идентификации вполне живой и добропорядочный участник экономической деятельности. Пример его

потребности – получить доступ к некоторым ресурсам. Он готов к сотрудничеству, готов выполнить некоторые действия, чтобы после успешной идентификации получить нужную ему услугу. Он заинтересован в правильной идентификации.

Активное противодействие системе может осуществлять хакер (или просто злоумышленник), добиваясь в свою пользу ложной идентификации. Противодействие направлено на достижение ошибки «*false negative*» – ошибки второго рода (принята ложная нулевая гипотеза).

Цель противодействия – выдать себя за другого. Вынудить субъекта принять нулевую гипотезу при том, что она ложна.

Технические средства – произвольные. Это обычные планшеты и смартфоны, ничем не защищенные от внедрения вредоносного ПО.

Для наглядности сведем в таблицу характеристики и установки объекта процесса идентификации (табл. 2.4). Вырожденные случаи (труп) не рассматриваем.

Таблица 2.4. Субъект идентифицирует объект. Цели объекта.

Сфера применения	Объект идентификации	Заинтересованность объекта в подтверждении гипотезы	Желательный результат
Криминалистика	Добропорядочный гражданин (подозреваемый)	Нет	Верный
	Преступник	Нет	Ошибка 1 рода
Цифровая экономика	Добропорядочный гражданин	Да	Верный
	Преступник	Да	Ошибка 2 рода

Мы видим полностью противоположные характеристики.

Не менее наглядны и отличия в позициях субъекта идентификации (табл. 2.5).

Таблица 2.5. Субъект идентифицирует объект. Характеристики процесса.

Характеристики процесса для субъекта	Криминалистика	Цифровая экономика
Гипотеза	Объект – тот, за кого его принимает субъект	

Доверенность среды идентификации и контролируемость инструмента	Да	Нет
Значимость того, жив ли объект	Нет	Да
Значимость согласия объекта на идентификацию	Нет	Да
Значимость согласия объекта с результатами	Нет	Да

Таким образом, процессы идентификации в криминалистике и цифровой экономике при заданной гипотезе полностью различны.

Не совпадают:

- объекты идентификации;
- их одушевленность/неодушевленность;
- заинтересованность объекта идентификации в ошибке;
- желательный для объекта идентификации результат;
- характер участия объекта в процессе идентификации.

При этом противоположными являются:

- контролируемость инструмента субъектом;
- доверенность среды идентификации;
- значимость того, жив ли объект идентификации;
- значимость согласия объекта идентификации с результатом идентификации;
- заинтересованность объекта идентификации в подтверждении гипотезы субъекта.

2.6.3. Новая биометрия. Замысел защиты

Для устранения уязвимостей, связанных с простотой подмены измерений на недоверенных устройствах, необходимо от статических показателей перейти к динамическим типа «стимул-реакция» со сложной динамикой связи. Динамическим звеном, чрезвычайно сложным на сегодняшний день для моделирования, являются нервная и вегетативная системы человека и связанные с этим особенности физиологии движений. В частности, индивидуальными оказываются непроизвольные реакции на внешние стимулы (в частности, аудио и видео раздражители).

Реакция на стимулы может быть зафиксирована датчиками клиентского устройства, обработана с помощью методов

искусственного интеллекта, например, искусственных нейронных сетей [28], и это позволит определить источник потоков данных и повысить достоверность идентификации, а также обеспечить решение задачи виталентности.

На недоверенном клиентском терминале не сложно подделать голос, лицо, подменить отпечатки пальцев и рисунок сосудистого русла, сымитировать движение глаз, но если в качестве биометрического признака использовать реакцию на раздражитель — то изменения этих модальностей при реальном источнике должны быть согласованными, и поэтому подделать потоки данных будет почти невозможно, так как для согласования поддельных данных нужна модель реакций *конкретного человека*, построение такой модели недоступно злоумышленнику, так как она чрезвычайно сложна.

На сегодняшний день психомоторные реакции человека исследуются, как правило, на сложном лабораторном медицинском оборудовании в контролируемых условиях. Однако исходя из параметров современных и перспективных технических средств (смартфонов), с их помощью среди динамических биометрических характеристик человека представляется возможным зафиксировать, по крайней мере, характеристики пульсовой волны, динамику изменения диаметра зрачка, динамику слежения взглядом за стимулом на экране. Для этого достаточно на смартфоне иметь камеру и вспышку (фонарик), а также сенсорный экран.

Перспективным является изучение движения глаз. Глаз не может быть неподвижным, клетки рецепторов «утомляются» и «подменяются» в процессе саккадических движений. Эти движения характеризуются высокой сложностью. Достаточно отметить, что движениями глаз управляют 7 мышц (!), и мышцы, ответственные за саккадические движения, являются самыми быстрыми. Многообещающим представляется изучение рефлекторной составляющей саккад, а также (а может, и в первую очередь) процессы фиксации и регрессии при чтении.

Изучение пульсовой волны предположительно позволит выделить реакцию сердца – изучить вариабельность сердечного ритма. Это тем более важно, что для жизнедеятельности организма сердце важнее зрения, и регулирование осуществляется более «старыми» (и, таким образом, более стабильными) механизмами, в том числе ЦНС и

вегетативной системой. При этом уровни регулирования могут меняться в зависимости от многих факторов, что позволяет считать механизм достаточно сложным для моделирования.

В качестве внешних раздражителей можно использовать имеющиеся у смартфона возможности – звук, цвет и свет, вибрацию, отображение текста (в том числе со случайным изменением числа пробелов).

Для движения по разработке данного подхода необходимо:

- проверить методом объективных измерений гипотезу о влиянии различных внешних раздражителей на рефлекторные реакции;
- создать алгоритмы сбора первичных данных на пользовательских устройствах (смартфонах)
- разработать искусственную нейронную сеть анализа данных, снимаемых средствами смартфона, либо применить другие адекватные задаче методы анализа.

Подробнее об этом см. [24. С. 65–83].

Безопасность такого подхода определяет сложность и количество параметров нейронной сети. Поскольку потенциальный злоумышленник не знает какие параметры реакций анализирует нейросеть, то и подделать саму реакцию представляется крайне сложным. С другой стороны, если злоумышленник вдруг получит набор данных, по которым обучалась нейросеть, то это не приведёт к тому, что он сможет её воспроизвести. Даже в том случае если будет построена и обучена сеть аналогичной архитектуры, получаемое представление будет отлично от имеющегося. Результат обучения сети, характеристики нейронов выходных и низкоуровневых слоёв носят стохастический характер, определяется случайными начальными параметрами и порядком поступления данных. К примеру, перестановка выходных нейронов местами не изменит точности работы сети, но принципиально изменит представление реакции, то есть идентификатор человека, который будет сравниваться на сервере с идентификаторами из базы.

Основой нового подхода является гипотеза о том, что зависимость реакций человека на внешние стимулы существенно зависит от когнитивных и кинезиологических особенностей человека, носит

динамический характер и отражается в измерениях в достаточной для анализа степени.

Принципиальными особенностями системы стимул-реакция является:

– наличие нервной системы человека как связующего звена между стимулом и реакцией. Если к симуляции интеллекта уже достаточно много подходов, то работ по симуляции нервной системы практически нет. Нервные системы людей крайне сильно отличаются между собой и сложны для моделирования. В отличие от интеллектуальных задач у нервной системы нет «правильного ответа», которому бы можно было научить машину.

– случайные, не повторяющиеся стимулы. Такой подход позволит принципиально исключить возможность воспроизведения ранее записанных реакций пользователя, то есть подлога первичных данных.

– обработка пары стимул-реакция может производиться на удалённом доверенном устройстве.

При этом:

Недоверенность клиентского терминала не влияет на результаты, так как генерация стимула и анализ реакции выполняется на отчужденных доверенных ресурсах, а искажение реакции не даст возможности злоумышленнику получить нужный для него результат

Перехватывать стимул нет смысла, так как зная стимул, невозможно сгенерировать реакцию в силу отсутствия модели человека

Извлечь параметры нейронной сети путем ее тестирования в заданных условиях невозможно, а акты идентификации постоянно уточняют параметры нейронной сети, и поэтому даже тотальное наблюдение не позволит в полной мере воспроизвести сеть.

Нетрудно видеть, что основная особенность, обеспечивающая безопасность идентификации на недоверенном устройстве, состоит в интерактивности – ни клиентский терминал, ни центр сами по себе не выполнят идентификацию. Процедура существенно интерактивна, что и позволяет генерацию стимула и принятие решения отнести к доверенному центру, а съем информации осуществлять на принадлежащем клиенту персональном устройстве.

СПИСОК ЛИТЕРАТУРЫ:

1. Аутентификация // Википедия [электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Аутентификация#Факторы_аутентификации (дата обращения – 29.04.2019).
2. *NIST Специальная публикация 800-63B. Руководство по цифровой идентификации. Аутентификация и управление жизненным циклом. 2017 [электронный ресурс]. URL:* https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения - 30.04.2019).
3. *Комаров А.* Современные методы аутентификации: токен и это все о нем…! // T-Comm. 2008. № 6. С. 13–16.
4. ISO/IEC 2nd WD 29003 -- Information technology – Security techniques – Identity proofing. 2013 [электронный ресурс]. URL: https://cabforum.org/pipermail/public/attachments/20130814/f2f4a333/attachment.pdf (дата обращения – 30.04.2019).
5. ГОСТ Р 58833-2020 «Идентификация и аутентификация. Общие положения».
6. *Стрельцов А. А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. - М.: «МЦНМО», 2002. – 296 с.
7. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. Минск: Серия «Библиотека журнала "УЗИ"», 2004 – 327 с.
8. ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации».
9. Большой толковый словарь русского языка / Гл. ред. С. А. Кузнецов. СПб.: Норинт, 1998.
10. Проект ГОСТ Р «Защита информации. Формальное моделирование политики безопасности Часть 1. Формальная модель управления доступом» [электронный ресурс] URL: https://docs.cntd.ru/document/560851933 (дата обращения: 15.12.2021).
11. Authenticator // Wikipedia [электронный ресурс] URL: https://en.wikipedia.org/wiki/Authenticator (дата обращения – 22.06.2019).
12. *Конявский В. А.* Серебряная пуля для хакера // Защита информации. INSIDE. СПб., 2013. № 4. С. 54–56.
13. *Конявский В. А.* Серебряная пуля для хакера (Окончание) // Защита информации. INSIDE. СПб., 2013. № 5. С. 69–73.
14. *Конявский В. А., Чугринов А. В.* Съемный носитель информации. Патент на полезную модель № 102139. 10.02.2011, бюл. №4.
15. *Конявский В. А.* Съемный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012, бюл. №36.
16. *Конявский В.А.* Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013, бюл. № 20.

17. *Конявский В.А.* Модем для безопасных коммуникаций в компьютерных сетях. Патент на полезную модель № 128055. 10.05.2013, бюл. № 13.

18. *Конявский В. А.* Новая биометрия. Можно ли в новой экономике применять старые методы? // Information Security\Информационная безопасность. 2018. № 4. С. 34–36.

19. *Конявский В. А.* Интерактивный способ биометрической аутентификации пользователя. Патент на изобретение № 267024.10.2018, бюл. № 30.

20. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. URL: http://docs.cntd.ru/document/gost-r-50922-2006 (дата обращения: 12.05.2020).

21. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 17.01.2022).

22. *Лихтенштейн В. Е., Конявский В. А., Росс Г. В., Лось В. П.* Мультиагентные системы: самоорганизация и развитие. М.: Финансы и статистика, 2018. – 264 с.: ил.

23. *Конявский В. А.* Идентификация и применение ЭЦП в компьютерных системах информационного общества // Безопасность информационных технологий. М., 2010. № 3. С. 6–13.

24. Конявский В. А., Конявская С. В. Доверенные информационные технологии: от архитектуры к системам и средствам. М.: URSS. 2019. –264 с.

25. Конявский В. А., Бродский А. В., Горбачев В. А., Карпов О. Э., Кузнецов Н. А., Райгородский А. М., Тренин С. А. Идентификация в компьютерных системах цифровой экономики // Информационные процессы, Том 18, № 4, 2018. С. 376–385.

26. *Сорокин В. Н., Макаров И. С.* Обратная задача для голосового источника. // Информационные процессы. 2006. Т. 6. № 4. С. 375–395.

27. Система оперативных проверок по оттиску пальца ПАПИЛОН «Фильтр» [электронный ресурс]. URL: http://www.papillon.ru/rus/38/ (дата обращения: 22.01.2019).

28. *LeCun, Y., Bengio, Y., Hinton G.* Deep learning. Nature. 2015. V. 521. P. 436–444.

ГЛАВА 3: РАЗГРАНИЧЕНИЕ ДОСТУПА

Защита неравенства

Вообще говоря, информация (ни в форме сообщений, данных, ни в форме процессов, технологий) в защите не нуждается. Как и в случае с любой собственностью – защита вклада, автомобиля, интеллектуальной собственности – речь идет на самом деле о защите интересов владельца.

Защитить их можно только при обязательном выполнении двух условий:

1) Известно, кто владелец,
2) Известно, в чем состоят его интересы.

Пытаться защищать что-то, не задаваясь этими вопросами, недопустимо, это не защита, а изображение бурной деятельности.

В защите информации ситуация осложняется несколькими ментальными факторами, в том числе:

1) Различными комплексами и травмами, связанными с открытостью информации (сюда стоит отнести и убежденность в том, что все должно быть открыто, и уверенность, что все должно быть скрыто, и позицию о том, что «кому надо» все в любом случае известно (или должно стать известно по первому требованию)).

2) Нечеткое понимание того, в каком смысле можно вообще *владеть* информацией (несмотря на чудовищную распространенность штампа «кто владеет информацией, тот владеет миром»).

3) Известная сложность формулирования интересов владельца информации, даже если он ясно определен и в общем виде отдает себе отчет в своих интересах.

С первыми двумя все понятно, для нейтрализации их негативного влияния нужно просто «по капле выдавливать из себя раба»[24]. Третье же по своей природе объективно. Если в отношении противоугонного средства для машины или замка от двери дома владельцу довольно несложно сформулировать свои интересы – и в соответствии с ними снабдить ключами тех, кого надо, и не снабжать тех, кого не надо, то в отношении своих интересов, связанных с данными и технологиями в компьютерных системах, такой ясности у владельца системы как правило нет. Это не всегда говорит о том, что владелец системы не понимает важности защиты информации, хотя бывает и так. Однако самая главная причина все же в том, что для полной и недвусмысленной формулировки требований к защите информации в той или иной системе, необходимо быть специалистом по защите информации. В компьютерной системе есть очень много нюансов, которые нужно представлять себе для этого очень хорошо. Владелец же системы зачастую является специалистом в какой-то другой области.

Здесь возникает проблема – перевод представления владельца о своих интересах в понятия реальной компьютерной системы часто выполняется недобросовестно. В лучшем случае при этом навязываются лишние средства защиты, а в худшем – защита подменяется видимостью защиты, так как не ставятся необходимые СЗИ.

Недобросовестность проистекает не всегда из злого умысла, часто специалисты по защите информации просто имеют низкую квалификацию.

Попробуем установить фундамент, на котором можно выстроить систему самоконтроля и убедиться, что в замысле защиты нет явных лакун.

Итак, защита информации направлена на защиту интересов ее владельца. В то же время ни данные, ни средства вычислительной

[24] Эта идиома восходит к письму А. П. Чехова издателю. Если долго и настойчиво это делать, рано или поздно ощутишь в себе человеческую, а не рабскую кровь.

техники, ни каналы связи – ничего об этом не знают. Они универсальны, так же, впрочем, как и любые предметы – для автомобиля нет никакой разницы между человеком, который за него заплатил, и любым другим человеком. То же с компьютером и революционной разработкой в нем – они понятия не имеют, чьи они, они универсальны.

Значит, цель любой защиты интересов собственника – сделать универсальный объект не универсальным.

При этом хорошо понятно, что владелец и пользователь – это не всегда одно и то же лицо. Как в случае с компьютером или флешкой, так и в случае с автомобилем. Задача защиты не сводится к тому, чтобы использовать свою собственность (иметь доступ к собственности) мог только владелец. Она в том, чтобы доступом к собственности, в том числе, информации *мог управлять* владелец.

Стало быть, наличие четко определяемого владельца – совершенно необходимое условие для обеспечения информационной безопасности. Владелец – это та точка отсчета, которая необходима для построения системы защиты.

Поэтому нельзя одинаково относиться к элементам системы, принадлежащим (а значит, принципиально подконтрольным) владельцу системы, и элементам, принадлежащим кому-то еще, относящимся к смежным системам, системам общего пользования, принадлежащим сотрудникам или клиентам организации-владельца. Контролируемость таких элементов никогда не может быть такой же, как контролируемость собственных ресурсов. Про это надо помнить.

Защита информации должна обеспечить *владельцу информации* – возможность распоряжаться доступом к информации на его усмотрение, а всем остальным – действовать в соответствии с *назначенными для них владельцем правами*.

Защищенные устройства или системы – это такие, пользоваться которыми могут не все.

Защита интересов владельца – это защита его приоритетного положения по отношению к своей собственности.

Эта глава посвящена различным аспектам ограничения в правах легальных пользователей устройств и систем.

В этой главе не пойдет речь о ситуации, когда владелец данных и владелец системы – разные субъекты, хотя это важно и совсем не редко бывает. На момент написания этого текста ОКБ САПР принимает участие в разработке информационной системы, где приоритетное право на распоряжение собственными данными владельцам данных, не совпадающим с владельцем системы, обеспечивается технически, а не организационно. Описание его в учебнике по введению в дисциплину неуместно не из соображений охраны know-how, а просто потому, что совершенно новое очень трудно описать достаточно просто.

3.1. Разграничение доступа к ресурсам в доверенной среде

Речь в этом разделе пойдет о тех случаях, когда средства разграничения доступа являются частью той подсистемы защиты информации, которая создает и поддерживает на тех или иных СВТ доверенную вычислительную среду.

3.1.1. Разграничение доступа в ОС

Про разграничение доступа внутри операционных систем написано очень много всего, что вы будете изучать по разным базовым и общеобразовательным предметам. Для начального представления, которое позволит более-менее систематизировано воспринимать все, что будет преподаваться далее, достаточно представлений о дискреционном и мандатном механизмах разграничения доступа. Именно к их реализации, кстати, есть требования в нормативной методической базе, и в дальнейшем, прочитав книги В. А. Конявского [1 и 2], вы хорошо поймете, почему так.

Определение:

Дискреционный механизм разграничения доступа – это способ выражения прав доступа через доступ субъектов к объектам, который может быть запрещен или разрешен для определенных видов действий.

Определение:

Мандатный механизм разграничения доступа – это способ выражения прав через сопоставление субъектов и объектов некоторым меткам и категориям.

Также сразу стоит определиться с рядом понятий того же семантического поля, в применении и толковании которых есть известная путаница и она может критически негативно сказаться на понимании этого раздела в целом.

Речь о понятиях «правило доступа», «право доступа», «правило разграничения доступа», «политика разграничения доступа», «политика безопасности информации».

В первую очередь, сразу необходимо оговорить, что порядка в определении и применении перечисленных понятий нет, поэтому невозможно с полным основанием назвать их терминами. Однако, безусловно, это, как минимум, идиомы. Более того, вы точно встретите, в том числе в, как говорится, «авторитетных источниках» случаи применения этих идиом не в таких значениях, как даны ниже, а часто даже просто как синонимов. С этим ничего невозможно поделать, так как терминологическая система защиты информации, с одной стороны, слишком молода по сравнению со «старыми» науками, а с другой стороны, слишком подвержена воздействию нормативных методических, а не научных работ.

Поэтому в отношении применения терминологии целесообразно придерживаться следующих соображений:

1) использовать те определения терминов, которые формируют непротиворечивую систему (или как минимум, не создают противоречий в рамках текущего рассуждения);

2) использовать только те термины и только в тех значениях, которые необходимы для вашего рассуждения, так как каждый лишний термин – лишний предмет для дискуссий (если дискуссия продуктивна – термин стоит использовать, если она будет только мешать – не стоит);

3) всегда указывать и аргументировать источник определения дискуссионных терминов, даже если оно не приводится буквально, чтобы, с одной стороны, контекст был правильно понят, а с другой, опять же, была минимизирована дискуссия о терминах и определениях.

К правилам использования определений мы вернемся в рамках другой дисциплины и рассмотрим их намного детальнее.

В нашем случае определения не требуются, ограничимся тем, что установим и зафиксируем системные отношения понятий.

Политика безопасности информации (или политика информационной безопасности) – это общее описание того идеального состояния системы, которое должно быть воплощено в реальность путем применения средств защиты информации. Зачастую ее называют просто «политика безопасности», так как предполагается, что контекст четко определяет, что речь не идет о противопожарной, экологической или эпидемиологической безопасности.

Политика безопасности – состоит из **правил доступа**, которые не должны противоречить одно другому (политика должна быть непротиворечивой).

Правила доступа (и, соответственно, политику как совокупность, систему этих правил) формулируют люди (владелец системы или ответственный за это направление руководитель), выражены они вербально, то есть словами, на естественном языке (например, на русском).

Затем **правила доступа** формализуются в правила разграничения доступа (ПРД). Это делают безопасники, выражая заданные в политике правила в категориях того (тех) **механизмов разграничения доступа** (мандатный, дискреционный), который (которые) реализованы в используемом средстве защиты информации.

Правила разграничения доступа задаются непосредственно в компьютерной системе наборами **прав доступа** на основе алфавита реализованных в нем **атрибутов**.

Требование к корректной **реализации механизма** разграничения доступа в средстве защиты информации звучит так – с его помощью должно быть возможно реализовать любую непротиворечивую политику безопасности. Очевидно (из изложенного выше и из соображений здравого смысла), что для этого требуется не только

корректная реализация механизма, но и полнота алфавита – набора атрибутов.

Разберем подробнее и на примерах.

3.1.1.1. Дискреционный механизм

Требование реализации дискреционного механизма разграничения доступа обобщенно звучит так: комплекс средств защиты (КСЗ) должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т. д.).

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Для каждой пары (субъект–объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (пользователя или группы пользователей) к данному ресурсу СВТ (объекту).

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа (ПРД), как для явных действий пользователя, так и для скрытых. Под «явными» здесь подразумеваются действия, осуществляемые с использованием системных средств — системных макрокоманд, инструкций языков высокого уровня и т. д., а под «скрытыми» — иные действия, в том числе с использованием собственных программ работы с устройствами.

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам (администраторам безопасности информации).

Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Итак, если дискреционный механизм разграничения доступа – это способ выражения правил доступа, то для его реализации необходимо создать формальное описание тех правил, которые должны быть заданы в системе. Вспомним, что контролировать использование своих ресурсов должен по логике вещей их владелец. Стало быть, целесообразно исходить из того, что полученная модель должна, с одной стороны, быть ему (или, что более реалистично – уполномоченному им привилегированному пользователю, администратору безопасности информации) понятна, с другой — не ограничивать его в реализации процедур разграничения доступа и как можно ближе соответствовать особенностям архитектуры технических средств компьютера и особенностям операционной системы.

С этой точки зрения необходимо определить, что целесообразно выбрать в качестве *объектов* разграничения доступа, и какие допустимые *типы доступа* целесообразно использовать.

В качестве объектов в ОС обычно используются:

— диски;

— каталоги;

— файлы (задачи).

Конечно, использование файлов (задач) в качестве основного типа объектов разграничения доступа нецелесообразно, т. к. в этом случае объем и сложность описаний ПРД были бы неоправданно увеличены.

Нужно отметить, что выбор базового уровня объектов разграничения доступа зависит от уровня развития средств вычислительной техники и политики информационной безопасности, принятой в организации. Даже из общих соображений ясно, что количество объектов, которыми может управлять оператор, конечно. С ростом количества объектов существенно возрастает трудоемкость управления защитой — в частности, резко растет объем описаний правил разграничения доступа, усложняются процедуры анализа

корректности этих описаний и т. д. Рано или поздно целесообразным становится переход на более высокий уровень иерархии объектов — от записей к файлам, от файлов к каталогам, от каталогов к логическим дискам.

Тем не менее, основным объектом иерархии в ОС являются каталоги, и, таким образом, естественным выбором в качестве основного объекта доступа является выбор каталогов.

Выбор типов доступа целесообразно связать с функциями ОС, посредством которых осуществляется доступ к ресурсам. Перехват вызовов этих функций позволит реализовать ПРД для явных действий пользователя.

Реализация ПРД для скрытых действий пользователя может быть осуществлена за счет ограничения перечня задач, которые пользователь имеет право запускать. Это означает, что средства РД должны содержать возможность явного и недвусмысленного описания перечня задач, запуск которых разрешен пользователю, и средства контроля за использованием этих задач. Формирование перечня должно осуществляться администратором безопасности информации в порядке, предусмотренном для формирования и изменения ПРД.

Разграничение доступа в СЗИ «Аккорд» реализовано при помощи резидентной программы, которая перехватывает на себя обработку функций ОС.

Смысл работы этого резидентного модуля в том, что при получении от пользовательской программы запроса, например, на удаление файла — сначала производится проверка наличия таких полномочий у пользователя. Если такие полномочия есть — управление передается обычному обработчику ОС для исполнения операции. Если таких полномочий нет — имитируется выход с ошибкой.

В большинстве систем разграничения доступа в качестве атрибутов используется триада (*R, W, X*), где

R – разрешение на чтение объекта (диска, каталога, файла),

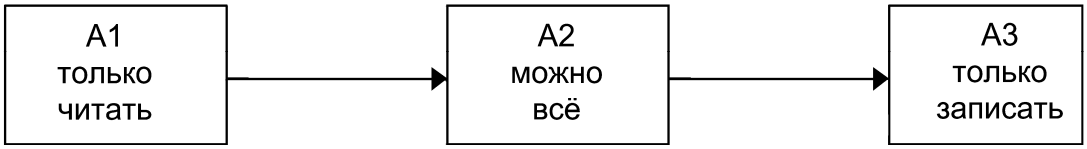
W – разрешение на модернизацию объекта,

X – разрешение на запуск задач.

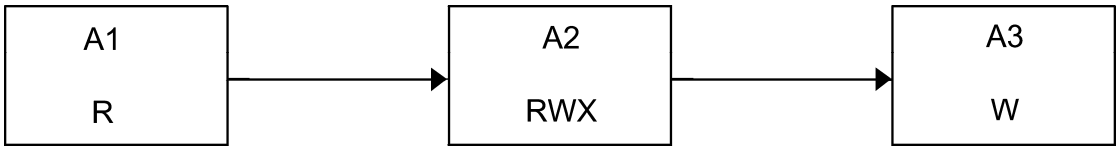
Достаточно ли этих атрибутов, чтобы на их основе реализовать «любую разумную непротиворечивую политику безопасности» (именно это является критерием качества реализации механизма разграничения доступа) предприятия (организации)?

Очевидно, что нет. Рассмотрим на примере процедуры конфиденциального делопроизводства. Движение документов может в этом случае быть таким:

Исходный документ (файл) может быть только прочитан пользователем из каталога *A1* и переписан в каталог *A2*. В каталоге *A2* документ обрабатывается по произвольной технологии, а после завершения записывается в каталог *A3*, после чего документ уже не может быть модифицирован (и даже прочитан) этим пользователем.



С использованием триады (*R, W, X*) права доступа могут быть назначены следующим образом.



Обратим внимание — при этом итоговый документ, записанный в каталог *A3*, может быть модифицирован оператором, так как атрибут <*W*> разрешает не только запись, но и модификацию (переименование, удаление, изменение) объекта.

Даже этот пример показывает, что трех атрибутов недостаточно для описания политики безопасности организации.

В СЗИ «Аккорд» используется полная, на наш взгляд, система атрибутов, позволяющая реализовать любую разумную политику безопасности.

Для описания взаимодействия <субъект-объект> в СЗИ «Аккорд» применяются следующие атрибуты:

R – открытие файлов для чтения;

W – открытие файлов для записи;

O – подмена атрибута *R* атрибутами *RW* на этапе открытия файла;

C – создание файлов;

D – удаление файлов;

N – переименование файлов и подкаталогов;

V – видимость файлов;

M – создание подкаталогов;

E – удаление подкаталогов;

G – доступность данного каталога (т. е. переход к нему);

X – запуск задач;

S – наследование подкаталогами атрибутов каталога.

В СЗИ «Аккорд» поддерживается также два списка файлов, применение которых повышает адаптивность системы. Это «белый» список и «черный» список.

Права доступа к файлам белого списка будут обеспечиваться в безусловном порядке, даже если файл расположен в каталоге, доступа к которому данный пользователь не имеет. Права могут быть такие:

— открытие файлов для записи;

— открытие файлов для чтения;

— создание файлов;

— удаление файлов;

— переименование файлов;

— видимость файлов.

Предусмотрена также возможность установки разрешения на исполнение задач, размещенных в данном файле.

Файлы из «черного списка» становятся недоступными пользователю, даже если они расположены в каталогах, к которым пользователь имеет доступ. В «черный список» можно включать также логические имена устройств и драйверы устройств. Эти объекты после такого описания становятся недоступны пользователю. Таким образом осуществляется сопоставление пользователя и доступных ему устройств.

С помощью описанных механизмов назначаются ПРД для каждого пользователя.

Еще одним существенным фактором является дисциплина взаимодействия атрибутов. В обычных системах по отношению к иерархическим элементам файловой системы (логический диск-каталог-файл) действует правило, по которому право доступа к объектам нижнего уровня определяются минимальными правами доступа ко всем объектам вышележащих уровней. В СЗИ «Аккорд» такое правило действует на уровне «логический диск — остальные объекты», но на всех других уровнях (каталог — подкаталоги — файлы) атрибуты независимы, если не используется специально введенный атрибут наследования «S» — наследование подкаталогами атрибутов каталога.

Очевидно, что задача конфиденциального делопроизводства легко решается в системе атрибутов СЗИ «Аккорд».

Однако пусть дискреционным механизмом определено, что субъект S_1 имеет доступ к объектам F_1 и F_2, а субъект S_2 имеет доступ только к объекту F_2. В этом случае ничто не помешает S_1 скопировать сведения из F_1 в F_2. При этом S_2, обладая доступом к F_2, фактически получает доступ к сведениям из F_1.

Таким образом, защита информации посредством дискреционного механизма не является полной. Необходимо с учетом возможности доступа S_2 контролировать также поток от F_1 к F_2, организованный S_1, т. е. необходимо введение мандатного механизма.

3.1.1.2. Мандатный механизм

Отсутствие мандатного механизма является, на наш взгляд, основной допускаемой в настоящее время ошибкой, от преодоления которой зависит эффективность защиты. Причина же повторения вновь и вновь этой ошибки заключается преимущественно в том, что мандатный механизм разграничения доступа считается очень сложным для понимания, а тем более – использования.

Рассмотрим, так ли это сложно, и почему это так уж важно (на основе рассуждения из § 13 главы 3 второго тома книги «Компьютерная преступность», где оно приводится в связи с межсетевыми экранами [3]).

Принятие решения о доступе субъекта к объекту связано с *характеристиками субъекта и объекта*, но все еще очень слабо связано с тем, *откуда* субъект запрашивает сведения из объекта и с помощью *каких средств* он это делает.

Известны механизмы управления потоками на основе меток безопасности, включающих как иерархические, так и неиерархические признаки. Эти метки ассоциируются с объектами и субъектами АС, и решение о возможности доступа (организации потока) принимается на основе анализа меток. Проиллюстрировать этот механизм можно следующим примером.

Рассмотрим описание типа

ID (I; P_1, P_2,...P_n), где

ID — идентификатор или субъекта (S_i), или объекта (F_i);

I — иерархический признак;

P_i — неиерархический признак.

Пусть иерархические признаки описывают подмножества степеней зрелости:

I – белый, зеленый, желтый, красный

II – белый, зеленый, желтый

III – белый, зеленый

IV – белый

Неиерархические признаки описывают семантику (содержание) сведений, содержащихся в объекте:

1 — манго

2 — яблоки

3 — груши

Пусть:

S_1 (II; 1, 2, 3)

S_2 (I; 2, 3)

F_1 (III; 2, 3)

F_2 (IV; 1, 2),

Что все это значит:

— субъекту S_2 доступны сведения о яблоках и грушах (неиерархические признаки 2 и 3) всех степеней зрелости — белых, зеленых, желтых и красных (иерархический признак I), но недоступны никакие сведения о манго, даже самых незрелых;

— субъекту S_1, напротив, доступны сведения обо всех фруктах, информация о которых имеется в системе, но лишь пока они зреют. Сведения о созревших («красных» — иерархический признак I) фруктах субъекту S_1 не доступны.

При этом S_1 имеет доступ и к F_1, и к F_2. Для S_2 доступен F_1, но недоступен F_2, хотя допуск S_2 значительно выше грифа F_2. Дело в том, что по совокупности неиерархических признаков S_2 имеет право доступа к сведениям, касающимся яблок и груш, но не имеет права доступа к сведениям о манго, которые содержатся в F_2.

Пусть S_1 в процессе обработки F_1 и F_2 создает объект F_3, который при этом может быть описан как:

F_3 (III; 1, 2, 3).

Таким образом, хотя допуск S_2 позволяет иметь доступ к сведениям, имеющим гриф как у F_3, но S_2 не получит доступа к F_3, т. к. множество неиерархических признаков S_2 ỳже аналогичного для F_3.

Очевидно, что такой механизм позволит контролировать потоки. Необходимым условием при этом является наличие меток безопасности и средств их обработки.

Ставя перед собой задачу обеспечения необходимого уровня защиты информации в защищенной сети при доступе в том числе и из открытой внешней сети, необходимо разработать механизмы, позволяющие осуществлять:

— назначение меток субъектам и объектам АС;

— хранение (привязку) меток в ассоциированном с субъектами и объектами виде;

— сопровождение (обработку и преобразование) меток в жизненном цикле информации.

Это, в общем-то, и есть мандатный механизм разграничения доступа.

Управление потоками информации в рамках мандатного механизма разграничения доступа, на первый взгляд, представляется достаточно громоздкой и сложной задачей. Для корректной настройки мандатного механизма необходимо проанализировать, к каким объектам обращался процесс с запросом на создание, чтение, запись, а после выполнения анализа необходимо корректно установить соответствующие метки доступа процессу и соответствующим объектам (файлам, каталогам, сетевым ресурсам и т.д.).

Процедуры анализа и установки меток доступа занимают много времени, это и есть основная причина затруднений при использовании мандатного механизма разграничения доступа.

Однако процедуры установки меток доступа и анализа, к каким объектам обращался процесс с запросом на создание, чтение, запись в рамках мандатного механизма разграничения доступа можно упростить, используя СЗИ от НСД, в которых предоставляются соответствующие механизмы автоматизации.

Так, в СЗИ от НСД «Аккорд» управление потоками информации в рамках мандатного механизма разграничения доступа осуществляется по следующему алгоритму:

1. необходимо присвоить определенную метку доступа процессу;
2. необходимо присвоить соответствующую метку доступа объектам (файлам, каталогам, сетевым ресурсам и т.д.), к которым обращается процесс с запросом на создание, чтение, запись;
3. необходимо присвоить соответствующий уровень доступа пользователю, который работает с процессом в рамках выполнения должностных обязанностей;
4. необходимо разрешить в рамках одного сеанса пользователя выполнение процедуры редактирования документов с разными метками доступа.

После выполнения описанных действий запустить процесс может только пользователь с соответствующим уровнем доступа. После запуска процесс с установленным уровнем доступа может получить доступ к объектам (данным, другим процессам) только с соответствующей меткой доступа.

Для решения проблемы редактирования документов с разными метками доступа в рамках одного сеанса пользователя в ПО ПАК «Аккорд» есть механизм автоматизации, с помощью которого администратор информационной безопасности может:

1. определить перечень задач (включая системные процессы), использование которых необходимо для выполнения должностных обязанностей пользователя КС;
2. определить объекты, к которым выполняются запросы на открытие файлов для чтения/записи (эти запросы зачастую не зависят от переменных среды, а определяются разработчиками программных пакетов).
3. назначить метку «ОБЩИЙ_РЕСУРС» информации, которую необходимо обрабатывать в рамках сеансов работы пользователей с разными уровнями доступа. Если администратор безопасности

присваивает эту метку какой-либо папке, то далее создается несколько копий этого объекта, и каждой копии присваивается одна из меток доступа прописанных в конфигурационном файле системы защиты. Имена копий различаются на один символ, а в процессе работы монитор безопасности динамически перенаправляет ввод-вывод с объекта-оригинала на копию с нужной меткой доступа;

4.предоставить пользователю выбор уровня доступа запускаемой задачи или выбор уровня конфиденциальности сеанса пользователя.

Процедура определения перечня задач и объектов доступа основана на анализе журналов регистрации событий СЗИ от НСД «Аккорд». При этом требуется высокая детальность журнала, чтобы определить, какая программа к каким объектам обращается с запросами на чтение/запись.

ПО ПАК «Аккорд» позволяет выбрать из журнала список исполняемых файлов, отследить операции чтения/записи для отдельных процессов, и сохранить в файл процессы и объекты, которым нужно присвоить метку «ОБЩИЙ_РЕСУРС», а также сформировать списки «общих» ресурсов для конкретных процессов:

- «общих» ресурсов, необходимых для работы всех пользователей,
- «общих» ресурсов, необходимых для работы отдельного пользователя,
- процессов, которые требуется запускать как в конфиденциальном, так и в общедоступном режиме.

Итак, зная основные принципы работы мандатного механизма разграничения доступа, можно достаточно просто выполнить процедуру установки мандатных меток так, чтобы:

1. осуществлять корректную работу программ с реальным выполнением дисциплины контроля потоков информации;
2. выполнять обработку документов разного уровня конфиденциальности одним набором прикладного ПО без ухудшения надежности защитных механизмов.

3. выполнять обработку информации разных уровней конфиденциальности в рамках сеансов работы пользователя с выбором уровня доступа.

3.1.2. Разграничения доступа к элементам управления

До сих пор уже неоднократно звучала мысль о том, что устройства и системы защиты информации должны работать по-разному в режиме настройки и в основном режиме – режиме контроля, управления и так далее, в зависимости от целевой функции конкретного средства защиты.

Попытка контролировать того, кто тобой управляет, отражает идеалы демократии, но кажется довольно нереалистичной. Вы могли уже не раз слышать в тех или иных контекстах о невозможности (нецелесообразности) защищаться от администратора.

Рассмотрим этот вопрос чуть подробнее.

Итак, одновременно актуальны следующие посылки относительно средства защиты информации.

1) СЗИ должно реализовывать свои ограничительные функции так, чтобы те субъекты, действия которых они ограничивают, не могли повлиять на эти ограничения.

2) СЗИ должно быть управляемым – адаптируемым к изменениям задач.

3) СЗИ должно быть управляемым только со стороны лиц, уполномоченных владельцем системы (это означает простую вещь – производитель не должен иметь возможность влиять на работу своих средств в чужой системе, кроме случаев, когда его уполномочивает владелец системы).

Все это недвусмысленно говорит о том, что любое средство защиты информации должно так или иначе содержать собственную подсистему разграничения доступа, управляющую полномочиями пользователей

этого средства в отношении использования функций этого средства. Проще говоря, разграничивающее доступ к функциям СЗИ пользователей и администраторов – управляющего персонала.

Общая логика разграничения просто – пользователь не управляет функциями СЗИ, а администратор – управляет.

Однако если остановиться на этой общей логике, то окажется, что администраторы имеют неограниченные (в рамках функциональности конкретного СЗИ, разумеется) возможности – они могут получать любой доступ к любым ресурсам пользователя, а самих пользователей могут в любой момент их прав лишить.

Часто производители средств защиты преподносят такое положение дел как нормальное, относя так называемую «проблему суперпользователя» к неизбежным проблемам уровня «человеческого фактора» и предлагая решать ее организационными мерами.

Однако, как мы помним, корректно реализованное средство разграничения доступа должно давать возможность реализовать любую непротиворечивую политику безопасности.

Первое, что для этого необходимо сделать – это разделить функции управления на несколько ролей.

Здесь важно не путать организационно-штатные мероприятия – делегирование разных должностных обязанностей и полномочий системному администратору и администратору безопасности информации (сотрудникам компании), и права доступа, назначаемые тем или иным субъектам доступа.

Действительно, предпосылкой, без которой система разграничения доступа не будет выполнять своих задач, является, как и прежде, осознание и вербальное выражение того, кому что можно, и что нельзя делать. Но, для того чтобы дальше это вербальное описание превратилось в настройки средства защиты информации, средство защиты информации должно предоставлять возможность ограничивать права управляющего персонала.

Фактически, это самое главное, так как многие средства защиты информации этого не предполагают в принципе. Есть разграничение пользователя и администратора, при этом администраторы могут (и должны) назначать права пользователям, а у самих администраторов права установлены по умолчанию и не меняются, так как они объявлены заведомо доверенным пользователем.

Разберем, в чем следует ограничивать управляющий персонал и каким образом это можно сделать.

1) Самое очевидное, в чем следует ограничить администратора – это *в доступе к ресурсам пользователей*. Казалось бы, для этого достаточно, чтобы этих прав не было в наборе администратора по умолчанию, и возможность настройки его прав на ситуацию не влияет. Например, при авторизации в СДЗ пользователя – после успешного завершения контрольных процедур будет производиться загрузка ОС, а загрузка системы администрирования СДЗ – не будет. А в случае авторизации администратора – будет производиться загрузка системы администрирования СДЗ, а загрузка ОС производиться не будет. Казалось бы, таким образом вопрос с доступом администратора к ресурсам ОС исчерпан. Однако администратор, не ограниченный в правах, может завести для себя учетную запись пользователя и пользоваться ею. Если же функции заведения пользователя и назначения ему прав разнесены по разным администраторам, то для реализации такой возможности попасть в ОС злоумышленнику потребуется сговор, что, как говорится, уже другая статья.

2) Второе, менее очевидное – это необходимость *разделения функций управления и функций контроля*. Они кажутся очень близкими и имманентными самому понятию «управляющий персонал». Однако хорошо понятно, что когда права формулирует, задает в форме настроек, контролирует корректность этих настроек и их неизменность, а также и результаты их применения, отображаемые в журналах событий – один и

тот же человек, и он же осуществляет операции архивирования и очистки журналов – ситуация даже на слух уже не кажется защищенной. А из этого перечня уже устранены операции, связанные с заведением пользователей и формированием их вычислительной среды (об этом разделении – администратора и администратора безопасности информации идет речь в предыдущем пункте).

Значит, роли персонала, управляющего безопасностью информации тоже должны быть разделены на роли с разным набором функциональных задач и связанных с ними возможностей.

Первый из описанных пунктов осмыслен в мире более отчетливо и даже имеет название – «проблема суперпользователя». Второй же преимущественно в отраслевых стандартах и нормативных методических документах (в первую очередь это нормативная методическая база Банка России), однако и ему можно дать наименование в той же парадигме – «проблема супербезопасника».

Рассмотрим их по порядку.

3.1.2.1. Победить суперпользователя

Проблема суперпользователя интересна нам с вами потому, что она не решается встроенными средствами разграничения доступа, а решается только наложенными. Это известно с конца XX века, однако эксперименты в этой области продолжаются до сих пор. Разберем, почему все так.

Встроенные и наложенные средства разграничения доступа – это относительно новая терминология ФСТЭК России, разделяющая средства разграничения доступа, встроенные в ОС или другое прикладное либо инфраструктурное программное обеспечение (в ПО виртуализации, в ПО Active Directory), и средства разграничения доступа, устанавливаемые в систему специально – как часть подсистемы защиты информации. Вообще говоря, как минимум после установки в систему они тоже сразу становятся встроенными, поэтому с этими

понятиями возникает некоторая путаница, но по мере привыкания к терминологии она возникает все реже. Запомнить разницу легко: встроенные – это те, что были изначально в ПО, а наложенные – те, что устанавливаются потом, специально.

Первое же, что из этого вытекает – встроенные средства разграничения доступа разрабатываются не разработчиками средств защиты информации, а разработчиками совершенно других продуктов. Причем в этих продуктах собственно эти встроенные средства выполняют маленький до незаметности объем функций, да еще и не целевых для этого ПО. Приоритетом разработчиков ОС, ПО виртуализации, баз данных, прикладного ПО – всегда будет закономерно оставаться эффективность выполнения целевых функций ПО и их доступность. Все, что может на них негативно повлиять, всегда будет минимизироваться, это очевидно. Это дает косвенную улику, опираться на которую, конечно, можно только неформально, в пользу того, что с точки зрения собственно защитных свойств наложенные средства, скорее всего, эффективнее.

Однако в отношении проблемы суперпользователя как раз этот фактор оказывается решающим: эта проблема принципиально не может быть решена техническими мерами на уровне встроенных средств.

Целевая, функциональная система не может проектироваться без суперпользователя, это повлекло бы за собой риск полной утраты работоспособности в случае наступления нештатной ситуации, требующей каких-то радикальных мер – например, необходимости внеплановой смены управляющего персонала, каких-то аварий и тому подобных. Поэтому суперпользователь в системе есть всегда.

Разумеется, нужен он и в наложенных средствах. Но в правильно спроектированных наложенных средствах таким «суперпользователем», как правило, является администратор нештатного режима, и для того, чтобы загрузить систему под этой учетной записью, необходимо участие

сразу нескольких администраторов (в общем случае – администратора и администратора безопасности информации).

Рассмотрим на примере задачи разграничения доступа к функциям управления виртуальных сред. Администратор виртуальной инфраструктуры (АВИ) имеет максимальный уровень доступа ко всем объектам (включая, разумеется, виртуальные машины (ВМ)) и функциям управления информационной системы.

Нет никакой встроенной в среду виртуализации роли, которая могла бы ограничивать действия АВИ: запрещать критичные для безопасности действия (например, случайное или умышленное переключение ВМ из подсети ограниченного доступа в подсеть к общедоступным или миграция ВМ на другое хранилище, где ей храниться не положено), а некоторые разрешать только по согласованию (например, удаление виртуальной машины или ее экспорт на диск).

Если вы внимательно читали предыдущий параграф, вы помните, что роли – это не единственный способ разграничения доступа, можно прибегнуть к мандатному механизму и ограничить нежелательные действия назначением меток. Но встроенных мандатных механизмов разграничения доступа в виртуальных средах нет, а инструментов сетевого сегментирования (VLAN или межсетевые экраны) недостаточно в случае, если необходимо обеспечить не только изоляцию сети, но и изоляцию среды обработки информации и средств ее хранения.

Когда задачу невозможно решить техническими мерами, ее решают организационными.

Организационные меры выглядят примерно так.

Для поддержания режима действий «по согласованию» с АБИ создается учетная запись АВИ с урезанными правами, а учетные данные «суперпользователя» (настоящего полноценного АВИ) запечатываются

в конверте и прячутся в сейф до возникновения нештатных ситуаций. Тогда и осуществляется – в физическом мире, путем переговоров людей – это самое согласование с АБИ, после чего согласованное действие выполняется под учетной записью «из конверта».

Это, конечно, не решение. Чаще всего обращение к «конверту», особенно в крупных инфраструктурах, происходит постоянно.

С сегментированием организационными мерами дело обстоит не лучше. Вариантов два:

1) Полное физическое разделение, то есть под каждый сегмент (например, ВМ бухгалтерии и ВМ юридического отдела, а также ВМ с общедоступными данными и данными ограниченного доступа для каждого подразделения (где это разделение есть)) выделить отдельные сервера, не имеющие связи между собой (чтобы АВИ не имел физической возможности смешать ВМ разных сегментов).

Минус такого подхода очевиден – серверов получается немыслимо много, использоваться они будут нерационально, балансировка нагрузки практически исключена, а отказоустойчивость снижена.

2) Можно не делить серверы, но для каждого сегмента сделать отдельную учетную запись АВИ, которой выделить права только в отношении «своего» сегмента. В этом случае резко возрастает число учетных записей АВИ. Значит, либо будет раздуваться штат администраторов, что вряд ли, так как это дорого и неудобно, либо, что более вероятно, выполнять функции всех этих АВИ будет один и тот же человек, которому будет сложнее отслеживать состояние всей системы целиком, зато очень просто во всех этих учетных записях запутаться.

Очевидно, что встроенными средствами задача не решается. Возможно ли решить ее наложенными, рассмотрим ниже на основе работы [4].

В большинстве виртуальных систем можно выделить следующие составные части (рис. 3.1):

1. серверы виртуализации;
2. виртуальные машины;

3. сервер управления виртуальной инфраструктурой;
4. система хранения данных;
5. АРМ администраторов;
6. рабочие места пользователей виртуальной инфраструктуры;
7. сеть передачи данных.

Центральным элементом виртуальной инфраструктуры являются серверы виртуализации с установленным на них гипервизором. Гипервизор – это программа, создающая среду функционирования других программ (в том числе других гипервизоров) за счет имитации аппаратных средств вычислительной техники, а также управления этими средствами и гостевыми операционными системами, функционирующими в данной среде (см. рис. 3.1).

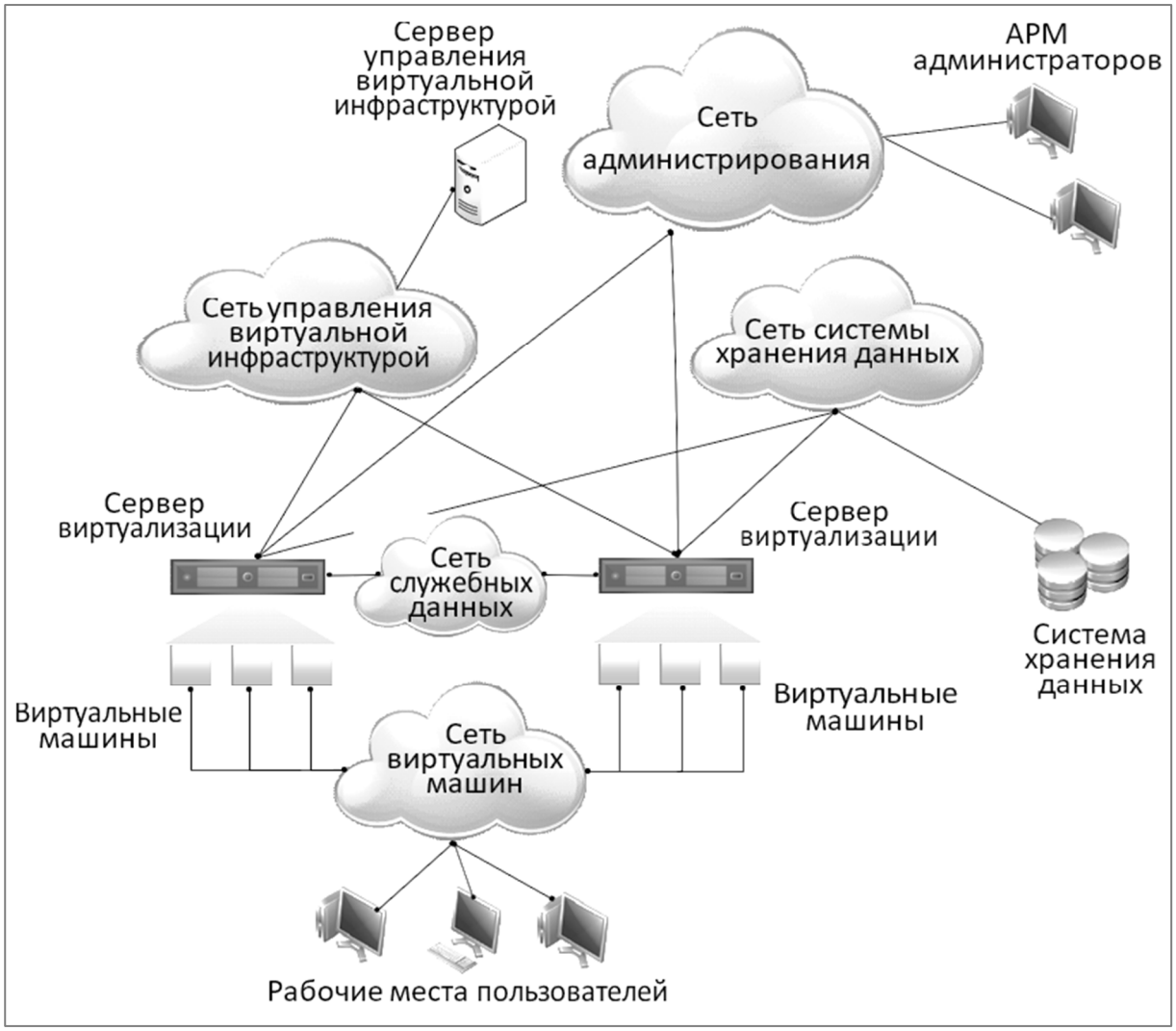


Рис. 3.1. Архитектура виртуальной инфраструктуры

Сами виртуальные машины представляют собой набор файлов, хранящих конфигурацию оборудования, образы жестких дисков и снапшоты (мгновенные снимки виртуальной машины). Виртуальные машины обычно хранятся в общих для серверов виртуализации хранилищах данных, что позволяет им свободно перемещаться для распределения нагрузки и обеспечения отказоустойчивости.

Сервер управления виртуальной инфраструктурой позволяет управлять всеми элементами системы: серверами виртуализации, виртуальными машинами, сетевыми хранилищами и сетью.

В зависимости от обрабатываемых данных и их назначения выделяют несколько видов сетей. Для организации доступа администраторов к объектам виртуальной инфраструктуры

используется сеть администрирования, по ней осуществляется передача управляющих команд от клиента с рабочего места администратора к серверу управления виртуальной инфраструктурой или серверу виртуализации.

Запрос на доступ представляет собой информационный поток, и в свете вышеописанных сложностей с разграничением доступа в виртуальной среде, представляется логичным спроектировать наложенное средство на основе контроля информационных потоков.

Администрирование виртуальной инфраструктуры производится с рабочих мест администраторов с помощью специального клиента, который подключается к серверу управления виртуальной инфраструктурой или отдельным серверам виртуализации через сеть администрирования. Таким образом, для перехвата и управления информационными потоками необходимо расположить между рабочими местами администраторов и сервером управления (серверами виртуализации) сервер контроля информационных потоков (прокси-сервер).

Для клиента управления прокси-сервер представляется сервером управления виртуальной инфраструктурой и устанавливает защищенное SSL-соединение. Затем прокси-сервер соединяется с сервером управления и, представляясь ему клиентом, устанавливает второе соединение. Таким образом, мы получаем возможность перехватывать и расшифровывать трафик, посылаемый с клиента на сервер управления.

Полученное после расшифровки HTTP-сообщение поступает в модуль принятия решения о предоставлении доступа, в котором оно анализируется, выделяется информация, необходимая для принятия решения, и на ее основе принимается решение о предоставлении или отказе в доступе инициатору в установлении доступа к целевому объекту. После либо запрос передается целевому объекту, либо инициатору посылается сообщение об отказе в доступе (рис. 3.2).

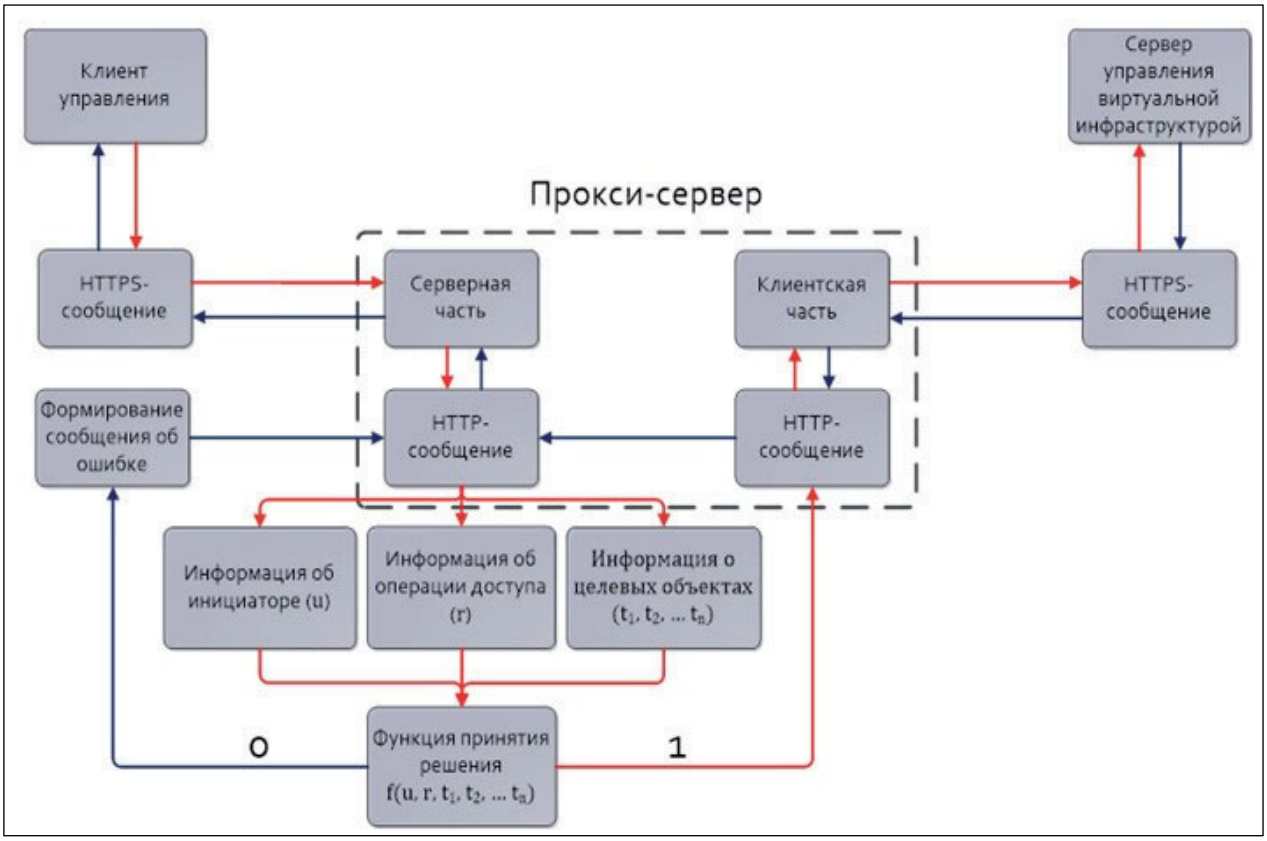


Рис. 3.2. Структура модуля управления доступом

Построенное таким образом средство разграничения доступа к функциям управления VMware vSphere разработки ОКБ САПР называется «Сегмент-В.» («В.» – это отсылка к слову «виртуализация» и к идиоме «Посторонним В.» (вывеска, под которой жил Пятачок)).

С точки зрения Сегмента-В., vCenter является внутренним элементом по отношению к ВИ, а администратор ВИ внешним.

Принципиальная схема выглядит следующим образом (рис. 3.3):

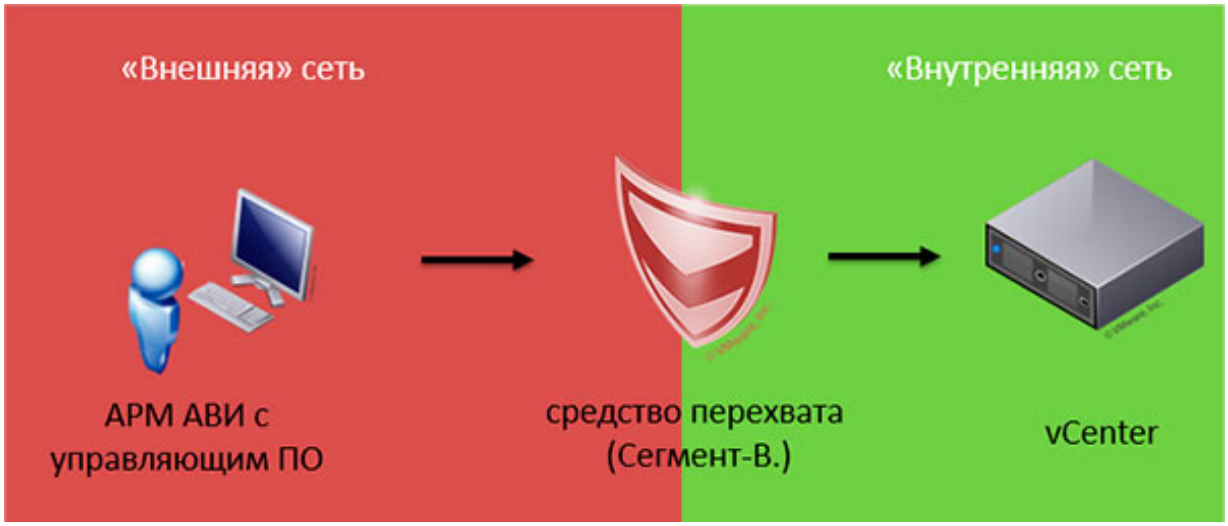


Рис. 3.3. Размещение Сегмент-В.

Применение продукта требует дополнительной настройки ВИ так, чтобы все запросы к vCenter и ESXi проходили через Сегмент-В. (рис. 3.4).

Рис. 3.4. Настройка маршрутизации

Контролировать все возможные действия пользователей не имеет смысла. Более того, избыточность функционала усложняет работу с ПО. Интерес представляют в первую очередь действия, выделяемые регулятором + специфичные функции конкретных платформ, которые

не учтены регулятором (например, lockdown mode). По результатам анализа нормативной базы (17 и 21 приказов ФСТЭК России) и всех функций в API vClient было выделено 23 операции:

Вход

1) Вход в систему (вход в систему по паролю или с учетными данными текущей сессии)

ВМ

2) Доступ к файлам ВМ (просмотр хранилища и файлов виртуальных машин на нем)
3) Удаление ВМ (удаление ВМ и ее файлов с диска)
4) Создание ВМ (создание, импорт, а также добавление в инфраструктуру ВМ)
5) Запуск ВМ/vApp
6) Останов ВМ/vApp (выключение, suspend, перезапуск ВМ/vApp)
7) Создание копий ВМ (клонирование в ВМ/шаблон, разворачивание ВМ из шаблона)
8) Изменение конфигурации ВМ/vApp
9) Доступ к консоли ВМ (доступ к консоли — экрану ВМ по VNC)
10) Контроль подключаемых к ВМ устройств (контроль подключаемых к ВМ USB, CD, FDD)
11) Экспорт ВМ (экспорт ВМ в OVF формат)
12) Миграция ВМ (миграция/перемещение ВМ со сменой хоста и/или хранилища)

Сетевые устройства

13) Работа с сетью (изменение настроек сети хоста и сетевых устройств: свитчей, групп портов и их распределенных вариантов)

Хосты

14) Базовые операции с хостом (запуск, остановка, перезапуск, подключение, отключение, maintenance mode хоста)

15) Работа со службами хоста (запуск, остановка, перезапуск сервисов хоста)

16) Изменение настроек сетевого экрана (открытие, закрытие портов, ограничение диапазона IP)

17) Работа с Lockdown Mode (включение, отключение lockdown mode)

18) Конфигурация автостарта (включение, отключение автостарта, изменение порядка запуска ВМ)

19) Настройка DNS и маршрутизации хоста (настройка DNS и маршрутизации хоста)

20) Настройка домена на хосте (ввод сервера в домен и вывод из него)

21) Настройка времени на хосте (ручное изменение времени, добавление NTP сервера, включение и отключение NTP сервиса)

Снапшоты

22) Работа со снапшотами (создание, откат — к предыдущему состоянию и удаление снапшотов)

Роли

23) Управление правами (управление ролями, назначение и удаление прав)

Рассмотрим, как это можно использовать.

Например, владелец хочет организовать свою инфраструктуру так, чтобы не смешивались ресурсы, относящиеся к разным категориям (условно «автобусы» и «троллейбусы»), не нарушались уровни конфиденциальности разных ресурсов, и операции по переносу ВМ из одной подсети в другую могли осуществлять не все администраторы, а только специально уполномоченные.

Предположим, что администратор хочет перенести виртуальную машину из одной подсети в другую, то есть изменить для ВМ «А» сеть с «сеть1» на «сеть2».

Эту операцию можно произвести, если

- этот администратор, эта ВМ и эта сеть вообще легальные,

- если этому администратору вообще можно работать с сетью,

- этому администратору можно работать с сетью, предназначенной для данных, связанных, допустим, с троллейбусами (сетью категории «троллейбусы»)

- можно работать с виртуальными машинами, обрабатывающими данные, например, об «автобусах» (категории «автобусы»),

- можно работать с виртуальными машинами этого уровня (например, «конфиденциально», или «уровень 3»).

Плюс могут быть еще дополнительные ограничения, при которых операция может производиться только если все ее участники (и субъекты и объекты) полностью совпадают и по категориям, и по уровням. То есть, например, категория «автобусы» должна характеризовать и «сеть2», и ВМ «А», и быть назначена администратору (что логично, зачем переносить ВМ про автобусы в сеть про троллейбусы?!), и все трое должны иметь «уровень 3», ни больше, ни меньше.

Как это будет протекать в системе. Администратор попытается осуществить действие. Прокси-сервер получит пакет, из которого узнает:

* субъект (администратор)

* объекты (ВМ «А» и «сеть2»)

* действие (изменение сети ВМ – это действие из группы «работа с сетью»)

Блок принятия решения начнет проверку:

1. Зарегистрирован ли субъект в Сегмент-В.?

Если нет, то блокируем.

2. Зарегистрированы ли объекты (ВМ «А» и «сеть2») в Сегмент-В.? Т.е. назначен ли им уровень? Если нет, то блокируем.

3. Выше или равен уровень субъекта уровню каждого из объектов (ВМ «А» и «сеть2»)? Если нет, то блокируем.

4. Все ли категории, которые назначены объектам, есть у субъекта? Если нет, то блокируем.

5. (Если включена опция проверки уровня сессии) Одинаковый ли уровень у всех объектов? Если нет, то блокируем.

6. (Если включена опция проверки категорий сессии) Есть ли общие категории у всех объектов, участвующих в операции? Если нет, то блокируем.

7. Разрешено ли субъекту выполнять действие? Т.е. будет проверено, стоит ли для субъекта разрешение на работу с сетью. Если нет, то блокируем.

8. Разрешаем выполнение действия.

Из этого примера мы видим, что тот факт, что тот или иной пользователь является администратором инфраструктуры виртуализации, еще не дает ему каких-то сверхполномочий, он остается вполне управляемым.

Хотя каждая формула уменьшает аудиторию книги вдвое, аудитория этой книги не совсем обычная, поэтому рискнем и формализуем изложенное выше.

Решение о предоставлении доступа принимается на основе предиката предоставления доступа. Введем следующие обозначения:

пусть U – множество пользователей, R – множество операций, O – множество объектов доступа, $u \in U$ _ инициатор запроса, $r \in R$ _ запрашиваемое действие; $T \subset O$ _ множество целевых объектов для данной команды.

1. Иерархические метки:

(I; ≤)– шкала уровней доступа к информации, на основе иерархических меток;

level: U ⟶ I – функция уровней доступа пользователей;

level: O ⟶ I – функция уровней конфиденциальности объекта.

2. Неиерархические метки:

L – множество неиерархических меток, L_U – множество неиерархических меток, принадлежащих пользователю u; L_t – множество неиерархических меток, принадлежащих объекту t, где t ∈ T.

3. Предикат «операция доступа разрешена».

M – матрица доступов, A ⊂ R, A = M[u, t]; A – множество разрешенных пользователю u операций над объектом t.

То есть если r ∈ A, то операция считается разрешенной. Таким образом, предикат «операция доступа разрешена» записывается:

$$f_D(r,u,T) = \bigwedge_{t \in T} D(r,u,t), \text{ где:}$$

$$D(r,u,t) = \begin{cases} 1, & r \in M[u,t]; \\ 0, & r \notin M[u,t]. \end{cases}$$

4. Предикат «поток типа “субъект-объект” разрешен».

Поток типа «субъект-объект» называется разрешенным, если:

1) Уровень иерархической метки инициатора не ниже уровня метки объекта;

2) Множество неиерархических меток объекта является подмножеством неиерархических меток пользователя

$$f_{SO}(u,T) = \bigwedge_{t \in T} f_{SO}(u,t) = \bigwedge_{t \in TF} \{ I_{SO}(u,t) \wedge L_{SO}(u,t) \}, \text{где:}$$

$$I_{SO}(u,t) = \begin{cases} 1, & level(u) \geq level(t); \\ 0, & level(u) < level(t). \end{cases} \qquad L_{SO}(u,t) = \begin{cases} 1, & L_t \subset L_u; \\ 0, & L_t \not\subset L_u. \end{cases}$$

5. Предикат «поток типа “объект-объект” разрешен».

Поток типа «объект-объект» называется разрешенным, если выполняется требование информационного невлияния [5], то есть все объекты, участвующие в нем, имеют одинаковые уровни доступа.

Поэтому предикат «поток типа “объект-объект” разрешен» будет записан:

$$f_{OO}(u,T) = \bigwedge_{t_i,t_j \in T} I_{OO}(t_i,t_j), \text{где:}$$

$$\text{Для } \forall i,j : t_i,t_j \in T,\ t_i \neq t_j \ \rightarrow I_{OO}(t_i,t_j) = \begin{cases} 1, & level(u) = level(t); \\ 0, & level(u) \neq level(t). \end{cases}$$

Команды управления могут относиться к нескольким объектам или использовать их в качестве параметров. Для каждого объекта данной операции по отдельности решается, будет предоставлен доступ или нет. Если хотя бы для одного объекта команды доступ запрещен, запрещается исполнение всей команды. Для каждой тройки инициатор-объект-операция доступ разрешается при истинности трех предикатов: предиката «операция доступа разрешена», предиката «поток типа “субъект-объект” разрешен» и предиката «поток типа “объект-объект” разрешен».

Предикат предоставления доступа записывается:

$f(r, u, T) = fD(r, u, T) \wedge fOO(u, T) \wedge fSO(u, T)$, то есть доступ предоставляется, если потоки типа «субъект-объект» и «объект-объект» являются разрешенными и операция доступа разрешена в матрице доступов.

К сожалению, есть ряд операций, для которых невозможно получить сведения об объекте, с которым производится действие, поэтому разграничить доступ к ним нельзя. Такие действия можно только либо всегда разрешать, либо всегда запрещать. Те из них, что были определены как потенциально опасные, приходится всегда запрещать:

- Полное [delete] удаление папок/vApp (включая ВМ внутри),
- Экспорт vApp,
- Клонирование vApp.

Разумеется, это не значит, что выполнить эти операции невозможно совершенно. Здесь помогает как раз разделение ролей

администратора инфраструктуры и администратора безопасности. Выполнить запрещенные операции можно, переведя систему в «мягкий режим» (где запрещенные действия фиксируются, но пропускаются). Перевести систему защиты в «мягкий режим» может только АБИ, а выполнить саму операцию (допустим, удалить папку) – только администратор. Таким образом, ни один из них не сделает этого на основании собственного единоличного решения.

Функции системных администраторов и администраторов безопасности информации разделены во всех продуктах ОКБ САПР, в которых это может иметь хоть какой-то смысл.

3.1.2.2. Победить супербезопасника

Из описания того, как можно управлять полномочиями администраторов с помощью «Сегмент-В.» уже проглядывает принципиальный подход к тому, как можно решить проблему «супербезопасника». Если можно вводить роли управляющего персонала с различными наборами прав (а почему, собственно, это должно быть нельзя?), то можно и распределить управляющие функции между несколькими ролями, реализованными в том или ином продукте по умолчанию, если сама концепция продукта предусматривает такую стратегию.

Примеры ролевой структуры, тесно связанной с замыслом продукта, вы увидите ниже, когда речь пойдет о концепциях продуктов линейки «Секрет» и программно-аппаратном неперезаписываемом журнале ПАЖ.

Здесь в качестве примера лучше всего подойдет продукт «Система удаленного централизованного управления СЗИ НСД “Аккорд”» (СУЦУ). Как видно из названия, это система принципиально управляющая, по самому своему предназначению. Причем, управляющая СЗИ НСД. То есть именно инструмент «супербезопасника».

СУЦУ работает, вкратце, так. В систему вводится сервер Управления СУЦУ (один или два – основный и резервный), на котором запускается

и работает управляющее ПО. Разумеется, он защищен так, как должен быть защищен сервер. Если нужно, он входит в некоторую иерархию серверов – в зависимости от архитектуры управления информационной системой, на этот сервер могут оказывать управляющие воздействия сервера более высокого уровня централизации (например, если сервер Управления СУЦУ управляет ИС на уровне региона, а есть еще централизация на уровне страны), сервера СКУД, сервера систем BI (Business Intelligence, погуглите, что это такое, если это понятие вам пока незнакомо). Сейчас оставим эти вопросы в стороне и вернемся к ним в одном из следующих разделов.

Непосредственно на сервере Управления СУЦУ никто не работает (обычно это физический сервер, он стоит в стойке в серверной комнате), управляющий персонал работает с управляющим ПО в режиме терминального доступа со своих АРМ (они так и называются АРМ управляющего персонала).

На те компьютеры, средствами защиты на которых СУЦУ управляет, устанавливается ПО «агент СУЦУ», которое обеспечивает передачу управляющих команд с сервера и передачу журналов и других данных в случае необходимости (например, данные о смене пароля в СДЗ) – на сервер Управления.

«Система сдержек и противовесов»[25] организована в СУЦУ так.

В ней реализованы 6 ролей, одни из которых должны выполнять сотрудники подразделений информатизации (условно «системные администраторы»), а другие – сотрудники подразделений безопасности (условно «АБИ»). Одна из этих ролей – «суперпользователь» – Администратор нештатного режима – должна быть по возможности групповой и выполняться сотрудниками обоих подразделений – системным администратором и безопасником, вместе. Оговорка «по

[25] Система сдержек и противовесов – это механизм реализации в политической системе демократического государства принципа разделения властей (законодательной, исполнительной и судебной).

возможности» требуется потому, что мы а) не можем, вообще говоря, проследить за тем, как будет действовать эксплуатирующая организация, б) в организации просто не всегда есть достаточно сотрудников, и тогда нашими рекомендациями, скорее всего, пренебрегут. Но имеет смысл хотя бы сообщать, как должно быть.

Кроме разделения на информатизацию и безопасность, роли разделены еще на те, что выполняют функции непосредственно управления и те, что занимаются контролем функционирования и мониторингом.

Итак, ролевая структура СУЦУ выглядит следующим образом (рис. 3.5).

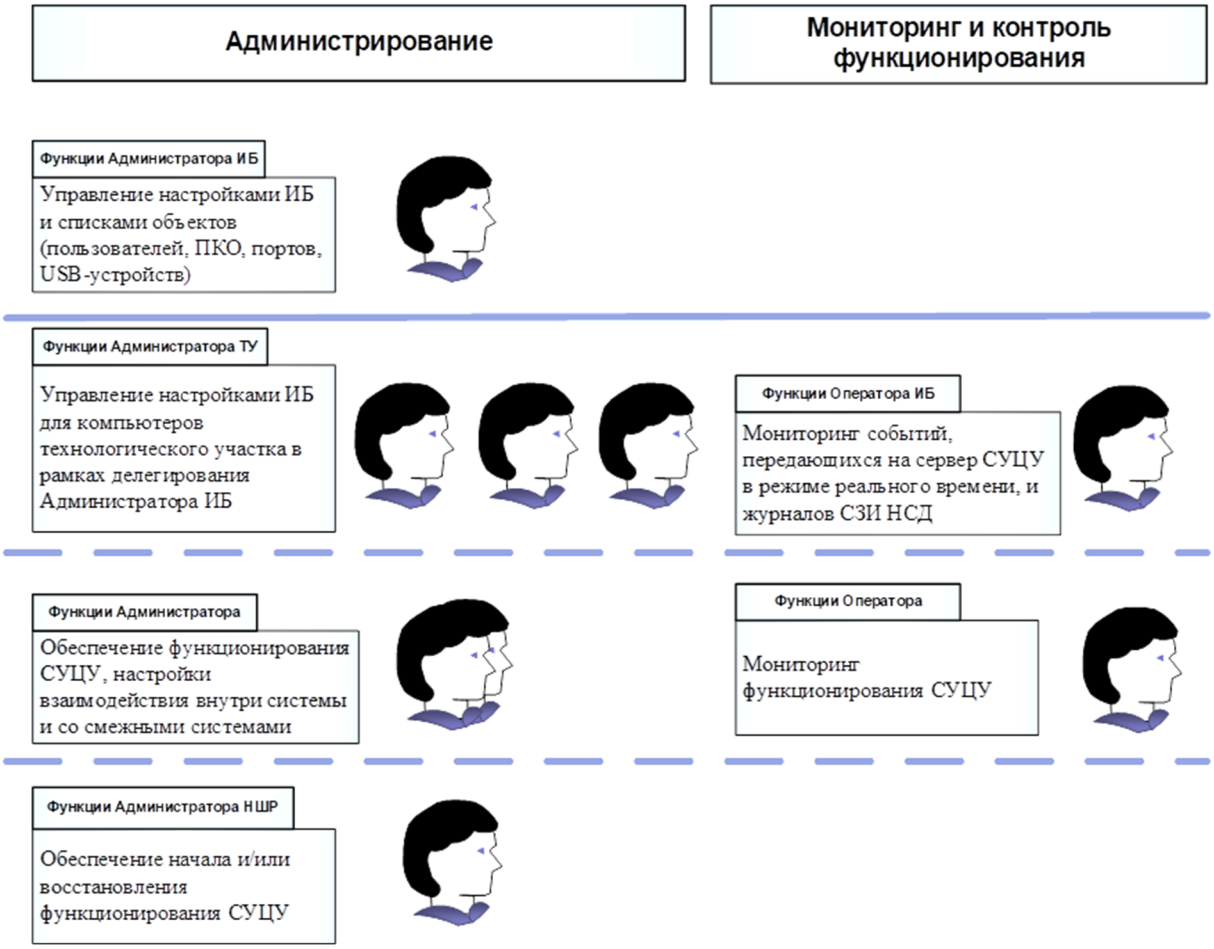


Рис. 3.5. Роли СУЦУ

Администратор СУЦУ, сотрудник подразделения информатизации. Функции роли: установка ПО СУЦУ, обеспечение общего

функционирования комплекса технических средств (КТС[26]) и ПО СУЦУ, формирование списков пользователей, подконтрольных объектов, баз контролируемых устройств, установка сетевых и других настроек взаимодействия, обновление ПО СУЦУ, и так далее (полный список функций каждой роди для справки – в таблице ниже).

Администратор ИБ СУЦУ, сотрудник подразделения безопасности информации. Функции роли: управление настройками СЗИ НСД на подконтрольных объектах, управление учетными записями управляющего персонала СУЦУ, в том числе, делегирование функций Администраторам ИБ Технологических участков. Идея в том, что вся система делится на участки, в каждом из которых настройками СЗИ НСД управляет отдельный Администратор ИБ (АИБ). И то, в какой мере он может ими управлять самостоятельно, – определяет АИБ СУЦУ. Он может делегировать все функции относительно тех подконтрольных объектов, что формируют участок, а может какие-то оставить только за собой, например. АИБ ТУ не может никак воздействовать на настройки безопасности других участков, а АИБ СУЦУ может управлять настройками СЗИ НСД на любом компьютере системы.

Оператор СУЦУ, сотрудник подразделения информатизации. Функции роли: мониторинг функционирования СУЦУ. Проще говоря, он убеждается, что на всех подконтрольных объектах заработали агенты СУЦУ, все они обнаруживаются сервером СУЦУ, и если не все – то чинит.

Оператор ИБ СУЦУ, сотрудник подразделения безопасности информации. Функции роли: мониторинг событий, передающихся на сервер в режиме реального времени, а также действия с журналами СЗИ НСД, которые необходимо по тем или иным причинам выполнить не по регламенту автоматически, а вручную (например, если конвертация и отправка журналов в смежную систему по регламенту –

[26] Это очень полезная аббревиатура, крайне желательно ее запомнить.

раз в сутки, а почему-либо необходимо сделать отправку дополнительно в другое время).

Администратор ИБ технологического участка, сотрудник подразделения безопасности информации. Функции роли: управление настройками СЗИ НСД в том объеме, в котором делегировал Администратор ИБ СУЦУ для всех подконтрольных объектов соответствующего участка.

Администратор нештатного режима функционирования СУЦУ, в идеале групповая роль. Функции роли: обеспечение начала и/или восстановления функционирования СУЦУ. Выполняет функции только в сервисном и нештатном режимах работы Системы.

При начальной настройке СУЦУ Администратор нештатного режима функционирования в рамках сервисного режима функционирования назначает пользователей, выполняющих роли Администратора СУЦУ и Администратора ИБ СУЦУ. В свою очередь Администратор ИБ СУЦУ назначает пользователей, выполняющих роли персонала ИБ СУЦУ: Оператора ИБ, АИБ технологического участка.

Кроме того, Администратор ИБ делегирует полномочия администраторам ИБ соответствующих технологических участков.

Оператор СУЦУ не имеет собственной учетной записи в ПО СУЦУ, поэтому его назначение – это организационный процесс, специальной учетной записи «Оператор СУЦУ» в ПО СУЦУ не создается.

Для понимания главной идеи – разделения функций безопасников между разными людьми во избежание излишней концентрации власти в одних руках – описанного достаточно, но для более детального представления в таблице 3.1 приведены все основные функции всех ролей.

Таблица 3.1. Функциональные обязанности ролей СУЦУ.

Роль	Функциональные обязанности
Администратор	Установка компонентов Системы. Обеспечение взаимодействия и функционирования технических и программных средств Системы. Поддержка функционирования КТС Настройка механизмов взаимодействия между СУЦУ и смежными системами. Установка обновлений ПО СУЦУ. Формирование списка пользователей Системы. Регистрация АРМ и серверов в качестве участников информационного обмена в централизованной базе Сервера Управления (формирование базы подконтрольных объектов). Формирование базы USB-устройств Системы
Администратор ИБ	Настройка политик безопасности. Настройка правил доступа к коммутационным портам и периферийным устройствам. Настройка механизмов взаимодействия между СУЦУ и ядром СОИБ (если оно есть) в части задания параметров фильтрации событий ИБ, зарегистрированных на подконтрольных объектах, при передаче в ядро СОИБ Управление учетными записями персонала (назначение пользователей, выполняющих роли персонала СУЦУ). Контроль управляющего воздействия на компоненты СУЦУ в части: - изменения настроек (включая настройки мониторинга); - применения шаблонов настроек. Формирование шаблонов настроек для СЗИ от НСД, управляемых по децентрализованной схеме. Формирование логических групп из серверов и АРМ (технологических участков). Формирование групповых политик для управления СЗИ от НСД. Контроль состояния ИБ путем просмотра журналов событий. Участие в разборе и устранении нештатных ситуаций, связанных как с работой СУЦУ, так и с работой средств защиты информации от НСД

Роль	Функциональные обязанности
Оператор	Обеспечение мониторинга взаимодействия и функционирования технических и программных средств Системы. Установка контроллера ПАК СЗИ от НСД «Аккорд-АМДЗ» в свободный слот ПЭВМ подконтрольного объекта. Регистрация нештатных ситуаций на КТС Системы, КТС смежных подсистем, на которых размещены компоненты СПУМ, или каналах их взаимодействия и уведомление о них администратора СУЦУ
Оператор ИБ	Обеспечение мониторинга состояния ИБ в части защиты от несанкционированного доступа средствами Системы или ядра СОИБ. В случае выявления фактов несанкционированного доступа, Оператор информационной безопасности СУЦУ сообщает о них администратору информационной безопасности СУЦУ. Регулярное создание отчетов о зафиксированных событиях ИБ СУЦУ, выгрузка их в общепринятые форматы и уведомление о результатах Администратора ИБ
Администратор ИБ технологического участка	Настройка политик безопасности. Настройка правил доступа к коммутационным портам и периферийным устройствам. Создание ролей Системы и определение пользователей (в случае делегирования функций Администратором ИБ). Формирование шаблонов настроек для СЗИ от НСД, управляемых по децентрализованной схеме. Формирование групповых политик для управления СЗИ от НСД. Контроль состояния ИБ путем просмотра журналов событий. Участие в разборе и устранении нештатных ситуаций, связанных как с работой СУЦУ, так и с работой средств защиты информации от НСД
Администратор нештатного режима	Проведение мероприятий по восстановлению работоспособности Системы и компонентов СУЦУ на объектах защиты в случаях сбоев и аварийных ситуаций. Выполнение функций только в нештатном режиме работы Системы. В случае необходимости может выполнять любые функции ASM

3.1.2.3. Режим «4 глаза»: работа с контролером

Некоторые задачи, выполняемые пользователями информационных систем, по тем или иным причинам настолько важны, что должны обязательно выполняться не в одиночестве, а под присмотром другого человека. Вы, вероятно, сталкивались с такими действиями в коммерческих банках, когда для того, чтобы отключить или подключить какую-то услугу, оператор зовет другого сотрудника и он каким-то способом подтверждает, что он все видел (как правило, прикладывает ТМ-идентификатор или карту).

Такой режим называется «работа с контролером» или «режим четырех глаз». Кстати, это не всегда именно операции на компьютере – в некоторых организациях нельзя, например, по одному заходить в некоторые помещения.

Здесь дьявол, как водится, в деталях. То, как должна строиться работа в таком режиме, очень сильно зависит от функционального ПО, в котором выполняются критичные функции, от того, подтверждение какой степени вовлеченности в процесс требуется от контролера, словом – от множества обстоятельств, специфичных для конкретной информационной системы. А это означает, что в хорошем средстве разграничения доступа параметры этого режима должны быть настраиваемыми. Должно быть возможно настраивать, например,

- кто первый должен идентифицироваться – пользователь или контролер,

- должен ли контролер постоянно находиться рядом с компьютером при работе пользователя, или только санкционировать его работу (для того, чтобы контролер находился рядом постоянно, можно, например, разрешать выполнение действий только при прислоненном идентификаторе контролера, а если этим идентификатором будет карта СКУД, которая нужна, чтобы выйти из помещения, то вероятность, что контролер положит карту и уйдет, будет минимизирована),

- допустимы любые пары контролеров и пользователей или они должны быть жестко закреплены один за другим,

- вся работа в определенном функциональном ПО (или на определенном АРм) должна вестись с контролером или только некоторые операции,

- может ли меняться контролер во время выполнения задачи или это недопустимо, а при посменной работе без прерывания сессии (такие процессы бывают, например, в платежных системах, когда пользователь меняется без остановки вычислительного процесса) может ли (должен ли) контролер менять не синхронно со сменой пользователя, а по какому-то иному регламенту, и тому подобные особенности.

Практически все эти требования так или иначе направлены на повышение контролируемости работы контролера, так как люди всегда склонны попробовать «договориться» там, где им что-либо не вполне удобно, а любые ограничения повышают безопасность в ущерб удобству, хотя бы психологически.

3.1.2.4. Интеграция СЗИ НСД с системами СКУД и с видеонаблюдением

В предыдущем разделе уже были упомянуты карты СКУД. Об интеграции СЗИ НСД и СКУД необходимо сказать в этом разделе подробнее, так как любопытный нюанс такой интеграции связан именно с разграничением доступа к элементам управления информационной системой. Сразу стоит упомянуть, что встречается такая интеграция очень редко. Это связано с тем, что системы защиты информации и СКУД не только разрабатывают разные разработчики, но и непосредственно эксплуатируют – разные подразделения [6, 7]. Подразделение физической охраны и безопасности, как бы они не назывались, никогда не занимаются информационной безопасностью и наоборот.

Однако, интеграция систем защиты информации и контроля доступа позволит достичь ощутимых преимуществ. А именно.

1) **Объединение персональных идентификаторов сотрудников, применяемых ими в СЗИ НСД и в СКУД.**

Иными словами, чтобы одна и та же карта или ТМ-идентификатор были и пропуском в помещения, и идентификатором для доступа к АРМ или к прикладному ПО.

Это даст возможность сократить количество инцидентов, связанных с

- забыванием идентификаторов (сотрудник не войдет в здание),

- передачей идентификаторов другому лицу или оставлением идентификаторов без присмотра в момент отсутствия пользователя на рабочем месте (сотрудник не выйдет без идентификатора, значит, никому его не оставит),

- практически исключить воздействие человеческого фактора на выполнение правила блокировки рабочего места пользователя в момент отсутствия последнего (по той же причине, пользователь не выйдет без идентификатора, а отключение идентификатора заблокирует рабочее место).

2) **Объединение систем управления СКУД и СЗИ НСД путем создания третьей управляющей системы.** Иными словами, это добавление в инфраструктуру надстройки, для которой СКУД и СЗИ НСД будут подсистемами. Проще говоря, появится некоторый сервер, который будет получать данные от обеих подсистем и раздавать им обеим команды с учетом полученных данных. Это позволит формировать правила доступа во взаимосвязанности результатов выполнения действий доступа к информационным ресурсам и помещениям.

Например, СЗИ НСД не будет позволять пользователю доступ в информационную систему, если нет информации от СКУД, что он вошел на территорию предприятия. Это довольно логично – как он тут оказался? Весьма вероятно, что это не он, а злоумышленник.

А СКУД, в свою очередь, будет различать, при каких обстоятельствах человека можно выпустить из комнаты, а при каких –

позволить покинуть предприятие полностью (и при каких, соответственно, вообще никуда не выпускать).

Например, можно позволять покинуть комнату, если пользователь заблокировал рабочее место, но покинуть территорию предприятия на тех же условиях нельзя, нужно выключить рабочее место надлежащим образом. Или может быть необходимо завершить сеанс работы того пользователя, который хочет покинуть территорию, начать сеанс его сменщика, и только после этого СКУД позволит работнику покинуть предприятие. Вариантов увязывания событий информационной и охранной систем может быть множество, в зависимости от сценариев работы предприятия.

При этом важно не только не допустить реализации сценария с подозрительными последовательностями событий, но и зафиксировать их для дальнейшего анализа, ведь отдельные как бы случайные «проколы» могут быть шагами подготовки атаки. В обычных условиях – когда системы СКУД и СЗИ НСД не интегрированы, ни одно из описываемых событий не попадет в разряд запрещенных или просто подозрительных (если не будут нарушены какие-то другие условия – например, разрешенное время работы и т. п.), поэтому выявить подготовку преступления даже при внимательном наблюдении и оперативном мониторинге не получится.

Рассмотрим подробнее пример обхода правил безопасности, который возможен из-за отсутствия связи между правилами разграничения доступа к информационным ресурсам и правилами контроля доступа в помещения.

С точки зрения СЗИ НСД разблокировка сессии и включение СВТ являются разными событиями, и в отношении этих событий в средствах защиты информации с развитой подсистемой разграничения доступа возможна настройка разных ограничений. Например, разблокировка сессии зачастую возможна не только тем пользователем, чья это сессия, но и администратором или другим пользователем с аналогичной ролью (или входящим в коллективную учетную запись), при этом

разблокируется та же самая сессия. О таком сценарии – непрерывных вычислений – уже заходила речь выше. Как правило, в таких случаях устанавливается, какой пользователь должен разблокировать сессию вслед за каким, а если этот порядок должен быть нарушен (например, с очередным пользователем что-то случилось, и он заступить на смену не может), то сессию должен разблокировать администратор и санкционировать работу внеурочного пользователя. Вся сессия при этом протекает с точки зрения СЗИ НСД под профилем единого «коллективного пользователя», обладающего одним набором прав.

Иначе в случае включения АРМ – если АРМ будет включаться, то стартует новая сессия, а не продолжается старая, она связана с учетной записью того пользователя, который включает АРМ, а не того, который его перед этим выключал, все начинается «с чистого листа».

Для разблокировки сессии могут быть установлены совершенно другие ограничения по времени, в которое допустима разблокировка, в отличие от времени, в которое разрешено включение АРМ. Более того, для АРМ, на которых ведутся работы под «коллективной учетной записью» зачастую включение вообще не может осуществляться ни одним из пользователей, входящих в эту учетную запись, а должно производиться специально назначенным пользователем, который, в свою очередь, никаких других прав, кроме включения АРМ, не имеет.

При этом и блокировка сессии, и выключение АРМ – это штатные события с точки зрения СЗИ НСД и никаких подозрений они не вызывают, ведь СЗИ НСД ничего не известно о том, собирается пользователь уходить или выходит покурить. Соответственно, если перед уходом пользователь (случайно или умышленно) не выключил АРМ, а только заблокировал сессию, то он открывает злоумышленнику возможность осуществить те или иные манипуляции с его рабочим местом, которые тот не смог бы осуществить, будь АРМ корректно выключен.

В развитых СЗИ НСД есть возможность настроить время допустимой работы, и по его истечении СЗИ НСД зафиксирует нарушение и через минуту, если не вмешается администратор,

выключит компьютер. Однако не для всех сценариев работы возможно использовать этот инструмент без ощутимого усложнения организации труда – если нельзя, например, без потерь для эффективности установить единое время окончания работы (хотя бы даже и разное для разных дней недели). Устанавливать новые правила день ото дня – это существенно повышать вероятность ошибок администрирования.

Если же интегрированная система безопасности не выпустит пользователя за пределы организации, пока тот не выключит компьютер надлежащим образом, то атака такого рода будет невозможна, хотя никаких сложных правил выдумывать не придется. Таких примеров может быть масса.

Для создания такой интегрированной системы видеомониторинга и контроля доступа (СВМиКД) в ОКБ САПР было разработано решение, состоящее из Сервера интеграции и комплексов «Рассвет-СВМиКД». Сервер обеспечивает взаимодействие серверов СЗИ НСД и СКУД, что дает возможность формирования новых, более сложных и комплексных правил доступа. А комплексы «Рассвет-СВМиКД», помимо взаимодействия с Сервером интеграции, выполняют функцию передачи видеоизображения с экрана монитора подконтрольного АРМ на заданный сервер, видеоизображения с IP-видеокамеры, снимающей оператора, на заданный сервер видеонаблюдения. К «Рассвету-СВМиКД» может подключаться считыватель биометрических данных, и тогда на карте СКУД может быть записан эталон, и при аутентификации в системе дополнительно будет проверяться соответствие фактически предъявленной руки (мы используем считыватель сосудистого русла ладони) сохраненному в карте эталону.

Подробнее про особенности продуктов линейки «Рассвет» можно прочитать на сайте ОКБ САПР, там много любопытных нюансов.

Вернемся, однако, к тому, почему это все находится в разделе о разграничении доступа к элементам управления.

При реализации такой системы мы сталкиваемся с задачей, которая осознается не в первую очередь. Глобально она сводится к вечному

выяснению – кто главный. При формулировании «сквозных» правил для этого достаточно здравого смысла – события в норме располагаются в каком-то определенном порядке, соответственно, если речь идет о входе в систему, приоритетным будет наличие или отсутствие события от СКУД – вход на предприятие, а если речь идет о выходе – то наличие или отсутствие события от СЗИ НСД – выключен АРМ. Не со всеми сценариями все настолько просто, но общая логика из этого примера ясна.

Однако, есть более сложные случаи – например, смена идентификатора пользователя. Каким должен быть порядок корректного ввода в такую интегрированную систему нового идентификатора (допустим, карты). Должен СКУД принять данные от СЗИ НСД или СЗИ НСД от СКУД?

Скорее всего, ни так, ни эдак. Правильно в большинстве случаев будет вводить новый идентификатор через общую для этих подсистем систему управления. Однако и СЗИ НСД, и СКУДы имеют функции смены идентификатора, более того, СЗИ НСД, естественно, имеют такие функции как на уровне собственных серверов, так и локально, на уровне отдельных АРМ. Что делать в случае коллизии?

Коллизии весьма вероятны также в связи с изменениями правил на различных уровнях – должен управляющий сервер учитывать изменения, произведенные на рабочих местах, или должен «насильно» разослать свою базу и вернуть все, как было?

Все эти вопросы должны быть заданы и продуманы на этапе проектирования системы. А в случае проектирования универсальных инструментов – целесообразно предусматривать возможности ограничений на управляющие воздействия в зависимости от архитектуры всей системы.

3.2. Разграничение доступа к ресурсу в зависимости от среды

Весь предыдущий раздел описывал различные аспекты ситуации, когда внутри защищенной информационной системы действуют некоторые правила разграничения доступа и с их помощью обеспечиваются те или иные целесообразные ограничения действий пользователей или иных субъектов. В этом же разделе речь пойдет о том, как можно ограничить нежелательное влияние на защищаемую систему смежных систем (или просто внешних по отношении к ней).

Традиционный инструмент решения такой задачи – межсетевой экран (МЭ). О решениях этого класса можно почитать в интернет или в последней главе книги «Компьютерная преступность», где в параграфе 13 «Межсетевые экраны. Зачем они нужны, какими они должны быть и где они должны устанавливаться» [3. С. 1258–1263] о них написано в таком ключе:

«Бородатый анекдот утверждает, что у параноиков и шизофреников есть общее – это воздушные замки, которые один строит, а другой в них живет. А психиатр при этом собирает квартплату.

Этот анекдот весьма похоже иллюстрирует сложившуюся ситуацию с межсетевыми экранами. Одни пугают нас жуткими последствиями, если мы не установим межсетевой экран, другие, напуганные первыми, покупают их по чудовищно высоким ценам, совершенно не понимая, зачем, а третьи, улыбаясь, выпускают все новые и новые изделия, которые снова покупаются, не являясь при этом защитным средством и практически никак не влияя на защищенность наших компьютеров» [3. С. 1258].

Здесь же будет не о них, а о решениях более замысловатых задач: о способах защиты USB-устройств, являющихся частью ИС, от их использования вне ИС (и, соответственно, о защите ИС от последствий такого использования), а также о том, как защитить ИС в тех случаях, когда ее легальные пользователи имеют возможность подключаться к ее ресурсам с использованием разных СВТ, не всегда доверенных или хотя бы известных.

3.2.1. USB-накопители и похожие на них устройства

Этот параграф посвящен носителям информации в форм-факторе USB-устройств. Мы рассмотрим типовые задачи разграничения доступа на примере устройств флеш-памяти. Этого достаточно, так как при применении носителей ключей (токенов) и других специализированных носителей этого форм-фактора возникают сходные задачи.

Носителями информации принято называть средства хранения данных. Носители информации (как, впрочем, и средства ее обработки) в информационной системе (ИС) могут быть стационарными и мобильными (стационарные – жесткие диски компьютеров, мобильные – внешние жесткие диски, флешки; системы хранения данных (СХД) и файловые серверы, как правило, носителями информации не называют). Помимо этого, носители информации могут быть составной частью оборудования, выполняющего также и *обработку* данных, а могут быть носителями в собственном смысле слова – устройствами, с помощью которых информацию носят, и во время того, как ее носят, она там хранится. А потом, когда информацию перенесли, она обрабатывается с помощью какого-либо другого оборудования. И вновь сохраняется на носитель, чтобы быть перенесенной куда-то еще.

Являясь частью защищенной ИС, носители информации тоже должны быть защищенными, то есть способными противостоять атакам. Разумеется, противостоять *именно тем* атакам, которые актуальны по отношению к данному элементу системы. Что это означает применительно к вопросу защищенности мобильных носителей информации?

Самая главная особенность мобильных носителей состоит в том, что они подвержены дополнительным угрозам (по отношению к угрозам, актуальным для основной («стационарной») системы), связанным с тем, что контур системы для них проницаем: они могут не только *выноситься* (и не только могут, но и выносятся!) за пределы

системы, но и *использоваться* там, за пределами. А, как следствие, это приводит к *утечкам информации из системы* и к *притоку вредоносного ПО в систему*.

Именно поэтому проекты защищенных ИС зачастую предусматривают полный запрет на использование USB-носителей. Однако это, как правило, не помогает. Некоторые причины такой «сопротивляемости» флешек «безопасникам» приведены в [8, 9].

Итак, флешки признаются «абсолютным злом» потому, что они могут использоваться вне системы. Значит, защищенный носитель – это такой носитель, который может использоваться только внутри той информационной системы, частью которой он является, и не может использоваться вне ее.

Назовем такой носитель служебным.

Служебный носитель – это такой носитель, который позволяет оперативно и просто переносить информацию внутри системы согласно ее внутренним правилам, но не позволяет ни выносить хранимую на нем информацию из системы, ни приносить в систему информацию, записанную на него вне системы. Никому, в том числе и легальному, пользователю. Только в этом случае носитель не будет снижать общего уровня защищенности системы даже при его физическом выносе за ее периметр.

Если посмотреть с этой точки зрения на продукты информационной безопасности, позиционируемые поставщиками как средства защиты информации на флешках, то выяснится, что при всех своих возможных плюсах необходимую задачу они не решают. Как правило они контролируют, какие флешки можно использовать на каких компьютерах, как и кому – внутри информационной системы, а не за ее пределами, так как установлены такие средства – на компьютерах информационной системы, а не на всех остальных в мире.

Критерии оценки, которые адекватны понятию «защищенный служебный носитель», следующие:

1) является ли продукт средством хранения и переноса информации (носителем),

2) удобно ли его использование (аппаратные требования, требовательность к навыкам эксплуататора, мобильность, дружественность),

3) снижает ли применение продукта степень негативных последствий кражи или утери носителя с данными для системы,

4) защищает ли продукт данные от доступа посторонних лиц,

5) при использовании вне защищенной системы способен ли продукт предотвратить «заражение» вредоносным ПО, которое в дальнейшем может попасть в систему,

6) можно ли при помощи продукта защитить данные от хищения мотивированным инсайдером.

До последнего времени не было предложено решения главной задачи: привязки носителя к системе. Первыми продуктами, решившими эту задачу, стали продукты линейки «Секрет», в которых именно эта функция является основной.

Что может предпринять злоумышленник в отношении флешки как элемента интересующей его информационной системы?

1. Украсть (или искать там, где есть шанс найти, и найти)
2. Отнять
3. Завладеть оставленным без присмотра устройством
4. Завладеть путем мошенничества и социальной инженерии
5. Купить у мотивированного инсайдера

Как правило, пп. 1, 2 и 5 имеют своей целью завладение данными с флешки, а п. 3 и 4 может также иметь целью внедрение подложных данных или вредоносного кода (реже, но тоже возможно – уничтожение данных на флешке).

В отличие от угроз данным в сетях или на локальных компьютерах, которые реализуются весьма разнообразными атаками, угрозы,

связанные с флешками, характеризуются очень мощными общими признаками возможных атак:

1) физическое завладение устройством и

2) получение доступа к его памяти путем подключения к какому-то (своему или произвольному) ПК.

Атаки на флешки через сеть весьма маловероятны и будут скорее атаками на данные на дисках компьютера (в данном случае – подключаемых), а не на данные на флешке. И в любом случае, вряд ли возможность реализации такого рода угрозы может быть классифицирована как уязвимость флешки.

Очевидно, что защитить маленькое устройство от физической кражи (или находки в результате целенаправленного поиска в местах возможных потерь, провокации потери) – крайне сложно и практически невозможно сделать это техническими методами.

Более того, и применение организационных мер крайне затруднительно, поскольку на ситуацию очень сильно влияет характер пользователя: он рассеянный, или любит прихвастнуть, или нечист на руку, и т.д.

Сейчас в специализированных изданиях выходит масса статей о том, как разговорами добиться от пользователя повышения ответственности и внимательности. Однако изменение человека – процесс долгий, сложный и непредсказуемый по своему результату. Изменение железки – процесс намного более предсказуемый и контролируемый.

Задача технической защиты флешки сводится к тому, чтобы сделать нелегальное физическое обладание ею бессмысленным. То есть, даже имея флешку, получить доступ к данным на ней на не разрешенном явно для этой флешки компьютере не разрешенному явно пользователю должно быть невозможно.

Именно эта логика и положена в основу защищенных флешек семейства «Секрет». Диск масстораджа «Секрета» монтируется только после успешной проверки того, зарегистрирован ли компьютер, к

которому подключают «Секрет» в списке разрешенных для работы с этим «Секретом». До успешной аутентификации компьютера, аутентификация пользователя не запрашивается, неважно, легальный ли он, если еще неизвестно, легальный ли компьютер. Разные продукты линейки различаются тем, как именно организована система этой аутентификации, обо всем этом можно почитать в их описаниях.

Также небезынтересно будет познакомиться с сопоставлением функциональности традиционного средства контроля использования USB-накопителей с функциональностью «Секретов» [10].

Интересным нюансом является наличие собственной ролевой структуры в продуктах линейки «Секрет». Рассмотрим на примере продукта «Секрет особого назначения», так как он самый простой.

В «Секрете» есть пользователь и администратор. Пользователь – это тот, кто, собственно, использует флешку – записывает на нее данные и читает их с нее. При начале использования автоматически выполняется аутентификация компьютера. При успешной аутентификации компьютера, пользователь вводит PIN-код, который известен только ему.

Все попытки пользователя подключить «Секрет» – как успешные, так и неуспешные – когда компьютер не прошел проверку и диск не был примонтирован – фиксируются в журнале «Секрета», который пользователю не доступен. Его может посмотреть только администратор.

Администратор же, напротив, не может увидеть диск с данными пользователя, он может только посмотреть журналы или поменять настройки безопасности – требуемую длину PIN-кода, допустимое количество неверных вводов, список разрешенных компьютеров с их параметрами («Секрет особого назначения» идентифицирует компьютеры по набору из 5 параметров), действия в случае заполнения журнала. У администратора свой пароль для входа в консоль администрирования, а инструментов для того, чтобы, например,

сбросить PIN-код пользователя, назначить новый и посмотреть данные на флешке – нет. Сбросить учетные данные пользователя можно только вместе с полным сбросом всех данных. То есть администратор может полностью уничтожить данные пользователя, но не прочитать их.

3.2.1.1. Ключевые носители

Криптографические ключи, так же, как и любые данные, существуют в трех процессах: хранятся, обрабатываются (в том числе – создаются и уничтожаются) и передаются.

Никаких других состояний у данных (и ключей как явлений этой сущности) не бывает.

Ключи отличаются от других данных только одним – компрометация ключей заметно более критична. Это сразу и хорошая, и плохая новость. С одной стороны, это значит, что ничего принципиально иного, чем с другими данными, с ними произойти не может, то есть никаких специфичных приемов для защиты именно ключей – не требуется. С другой стороны – обеспечиваться меры защиты должны более тщательно, чем в отношении любых других данных, а никаких специфичных приемов для защиты именно ключей – быть не может (так как они – не более чем данные).

Почему более тщательно – очевидно на уровне здравого смысла. Сравним случай компрометации документа и компрометации ключа. Если скомпрометирован документ, то наступают некие негативные последствия. Безусловно, они могут быть весьма существенными, поэтому защищать необходимо отнюдь не только ключи. Но все-таки, если происходит компрометация ключа (например, ключа электронной подписи (ЭП)), злоумышленник может создавать *неограниченное количество документов от имени пользователя*, чей ключ скомпрометирован.

К сожалению, здравый смысл не всегда детерминирует безопасное поведение, потому более жесткие требования по защите ключей (хотя

вернее было бы сказать – систем с ключом) предъявляются и регуляторами.

В свете требований к средствам электронной подписи (СЭП), в которых взаимоувязаны все три состояния ключа, это становится особенно наглядно: мы можем руководствоваться самыми разными соображениями, выбирая тип желательной для нас в тех или иных обстоятельствах ЭП, выбирая подходящее для нас СЭП, но как только мы выбрали усиленную ЭП (то есть «ЭП с ключом») мы попадаем в зону действия существенно более высоких требований.

Таким образом, с точки зрения безопасного существования криптографических ключей в информационной системе принципиальное значение имеют 2 фактора:

- защищенное хранение ключа (и, соответственно, носителя ключа)
- условия доступа к ключу и работы с ним (то есть среда функционирования криптографии (СФК)).

Очевидно и не нуждается в детализации, что второй фактор (условия доступа к ключу) касается и обработки, и передачи ключей – как части технологии, реализуемой СКЗИ (СЭП) при выполнении своих функций.

Сложившаяся практика применения ключей такова, что в качестве их носителей используются универсальные накопители (дискеты, флешки), идентификаторы пользователей, если они представляют собой устройства с доступной для записи/чтения памятью (ТМ-идентификаторы) или специализированные устройства (смарт-карты, USB-токены).

Однако, и специализированные средства – токены[27] – не идеальны.

Токены предоставляют возможность использования хранимых на них ключей и сертификатов после предъявления PIN-кода

[27] Это слово используется в разных значениях, но в рамках этого текста условимся понимать токен только одном из них: как защищенное тем или иным способом хранилище ключей в виде объектов PKCS.

(авторизации пользователя). Казалось бы, таким образом блокируются все уязвимости, связанные как с хранением, так и с доступом к ключу.

Однако очевидно, что ограничение доступа к ключу только использованием PIN-кода недостаточно. Токен должен использоваться только в той системе, в которой обеспечена защита от несанкционированного доступа (а именно – обеспечена доверенная СФК), а PIN-код можно правильно ввести в любой среде. Токен не может определить, в какой системе производится попытка работы с ним, у него нет для этого никаких механизмов. Невозможность расширения функций токена проистекает не из лени программистов, а из ограниченности его архитектуры (см. рис. 3.6).

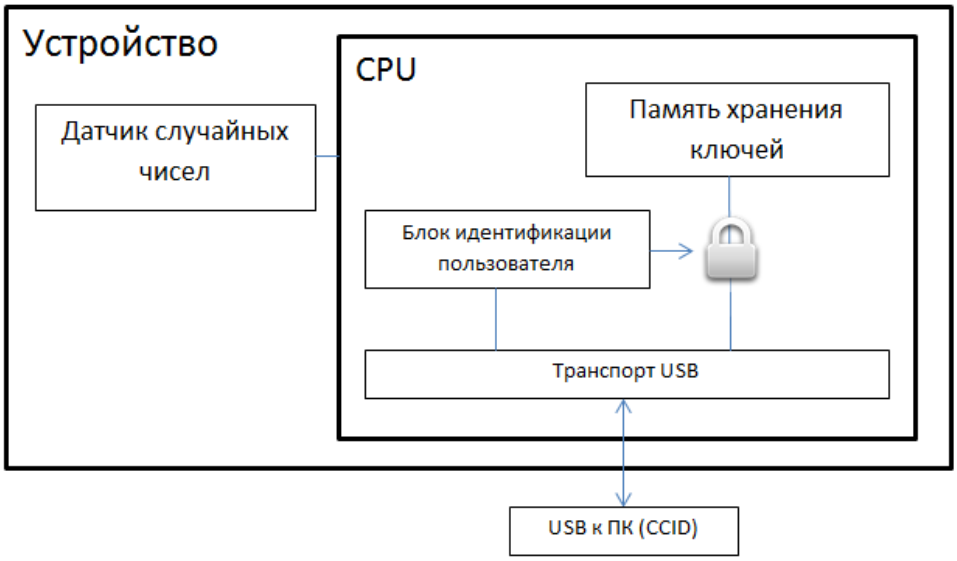


Рис. 3.6. Структурная схема токена

Чем же опасна невозможность контролировать внешнюю среду? Например, в ней могут быть предустановлены программные закладки, предназначенные для перехвата ключей или перехвата управления компьютером. При правильно введенном PIN-коде (а в некоторых случаях и до введения PIN-кода) все это вредоносное программное обеспечение получит доступ к ключам.

В части доступа к ключу очевидна необходимость учитывать не только условия доступа пользователя (человека), но и условия доступа

к ключам самих СКЗИ и другого системного и функционального программного обеспечения.

При этом необходимо учитывать особенности сред и систем, в которых пользователи выполняют задачи, связанные с криптографическими преобразованиями: работа в различных ОС, загруженных на СВТ различных архитектур из различных источников различными способами – может иметь целый ряд особенностей, существенно влияющих на безопасность ключа.

Отсюда вытекают требования к защищенному ключевому носителю. Защищенный носитель ключа в идеальном случае должен быть способен контролировать

- доступ к ключу *через любые интерфейсы*, в том числе и путем применения разрушающего программного воздействия (РПВ),

- среду, в которой производится попытка доступа к ключу.

Естественно, защищенный ключевой носитель не должен контролировать корректность работы СКЗИ или обеспечивать среду его функционирования (это функция средства доверенной загрузки). То есть задача «контроля» среды, из которой осуществляется доступ к ключу, сводится к тому, чтобы доступ к ключу предоставлялся не только исключительно легальному пользователю, но и исключительно на заданных рабочих местах (наличие «правильной» среды на которых обеспечивается в установленном в организации порядке). Принципиально это та же задача, что и для флешек: ограничение числа компьютеров, на которых технически возможна работа с токеном.

В случае реализации такой защитной меры при случайном или преднамеренном подключении токена к неразрешенному (а значит, недоверенному) компьютеру, устройство не будет примонтировано, значит, ключи не будут доступны ни пользователю (даже легальному), ни системе (с потенциально функционирующими в ней вирусами и закладками).

Кроме того, при этом будет исключено несанкционированное использование ключей легальным пользователем токена вне рамок его

служебных задач. Это важно, так как само по себе СКЗИ не может определить правомерность формирования данного документа на данном компьютере и подписание его с помощью того или иного ключа.

Вероятность подмены рабочего места звучит не очень страшно только по одной причине – кажется, что в этом никто особенно не заинтересован (например, трудно представить, что бухгалтер соберется сделать с домашнего ноутбука нелегальный перевод, подписав платежку своей ЭП).

Однако на самом деле представить себе сценарий как случайной, так и злонамеренной компрометации ключа и документа – несложно.

Рассмотрим несколько самых явных.

Начнем с добросовестного бухгалтера (таких, все-таки, мы уверены, большинство). Из лучших побуждений – выполнять часть работы сверхурочно – он может организовать себе дополнительное рабочее место дома. При этом он может разделить работы по критичности и для «домашнего» выполнения выделить не платежи, а только подготовку и отправку в налоговую инспекцию отчетов в электронном виде. Это делается с помощью одной из специальных программ, например, «Фельдъегерь» («Доклайнер», «Контур-Экстерн»), и бухгалтеру на его домашнем компьютере даже не потребуется «Клиент-банк».

Скорее всего, из средств защиты от НСД на этом «дополнительном рабочем месте» будет в лучшем случае только антивирус. Эта ситуация создаст предпосылки для компрометации ключа с помощью широко распространенных вредоносных программ. В случае направленной атаки это позволит злоумышленнику в дальнейшем использовать украденный ключ в своих целях. Если же компьютер используется и для проведения платежей, а не только для подготовки и отправки отчетов, то задача злоумышленника и вовсе упрощается.

Все еще хуже, если злоумышленником является сам бухгалтер (надеемся, что не доведем никого до греха).

Итак, если бухгалтер задумал провести нелегальный платеж, что его может остановить? Теоретически, его должна сдержать неотказуемость от ЭП на его ключе.

Однако в действительности при наличии технической возможности передачи ключевого носителя другому лицу и одновременно возможности применения ключа на произвольном СВТ, неотказуемость от ЭП – это уже вопрос алиби, а не криптографии.

Нарисуем такой «детектив»: злоумышленник организует рабочее место с необходимым для проведения платежа программным обеспечением. На собственном рабочем месте он подготавливает накануне несколько платежных поручений, подписанных его ЭП, но не отправляет их.

Вечером токен с ключом ЭП бухгалтер передает сообщнику и договаривается о времени проведения незаконного платежа таким образом, чтобы сам владелец ключа в это время был на рабочем месте на глазах у свидетелей.

В результате, в условленное время злоумышленник находится на виду у будущих свидетелей и отправляет заранее подготовленные платежки с легальной ЭП (токен ему для этого не нужен, ведь документы подписаны заранее). В это же время в другом месте с другого компьютера другое физическое лицо (сообщник) подписывает ключом нашего героя другое платежное поручение, используя токен.

При разборе инцидента злоумышленный владелец ключа имеет все шансы отказаться от своей ЭП, так как находился в это время на собственном рабочем месте и даже отправлял другой документ с подписью на том же ключе, а никаких следов отправки нелегального платежа на его рабочем СВТ нет. Очевидно, что он «совершенно не при чем».

Чтобы избежать обвинений в предвзятости к бухгалтерам, приведем пример, никак не связанный с платежами.

Предположим, что злоумышленником движет желание осуществить атаку на корпоративную информационную систему, обрабатывающую информацию ограниченного доступа.

Предположим, что система централизованная, клиент-серверная (допустим, система терминального доступа, или web-система). Предположим, что документы обрабатываются на сервере, сервер надлежащим образом защищен, клиентские СВТ не содержат средств обработки информации (тонкие клиенты), загружаются с обеспечением доверенности клиентской ОС, и каналы между клиентами и сервером тоже защищены.

Ключи СКЗИ, защищающего канал, хранятся в токене.

Наиболее очевидная атака – это подключение в качестве терминального клиента произвольного СВТ злоумышленника, оснащенного программами для осуществления какой-либо атаки на систему.

Если атаку осуществляет легальный пользователь системы – он обладает идентификатором к СЗИ НСД на сервере и токеном с ключами СКЗИ, защищающего канал (зачастую это одно и то же устройство).

Именно таких случаев касается п. 31 Требований к средствам электронной подписи [11]: «В состав средств ЭП классов КС3 должны входить компоненты, обеспечивающие: … управление доступом субъектов к различным компонентам и (или) целевым функциям средства ЭП и СФ на основе параметров, заданных администратором или производителем средства ЭП …».

Предотвратить эту атаку может только применение комплексной системы защиты, включающей взаимную аутентификацию клиентского СВТ и сервера. Это не рядовая функция, зачастую относительно сервера аутентифицируется только пользователь.

Все эти леденящие кровь сценарии невозможны, если токен просто различает СВТ, к которым его подключают.

Итак, защищенный ключевой носитель должен:

1) быть персональным отчуждаемым устройством,

2) быть специализированным именно для хранения ключей устройством (то есть обеспечивать возможность защищенного

хранения криптографических ключей с применением интерфейсов работы со смарт-картой (CCID или PKCS#11)),

3) предоставлять доступ к ключам только легальному пользователю после успешной аутентификации в устройстве,

4) предоставлять легальному пользователю доступ к ключам только на тех СВТ, на которых данному пользователю разрешено работать с данным ключевым носителем.

Функции токена с функцией ограничения числа разрешенных компьютеров объединяет в себе «Идеальный токен» – токен с несколько измененной архитектурой: она включает в себя блок идентификации компьютера, до прохождения проверки которым недоступен в том числе и блок идентификации/аутентификации пользователя (см. рис. 3.7).

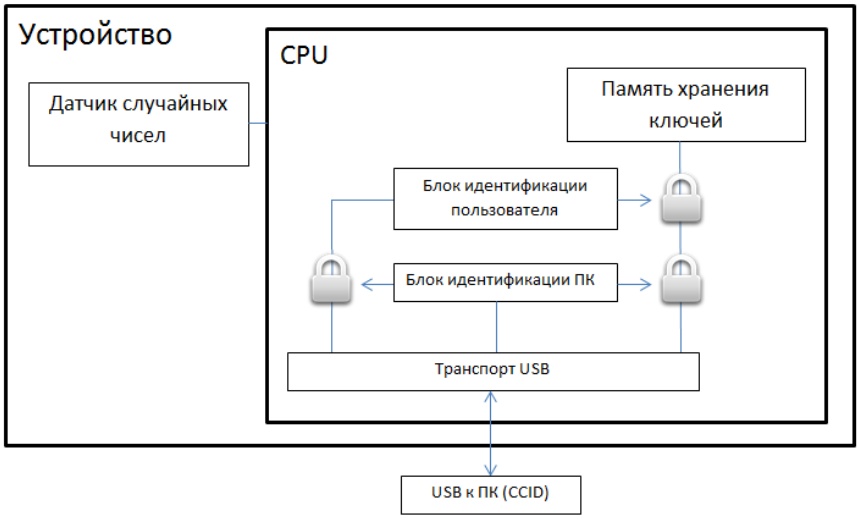


Рис. 3.7. Структурная схема Идеального токена

Технология «Идеального токена» запатентована [12], подробности о нем можно почерпнуть из описания продукта.

В «Идеальном токене» так же, как в «Секрете», есть роли администратора и пользователя, не имеющие возможности доступа к данным друг друга.

3.2.1.2. Другие служебные носители

По принципу, впервые реализованному в служебных носителях «Секрет», кроме «Идеального токена» построены и другие служебные носители для различных более узких целей. Например, это программно-аппаратный неперезаписываемый журнал ПАЖ – где свойства «Секрета» дополнены тем, что память, в которой сохраняются журналы событий различных устройств и приложений – Add only, то есть в нее можно только добавлять, а что-либо удалять или изменять в ней – нельзя. Это важное свойство, оно обеспечивает невозможность что-то «подчистить» в журналах, а значит, обеспечивает более высокое доверие к ним. Но без различения тех СВТ, к которым подключают ПАЖ, такое решение привело бы к заметному усложнению работы администраторов, ведь никогда не перепутать, на какую флешку переносить журналы с каждого конкретного компьютера, довольно сложно, а если записывать все без разбору, то анализ такого архива потом будет очень сложным и его результат будет выглядеть неубедительно («это не смотрим, это журналы с другого компьютера.... Теперь берем другую флешку, продолжение тут..., теперь опять эту...»). При этом, напомню, исправить ошибку нельзя – журнал не перезаписывается, память Add Only.

Возможность перенести контроль упорядоченности архива с человека на техническое устройство существенно улучшит результат и повысит комфортность работы сотрудников. Если ПАЖ подключен не к тому компьютеру, с которого должен собирать журналы, его диск не примонтируется, и ошибка не совершится.

Собственная ролевая структура ПАЖ даже более сложная, чем у «Секрета» и «Идеального токена», кроме администратора и пользователя устройства в нем есть еще роль аудитора.

Под учетной записью пользователя устройства доступ к памяти предоставляется только на запись: пользователь ПАЖ может

подключить устройство к компьютеру, и если тот разрешенный, то скачать с него журналы. Посмотреть журналы – он не может.

Под учетной записью администратора доступ к памяти вообще не дается, администратору доступно только изменение настроек – свойств пароля, параметров собственного журналирования ПАЖ (то есть тех журналов, которые ведет он сам с событиями его работы, а не журналов, которые на него записываются), и так далее. То есть администратор не может ни записать, ни прочитать журналы, но может управлять настройками остальных пользователей.

Под учетной записью аудитора доступ к памяти дается только на чтение, если компьютер входит в число разрешенных. При этом возможно настроить устройство так, чтобы доступ на чтение (аудитору) и доступ на запись (пользователю) давался на разных компьютерах (как правило, читать журналы должно быть возможно на каком-то специальном рабочем месте того сотрудника, которому вменена эта обязанность, и который, соответственно, регистрируется в ПАЖ аудитором. Это весьма целесообразно, так как если такое разделение не реализовано, аудитор от пользователя отличается только паролем, а это недостаточно непреодолимая преграда. Если же права на доступ к памяти задаются уже при монтировании устройства (если компьютер А, то на чтение, если компьютер Б – то на запись), то просто ввод пароля аудитора не даст пользователю возможность прочитать память, понадобится еще и завладеть его рабочим местом.

3.2.2. Разграничение доступа к ресурсам ИС при доступе к ним с разных устройств

Другая сторона той же медали (если это сейчас не очевидно, не страшно, ниже разберемся, почему это одна медаль) – организация доступа к ресурсам защищенной ИС с различных клиентских устройств (компьютеров, ноутбуков, смартфонов и прочего, с чего вообще можно

получить доступ к системе) так, чтобы права, которые получает пользователь на конкретную сессию, зависели от того, что это за устройство и насколько можно доверять его вычислительной среде.

В первой главе уже велась речь о том, что те компьютеры (в широком смысле слова), с которых пользователи получают доступ к ресурсам информационной системы, могут оказывать самое серьезное влияние на систему, и должны считаться частью этой ИС. При этом в целом ряде случаев архитектура ИС предусматривает возможность доступа к ней с различных (в предельном случае – с любых) СВТ. Самой очевидный пример – информационные ресурсы, такие, как, например, расписание РЖД или аэропортов. Любой пользователь с любого устройства, позволяющего выйти в Интернет, должен иметь возможность посмотреть расписание.

Значит ли это, что все устройства в мире (ведь доступ должен быть получен с *любого* устройства) должны силами РЖД защищаться одинаково серьезно?

Давайте рассуждать.

Любой пользователь с любого СВТ должен иметь возможность посмотреть расписание. А внести в расписание изменения? Эти два случая отличаются не содержанием данных, а направлением их движения – *из системы* или *в систему*. Читать из базы данных и заполнять базу данных – это совсем разные задачи, с разным уровнем ответственности.

Важно не упустить, однако, и еще один аспект. К какой категории отнести задачу покупки билета или аннулирования покупки? Направление – в систему, однако, это не совсем то же, что изменение расписания.

Доступ к чему-то своему гражданин, строго говоря, может организовывать так, как считает нужным (или по крайней мере имеет смысл учитывать его пожелания), а вот если ему требуется доступ на изменение данных, которые будут касаться и других, то требования к его

идентификации/аутентификации и к тому, из какой среды он будет производить эти изменения – должны быть существенно выше.

Однако, первое, что мы узнаем в жизни о защите информации – это правило о том, что общая защищенность системы не выше защищенности ее самого слабого звена, или правило «дыры в заборе» (нет смысла наращивать высоту забора, в котором есть дыра, клубнику все равно украдут).

Можно ли совместить эти выкладки так, чтобы между ними не возникало противоречия?

Идея сегментирования информационных систем в целях снижения сложности (и, прямо скажем, стоимости) их защиты не нова, она получила наибольшую популярность сразу после выхода 152-ФЗ [13]. Однако, если посмотреть примеры (о них написано много, можно найти публикации в самых разных источниках), станет ясно, что идейная связь тут самая общая, сегментирование проводится совершенно иначе и различаются полученные сегменты по-другому: в них обрабатываются разные данные.

Нам же нужно создать условия, при которых легальный пользователь, получая доступ к своей учетной записи, мог получить доступ с разными правами в зависимости от того, с какого устройства он получает доступ. То есть при авторизации должны быть учтены не только результаты и/а, но и параметры клиентского устройства. Принципиально в этом нет ничего особенного – ведь учитывается же помимо и/а еще время, в которое пользователь пытается получить доступ.

На первый взгляд эти выкладки ведут к усложнению системы, так как чем больше факторов должно учитываться при принятии решения, тем сложнее такую систему реализовать. Однако если сравнить эту задачу с задачей защитить смартфоны граждан так же, как рабочие места сотрудников РЖД, которые работают с базами данных информационной системы этой организации, легко понять, что эти сложности не соизмеримы.

Итак, в ИС, для которых направление движения данных имеет ощутимое значение, имеет смысл строить подсистему разграничения доступа так, чтобы доступ предоставлялся с учетом того, идентифицировано ли устройство доступа и является ли оно доверенным.

В общем случае, более жесткие требования кажется логичным предъявлять к среде при доступе с целью передачи данных в систему, и менее жесткие – при доступе с целью получения данных из системы. Однако можно предположить и обратное: например, сбор медицинской статистики может быть организован так, чтобы передать свои данные мог любой желающий, а вот получить данные из системы – ограниченный круг сотрудников. Другими словами, система должна *проектироваться*, построение по образцу может быть чревато серьезными ошибками.

В заключение стоит отметить, что описанный подход может быть реализован очень гибко – различных вариантов урезания и наоборот – расширения возможностей пользователя в зависимости от того, откуда он получается доступ может быть много, не обязательно ограничиваться дихотомией «все или минимум». Особенно это может быть актуальным при всевозможных формах «удаленки» и дистанционных форм работы и учебы. Предположим, максимальные возможности – при доступе с рабочего места в офисе, минимальные – с телефона. Но между ними может быть доступ с использованием «МАРШ!» или какие-либо еще промежуточные варианты. Проектирование таких систем – крайне интересная и требующая высокого профессионализма область деятельности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД «Аккорд». М.: «Радио и связь», 1999. – 325 с.

2. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. Минск: Серия «Библиотека журнала "УЗИ"», 2004. – 327 с.

3. *Конявский В. А., Лопаткин С. В.* Компьютерная преступность. Т. II. М., 2008. – 840 с.

4. *Постоев Д. А.* Управление доступом в виртуальных системах на основе контроля информационных потоков // Безопасность информационных технологий. М., 2014. № 4. С. 86–91.

5. *Девянин П. Н.* Модели безопасности информационных потоков // Модели безопасности компьютерных систем: Учебное пособие для студентов высших учебных заведений. М.: Изд. центр «Академия», 2005. С. 55–66.

6. *Конявская С. В.* Интеграция СЗИ, СКУД и видеонаблюдения, или кто отвечает за костюм? // Национальный банковский журнал. М., 2015. № 12. С. 74.

7. *Счастный Д. Ю., Конявская С. В.* Интегрированная система контроля доступа и защиты информации на основе биометрической аутентификации сотрудников // Первая миля. М., 2013. N 2. С. 90–97.

8. *Лыдин С. С.* Психологические аспекты защищенного применения служебных носителей информации // Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15–18 мая 2012 года, Суздаль (Россия). М., 2012. С. 174–176.

9. *Лыдин С. С., Конявская С. В.* Флешки или сеть: почему из двух зол бессмысленно выбирать меньшее // Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15–18 мая 2012 года, Суздаль (Россия). М., 2012. С. 177–179.

10. *Шамардина (Чепанова) Е. Г.* Защищенная работа с флешками: служебные носители («Секрет») или USB-фильтры (ПК «DeviceLock»)? // Библиотека ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/library/links/chepanova_2013_1/ (дата обращения: 05.11.2021).

11. Приказ ФСБ России от 27 декабря 2011 г. № 796. Приложение 1. [электронный ресурс]. URL: http://base.garant.ru/70139150/ad65a43c549a45d32360a363f5d4fa2c/#block_66 (дата обращения: 12.08. 2019).

12. *Батраков А. Ю., Конявская С. В., Счастный Д. Ю.* Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014, бюл. № 31.

13. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.11.2021).

ГЛАВА 4: ПЕРЕОСМЫСЛЕНИЕ ГРАНИЦ ЗАЩИЩЕННОЙ СИСТЕМЫ: ТЕХНИЧЕСКИЕ СРЕДСТВА ДЛЯ РАБОТЫ В ОТКРЫТОМ МИРЕ

В предыдущих главах многократно упоминалась тенденция к тому, что информационные системы, которые нам предстоит защищать, меняются: уходят все дальше от корпоративных систем с перечислимым закрытым парком оборудования.

Рассмотрим, чем же так существенно различаются корпоративные системы и открытые. Для описания этого различия существуют понятия «контролируемая зона», «периметр», «контуры защиты». Они называют семантически близкие, даже смежные понятия, но все же они – о разном (да и, кроме первого, – не термины, а профессиональные жаргонизмы).

В двух словах об этих понятиях, так как глава посвящена все же не им.

«Контролируемая зона» – термин из понятийной системы ГОСТ Р «Защита информации. Автоматизированные системы в защищенном исполнении».

Определение:

Контролируемая зона: Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.

ГОСТ Р 52863-2007, п. 3.1.9. [1]

То есть, строго говоря, уже из самого определения видно, что это понятие имеет весьма опосредованное отношение к защите

информации. Привязывает его к этой области, во-первых, стандарт, которым понятие введено, и затем – Приказы ФСТЭК России. Ситуация усложняется тем, что документы, вводящие этот термин с его определением – закрытые. Поэтому в учебнике можно привести только фрагмент из Приказа ФСТЭК России № 21 [2].

Вот контекст из приказа: «Оператором персональных данных должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие персональные данные, и средства защиты информации, а также средства обеспечения функционирования.

В соответствии с пунктом 3.1.2 ГОСТ Р 56115-2014 [3] и пунктом 3.1.9 ГОСТ Р 52863-2007 [1] под контролируемой зоной понимается пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и (или) транспортных средств.

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора персональных данных и лиц, не имеющих постоянного допуска на объекты информационной системы персональных данных (ИСПДн) (не являющихся работниками оператора персональных данных), а также транспортных, технических и иных материальных средств.

Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите персональных данных.

Для одной ИСПДн (ее сегментов) может быть организовано несколько контролируемых зон».

Надо заметить, что из двух ГОСТ Р, на которые ссылается приведенный фрагмент, только второй содержит искомое определение, но это не имеет существенного значения, так как все упомянутые

источники определяют контролируемую зону совершенно одинаково, и контекст защиты ИСПДн или электромагнитных воздействий ни на что не влияет.

Смысл понятия остается неизменным – контролируемая зона

1) некоторое пространство,

2) контролируются в ней люди и транспортные средства.

В приказе ФСТЭК добавлено достаточно существенное уточнение – кроме людей и транспорта в контролируемой зоне не может бесконтрольно находиться какая-либо техника или иные «материальные средства».

При этом если относительно людей имеется оговорка «не являющихся работниками…», то относительно технических средств такой оговорки нет, то есть контролируемость распространяется и на «штатные» технический средства. Это позволяет использовать понятие «контролируемая зона» в значении «все то, что находится в границах защищенной информационной системы, относится к ней», хотя такая трактовка и является, как можно видеть, несколько искусственной.

Поэтому, чтобы не использовать термин не совсем по назначению, в профессиональном сленге используется «периметр».

«Контур защиты» в этом смысле использовать еще менее правильно, так как контуров защиты в информационной системе может быть несколько, такие информационные системы называются многоконтурными. Строго говоря, таких систем большинство, так как сложно себе представить, что абсолютно все информационные ресурсы в организации целесообразно относить к информации ограниченного доступа и так или иначе защищать. Как правило, часть ресурсов – общедоступные. Чаще градаций больше, но для общего понимания этого достаточно. Контуры могут быть организованы по-разному, иногда для работы с разными ресурсами надо использовать разные рабочие места, иногда – перезагружаться, например, подключив «МАРШ!», иногда требуется только переключить режим, как в решении «Двухконтурный моноблок».

Очевидно, что контуры защиты тоже не совпадают с «тем, что в границах защищенной ИС».

В то же время смысл этого понятия, для которого нет слова, хорошо ясен: это, собственно, и есть сама защищенная информационная система – то, что защищено по поручению владельца и по требованиям, установленным владельцем. «Граница» здесь является скорее метафорой, свойственной человеческому сознанию: вспомним, что мы защищаем не дверь, а квартиру, не забор, а клубнику. И защита собственно границы, а не того, что она ограждает – это, вообще говоря, деформация.

Однако, деформация понятная, так как защищать границу (забор) проще – он небольшой и четко локализованный. Есть искушение считать, что сделай его железным – и дело сделано.

Жизнь неизменно показывает, что это не так, и останавливаться на этом лишний раз не нужно.

Лучше попробуем разобраться, что же меняется, если границы – это и так не совсем границы, и что это означает для специалистов по защите информации.

До сих пор защищенную ИС, действительно, можно было локализовать, и эта локализация преимущественно совпадала с контролируемой зоной. Вне контролируемой зоны у территориально распределенных ИС могли располагаться каналы связи, которые, в этом случае, должны были защищаться определенным (описанным в нормативной базе) образом.

Процесс размывания этих физических, пространственных границ начался довольно давно – с появления флешек, об этом вы уже читали в предыдущей главе. Затем возникло понятие BYOD (bring your own device), в отношении которого сразу обострились вопросы, насколько можно контролировать личные устройства, и чья, собственно, информационная система, если устройства в ней – не принадлежат ее владельцу.

Эти процессы усилились и ускорились внезапно возникшей экстренной потребностью в переходе на дистанционную работу, но и без этого тенденция вырисовывалась вполне ясно – по мере «цифровизации» экономики. Так об этом написано в аннотации книги [4]: «Мир внезапно изменился – и все прежние наработки в области технической защиты информации резко, более чем наполовину, потеряли свою актуальность. Корпоративные системы, конечно, остались – но появились новые, открытые компьютерные системы цифровой экономики. И они немедленно стали важнейшими – а методов защиты их нет. «Здесь и сейчас» – вот лозунг цифровой экономики. Но как понять, «где» и «когда», если на пути к этому стоят полное отсутствие методов идентификации в открытой среде – а ведь нужно знать, кому мы оказываем услугу. Как применять криптографию – если пользовательские устройства недоверенные? На какую нормативную базу опираться – если для открытых систем ее нет совсем?!».

Пересмотр понятия «граница защищенной информационной системы» необходим именно в этом смысле. В смысле перехода от его «пространственного», физического понимания к логическому. Главное же должно остаться неизменным – все, что в границах защищенной ИС, должно контролироваться. В этой главе рассмотрим, как.

4.1. Удаленка

Итак, добавление в состав информационной системы (ИС) удаленного пользователя эквивалентно изменению границ системы и появлению связанных с этим рисков. В частности, удаленный пользователь и его рабочее место, как правило, размещаются за пределами контролируемой зоны, что снижает уровень защищенности системы. «Как правило», потому что удаленным доступом называется и доступ из территориально распределенных подразделений компании к серверам в ЦОД, а это совершенно другая ситуация, в этом разделе речь идет не о ней.

Рассмотрим в качестве примера ГИС 1-го класса, поскольку в этом случае можно минимизировать оговорки типа «если это определено моделью угроз» и «в соответствии с политикой безопасности», так как свобода ослабления требований регулятора в случае с ГИС 1-го класса минимальна, а добровольное усиление требований в соответствии с представлениями об особенностях эксплуатируемой системы – редкое, хоть и отрадное явление. Требования к ГИС 1-го класса заданы [5] и на них можно опираться без дальнейших оговорок. Нас будет интересовать защита клиентского компьютера.

Очевидно, что при снижении контролируемости, а тем более – при исчезновении некоторых функций контроля, соответствующие (связанные с ними) функции защиты в процессе функционирования системы ослабляются, что ведет к снижению защищенности системы в целом.

Для сохранения достаточного уровня защищенности системы нужно принимать дополнительные – компенсирующие – меры, применять дополнительные средства обеспечения защиты, которые бы компенсировали возникающие риски удаленного доступа. Так, при возникновении в системе неконтролируемой зоны или недоверенного пространства возникает необходимость применения средств криптографической защиты информации.

На первый взгляд это кажется не вполне очевидным – казалось бы, ослаблены совсем не те меры контроля, вовсе не связанные с криптографией.

При обычной организации работ пользователь использует этот компьютер в своем офисе, за своим рабочим столом, в контролируемой зоне, и компьютер подключен к ЛВС, не имеющей выхода в Интернет или имеющей выход через все необходимые защитные механизмы.

При этом контролируется и фиксируется вход в офис и в конкретное помещение. Контролируется и регистрируется доступ к компьютеру. Используется контролируемая и защищенная локальная вычислительная сеть.

При чем тут криптография? Первое и очевидное – при том, что передача данных производится по защищенным каналам, а в случае удаленки – по незащищенному. Средство защиты канала, каким бы оно ни было (VPN, TLS, SSL) – это СКЗИ, ни что иное.

Кроме этого, невозможность применения мер контроля доступа, наблюдения за пользователем – ставит под сомнение аутентичность и целостность получаемых от него сообщений и производимых им действий в целом. Если возникают какие-то сомнения в том, что за рабочим местом именно тот сотрудник, который должен быть, при работе в офисе есть масса возможностей снять эти сомнения – есть данные СКУД о том, что он пришел на рабочее место, его видят другие сотрудники, наконец, возможно, есть данные видеонаблюдения. При невозможности принять эти простые, но действенные меры, необходимо использование криптографии – электронной подписи (если речь идет о документах) или кодов аутентификации, если речь идет о технологических операциях (с точки зрения математики – и то, и другое – электронная цифровая подпись, разница (и существенная!) в нормативном методическом обеспечении).

Теперь рассмотрим несколько основных вариантов организации удаленного доступа.

Вариант 1. Защищенный в соответствии с требованиями к ГИС 1 класса [5] компьютер устанавливается на территории пользователя (проще говоря, у него дома), и используется как в автономном режиме, так и в режиме доступа к информационным ресурсам ГИС.

Поскольку компьютер размещен за пределами офиса, канал связи необходимо защитить. Для этого на компьютере дополнительно необходимо установить систему криптографической защиты информации (СКЗИ), сертифицированную ФСБ России. Класс СКЗИ – не менее КС2, это минимальный уровень в условиях, когда нарушитель может получить доступ к компьютеру. Конечно, класс КС3 предпочтительнее, но ни при каких обстоятельствах нельзя использовать СКЗИ класса ниже КС2 (до сих пор часто встречаются попытки использовать СКЗИ класса КС1 – вот это недопустимо совершенно).

Сертификация СКЗИ на класс КС1 не требует, чтобы при использовании СКЗИ принимались меры по защите ключей. А значит, такие меры и не реализуются ни в самих СКЗИ, ни в виде ограничений и требований в их документации. А в результате злоумышленнику уже не нужно направлять свои усилия на вскрытие шифра (что сложно, если СКЗИ сертифицировано), достаточно завладеть криптографическими ключами, мер по защите которых не принимается.

В целях защиты криптографических ключей **целесообразно применять решения, при которых ключи будут недоступны никому из персонала и будут храниться в неизвлекаемом виде** (подробнее об этом, в частности, про «атаку Грунтовича» можно прочитать в [4. С. 211–217; 6]).

В 1 главе уже упоминалось, что применение СКЗИ класса КС2 и выше требует обеспечения СФК (напомню – среды функционирования криптографии), важнейшими требованиями к которой, в свою очередь, является обеспечение линейности загрузки и и/а пользователя до загрузки ОС.

Все это сделать вполне реально, но цена подготовки клиентского компьютера по этому варианту удаленного доступа – около 100 000 руб., с учетом АПМДЗ, СКЗИ и других необходимых СЗИ.

Сегодня весьма популярна (и в смысле предложения, и в смысле спроса) возможность приобретения защищенного рабочего места сразу «под ключ», к таким решениям относится и упомянутый в 1 главе защищенный планшет «ПКЗ 2020», который, являясь решением «СКЗИ ready», может поставляться как интеграторам для установки СКЗИ самостоятельно, так и конечным заказчикам с СКЗИ, предустановленным по их заказу [7][28].

При этом на ответственности работодателя будет установка правильного средства доверенной загрузки в обеспечение требования УПД.17[29] и требований ФСБ России, что, в общем, ему пришлось бы сделать и для работы сотрудника в офисе. А вот нагрузка на пользователя в этом варианте доступа существенно увеличивается в связи с необходимостью строго следовать инструкции при работе с СКЗИ, которые в части мер по безопасности СВТ исполнить не так уж просто.

Отдельно следует подумать о выполнении требований по защите технических средств (ЗТС), и, в частности, ЗТС.2 – «организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения

---

[28] Любопытным ответвлением от этого применения является заказ версий планшета «ПКЗ 2020» для работы «в полях», то есть для сотрудников, которые должны работать не просто вне офиса, а вообще вне какого-либо стационарного помещения. Это не только приходящие в голову в первую очередь полицейские, очень похожи задачи логистики, инспекторов и аудиторов, переписчиков. Так, защищенный планшет ОКБ САПР, правда, не «ПКЗ 2020» (он появился позже), а планшет TrusTPad [8] на Новой гарвардской архитектуре, использовался при сельскохозяйственной переписи в 2016 году.

[29] УПД.17 – это «обеспечение доверенной загрузки средств вычислительной техники» [5, 2], мера, обязательная, начиная со 2 класса ГИС и со 2 уровня защиты ПДн.

функционирования». Ответственность за организацию контролируемой зоны в этом случае возлагается на пользователя, а руководитель должен объяснить, что входит в это понятие, и проконтролировать, что получилось. Удалось ли пользователю ограничить физический доступ к компьютеру различных посторонних (соседей, детей, и др.), исключить несанкционированный просмотр экрана (например, гостями), используется ли защита от внешних воздействий (жарко, холодно, броски питания и др.).

В целом, это возможно, и обеспечить выполнение мер – необходимо.

Отметим, что выполнение многих требований по ЗТС при применении планшета значительно проще: его вполне естественно и несложно носить с собой (не оставляя без надзора, когда покидаешь помещение), его расположение в пространстве легко менять так, чтобы никто не мог видеть экран, в том числе через окна и другими экзотическими способами, он менее зависим от качества электрической сети, так как в основном работает от батареи, и так далее.

Вариант 2. Защищенный компьютер в месте расположения пользователя отсутствует, а ему нужно по долгу службы получать кратковременный доступ к ГИС.

Что делать в этом случае?

Кратковременный доступ должен предоставляться в рамках доверенного сеанса связи (ДСС) с использованием средства обеспечения доверенного сеанса (СОДС) [9], им в этой книге посвящен раздел 1.3.3. Длительность сеанса должна составлять не более 20 минут, при использовании проверенных решений вероятность успешной атаки за это время низкая.

Особенность этого типа доступа – кратковременность. Если сценарий работы другой, и доступ нужен длительный, то этот вариант использовать неверно.

Как мы уже знаем, при организации ДСС загрузка сертифицированной ОС должна осуществляться с носителя, обеспечивающего ее неизменность – в качестве такового обычно применяется носитель в форм-факторе USB [9, 10, 11].

Этот носитель должен обладать определенными специальными свойствами, которые обеспечат защищенность сценария:

- включать в себя инструменты идентификации/аутентификации пользователя и передачи этих данных в ГИС;
- обеспечивать целостность ОС и СКЗИ при хранении на СОДС;
- обеспечивать целостность ОС и СКЗИ при исполнении на компьютере средствами динамического контроля целостности оперативной памяти, сертифицированными ФСТЭК России;
- обеспечивать ведение и хранение журналов идентификации / аутентификации в защищенном и некорректируемом виде;
- иметь возможность настройки на интернет, настройки должны храниться в защищенной памяти СОДС;
- обеспечивать неизвлекаемость криптографических ключей для тех СКЗИ, что исполняются на самом СОДС (тут нужно понимать, что такие СКЗИ используются для каких-то отдельных преобразований, например, на нем может быть реализована функциональность СЭП, но не могут использоваться, например, для защиты канала – для таких ресурсоемких действий необходимо СКЗИ, загружаемое на компьютер).

Также, поскольку компьютеры любые, появляются требования к ОС, загружаемой с СОДС – например, настройками исключить все, кроме самого необходимого (монитор, клавиатура, мышь, Интернет).

Рядом характеристик должна обладать и сама ГИС, в которой будет разыгрываться сценарий ДСС:

- возможность получать по защищенному каналу результаты идентификация и аутентификация, осуществленной средствами СОДС, и использовать эти результаты;

• в составе ИС должен быть отдельный LDAP, МЭ, криптошлюз и другие периферийные СЗИ, по параметрам защищенности соответствующие требованиям к мерам защиты ГИС.

С учетом перечисленных специальных свойств носителя, архитектуры системы и кратковременности сеансов можно сформулировать следующие особенности этого сценария:

• В состав ИС включаются СОДС – значит, нужны изменения в аттестационные материалы[30];

• Идентификация и аутентификация осуществляется средствами СОДС, результаты передаются по защищенному каналу в ГИС;

• Внутреннего нарушителя нет, потому что СОДС – персональное устройство;

• Внешний нарушитель – Н1, значит, СКЗИ – КС1, поскольку внешний нарушитель не имеет доступа к средствам СКЗИ (так как СОДС – персональное устройство), а при передаче по защищенному каналу связи данные, зашифрованные СКЗИ, сертифицированным на КС1 и на КС2 (или выше) – ничем не отличаются, разница между классами СКЗИ в том, какие условия его функционирования должны быть обеспечены, а не в том, как оно шифрует;

• Эксплуатация СКЗИ осуществляется вне контролируемой зоны (это означает, что нужны СКЗИ, сертифицированные именно для такого применения, либо принятие специальных организационных мер, если они предусмотрены правилами пользования СКЗИ);

• К компьютеру требования не предъявляются, поэтому на него никакие средства защиты не устанавливаются;

• Целостность ОС и СКЗИ, исполняемых на компьютере, при хранении на СОДС обеспечивается средствами СОДС;

---

[30] Если система аттестована, то просто так в ней нельзя ничего изменить, в том числе добавить что-то новое – все изменения должны быть документированы, а также пройдена специальная процедура – менее сложная, чем аттестация, но не тривиальная, для получения минимальных установочных представлений можно почитать в Интернете о том, что такое «аттестация информационной системы»

• Журналы идентификации/аутентификации ведутся и хранятся в защищенном и некорректируемом виде (средствами СОДС);

• Настройки на интернет задаются СОДС, хранятся они в защищенной памяти СОДС;

• При использовании СКЗИ, исполняемых на средствах СОДС, неизвлекаемость криптографических ключей обеспечивается средствами СОДС;

• ГИС защищена всеми необходимыми средствами периферийной защиты.

От пользователя в этом случае потребуется обеспечивать установленную длительность ДСС и хранение СОДС в условиях, исключающих доступ к нему третьих лиц.

Вариант 3. Используется незащищенный компьютер пользователя, но для подключения к ГИС используются специальные средства вычислительной техники удаленного доступа (ССВТ УД), блокирующие уязвимости, появившиеся при удаленной работе сотрудников. ОКБ САПР разработан вариант ССВТ УД на платформе m-TrusT[31] [12]. Он поставляется под торговым названием «TrusT Удалёнка». Решение сертифицировано ФСБ по классу КС3.

Схему работы при использовании ССВТ УД «TrusT Удалёнка» опишем следующим образом. К компьютеру пользователя подключен микрокомпьютер. На нем есть терминальный клиент, настроенный на соединение с ГИС. При необходимости подключения к ГИС, с этого микрокомпьютера на компьютер пользователя загружается технологическая ОС с терминальным клиентом, и микрокомпьютер становится для компьютера пользователя терминальным сервером. То есть он одновременно терминальный сервер для компьютера пользователя и терминальный клиент для ГИС.

[31] Предполагается, что о компьютерах Новой гарвардской архитектуры вы получили некоторое представление по ссылкам из раздела 1.3.2.

Чтобы оценить защищенность технологии, посмотрим, что где выполняется. У нас есть компьютер пользователя – он, как мы считаем, не защищен совершенно (если пользователь чем-то его защищает – хорошо, но на это не стоит рассчитывать, это его личное дело и его право), есть «TrusT Удалёнка» – этот микрокопьютер хорошо защищен и вычислительная среда на нем доверенная. И есть серверная часть ГИС (это ГИС – потому что мы с вами так условились в начале раздела, в реальности это может быть любая корпоративная ИС), которая находится в контролируемой зоне и по умолчанию ее защищенность не вызывает вопросов.

• *На компьютере пользователя выполняется:*

- PXE-загрузчик, интегрированный в BIOS,
- технологическая ОС, загружаемая с «TrusT Удалёнка»,
- ПО терминального клиента (в ОС, загруженной с «TrusT Удалёнка»);

• *На «TrusT Удалёнка» исполняется:*

- СДЗ уровня BIOS Аккорд-МКТ (сертифицированное ФСТЭК России),
- российская ОС, в которой:
    - ПО терминального сервера (навстречу ПЭВМ),
    - ПО терминального клиента (навстречу ГИС),
    - драйвера сети,
    - браузер,
    - TFTP-сервер (поддержка загрузки по PXE),
    - Аккорд-Х К (для изоляции программной среды по требованиям ФСБ России, сертифицирован ФСТЭК России),
    - СКЗИ DCrypt (сертифицирован ФСБ России на платформе m-TrusT на класс КС3).

• *На серверной части ГИС выполняется* все то функциональное ПО с которым в режиме удаленного доступа (терминальной или web-сессии) работает пользователь.

Сравним технологии СОДС и ССВТ УД.

При сравнении технологий нужно учесть:

1. Загрузка образа на недоверенный компьютер пользователя из m-TrusT и из СОДС почти равноценны с точки зрения безопасности. Однако при использовании микрокомпьютера загружаемый образ минимизирован существенно больше, чем в случае с СОДС, так как его задача – только поддержка терминального клиента. Большая часть компонентов, при использовании СОДС загружаемых на недоверенный компьютер, исполняются на доверенном микрокомпьютере. Это означает, что вариант с использованием микрокомпьютера все же лучше.

2. Требование УПД.17 – доверенная загрузка компьютера, на котором исполняется ПО доступа к ГИС – выполняется при работе с микрокомпьютером, и *не выполняется при загрузке с флешки*, так как при загрузке с флешки не проводится контроль целостности программного обеспечения и аппаратных компонентов *средств вычислительной техники*. При загрузке микрокомпьютера этим СВТ и является сам микрокомпьютер, и такой контроль производится СДЗ. В случае с СОДС – этим СВТ, на которое загружается ОС, является компьютер пользователя. Контроль целостности его аппаратных средств не производится. Здесь отметим, что в некоторых рекламных материалах встречается утверждение о том, что «микроконтроллер флешки загружается доверенным образом». Но доверенная загрузка флешки не означает доверенной загрузки того СВТ, на котором будет исполняться СКЗИ (оно будет исполняться на компьютере пользователя). Это подмена понятий, необходимо хорошо это понимать и не поддаваться на похожее звучание фраз. Доверенной должна быть загрузка именно СВТ, на котором исполняются СКЗИ и ПО ГИС.

С учетом отчуждения средств доступа к ГИС, в том числе криптографических, от недоверенного компьютера, при доступе с использованием «TrusT Удалёнка» получаем следующие преимущества (см. таблицу 4.1).

Таблица 4.1. Изоляция исполнения компонентов ПО от ресурсов недоверенной ПЭВМ при использовании технологий ДСС и «TrusT Удалёнка»

№	функция	Изоляция исполнения от ресурсов ПЭВМ	
		СОДС	m-TrusT
1	ОС	- исполняется на ПЭВМ	+ исполняется на m-TrusT
2	СКЗИ	- загружается в память ПЭВМ и там исполняется	+ размещается и исполняется на m-TrusT
3	Ключи СКЗИ	- применяются там, где СКЗИ, то есть на ПЭВМ	+ не попадают в память недоверенной ПЭВМ
4	ПО ТК	- исполняется на ПЭВМ	+ исполняется на m-TrusT
5	Сетевое ПО	- исполняется на ПЭВМ	+ исполняется на m-TrusT
6	Браузер	- исполняется на ПЭВМ	+ исполняется на m-TrusT

Есть еще несколько факторов в пользу решения «TrusT Удаленка». За счет реализации в m-TrusT функции неизвлекаемого ключа, использовать ключ (без замены) возможно до 3-х лет. Это существенно, так как замена ключей – хлопотная процедура, и за время жизни ключа стоит «бороться».

Кроме того, при использовании «TrusT Удаленка» не требуется дополнительный ключевой носитель, а значит, и меры по контролю этих носителей, так как m-TrusT в этом решении является персональным устройством.

Отметим, что требования ЗТС должны выполняться и в этом случае.

Подводя итог сказанному выше, можно отметить, что решения на базе СОДС (в том числе «МАРШ!» и LiveOffice) можно использовать в ГИС 3-го класса защищенности, а для ГИС высоких классов можно рекомендовать использовать защищенные планшеты или ССВТ УД «TrusT Удалёнка», как решение более стойкое и недорогое.

4.2. Объекты критических информационных инфраструктур «в полях»

В определенном смысле задача защиты объектов критических информационных инфраструктур (КИИ), расположенных вне контролируемых зон, имеет сходство с задачей организации защищенной «удаленки». В том смысле, что некоторое техническое средство, являющееся частью системы, но расположенное где-то удаленно, должно взаимодействовать с защищенной серверной частью информационной системы, и делать это защищенно. Однако КИИ имеют очень существенные отличия от информационных систем с рабочими местами офисного типа. И в этом смысле, у таких нетривиально размещенных объектов КИИ больше общего все же с остальными объектами КИИ, чем с нетривиально расположенными техническими средствами для решения офисных задач. Чтобы создать контекст для разбора особенностей, необходимо коротко обрисовать, в чем общие черты всех объектов КИИ, и чем они отличаются от большинства других защищенных информационных систем.

Технические меры, которые должны приниматься для обеспечения безопасности объектов КИИ, не являются какими-то принципиально отличными от тех, что должны приниматься в ГИС или системах обработки ПДн высоких классов. Регулируется обеспечение безопасности КИИ Федеральным законом № 187-ФЗ [13] и его подзаконными актами[32]. В части технической защиты информации – это в первую очередь приказы ФСТЭК России № 235 [14], 239 [15] и в части АСУ ТП – № 31 [16]. Однако при переходе к планированию выясняется, что с реализацией этих мер на практике возникает ряд сложностей.

Эти сложности в существенной мере связаны с тем, что объекты защиты информации всех типов (технические средства, данные,

[32] Краткий обзор этих нормативных методических документов можно прочитать, например, на сайте ОКБ САПР: https://www.okbsapr.ru/products/newharvard/m-trust/short-review/.

информационные технологии, каналы передачи данных), в КИИ крайне разнообразны[32], намного разнообразнее, чем в среднем в защищенных корпоративных или государственных информационных системах (см. табл. 4.2 и рис. 4.1).

Таблица 4.2. Особенности объектов защиты информации в КИИ

Объекты защиты информации	«обычные» защищенные ИС	КИИ
Технические средства	Сервера, ПК, терминалы	То же, плюс управляющие элементы КИИ, разнообразные датчики и контроллеры
Данные	Файлы и данные	То же, плюс сигналы управления, данные измерений и контроля
Каналы	Ethernet	То же, плюс WiFi, BlueTooth, LTE и др.
Информационные технологии	Прикладное и системное ПО	То же, плюс ПО управления технологическими процессами

Рисунок 4.1. Объекты защиты информации в КИИ

[32] Речь, разумеется, идет о некой обобщенной картине, так как какая-то конкретная КИИ может быть построена преимущественно из самых обыкновенных офисных ПК, а система, не являющаяся КИИ, может состоять из оборудования, нисколько не похожего на ПЭВМ. Подробно в вопросах о том, что является КИИ, и что из этого вытекает, вы будете разбираться на 4 курсе, в рамках дисциплины, посвященной изучению нормативной методической базы.

Что особенно важно – все это разнообразие практически не может быть унифицировано.

Особенно выпукло картина выглядит на примере защиты сетевого взаимодействия объектов КИИ. Обменивающиеся по сети разнообразными данными и сигналами технические средства объектов КИИ не только сами по себе разнообразны, но и располагаться могут весьма нетривиальным для обычных информационных систем образом – не только на стационарных, но и на мобильных и даже подвижных объектах[33].

При этом на всех местах выработки должны защищаться все сигналы и все каналы передачи данных: защищено должно быть все, а не только информационный уровень системы.

В подавляющем большинстве КИИ обязательной частью системы защиты сетевого взаимодействия являются средства криптографической защиты информации (СКЗИ), поскольку, как уже упоминалось, некоторые объекты КИИ взаимодействуют по незащищенным сетям общего доступа, причем с использованием стандартных цифровых каналов типа WiFi, BlueTooth и LTE. Изменение порядка взаимодействия с построением выделенных защищенных каналов не всегда возможно в принципе, а когда и возможно – то влечет за собой весьма продолжительные и дорогостоящие работы, несопоставимые с внедрением СКЗИ[34]. Если же используются незащищенные сети общего доступа, для защиты канала связи должны использоваться СКЗИ. Со стороны СКЗИ же, в свою очередь, предъявляются требования к среде функционирования криптографии (СФК), условиям хранения и применения ключей и т. п.

---

[33] Хотя необходимо признать, что и стационарные объекты могут ощутимо различаться – от центрального офиса до станции общественного транспорта или, скажем, маяка, но все же размещение мобильных (банкомат, инфокиоск), а особенно – подвижных объектов (поезд, автомобиль инкассации, скорая помощь, корабль) отличается еще большей непредсказуемостью.

[34] Откровенно говоря, даже не смешно представить себе такую постановку задачи для стоящего «в чистом поле» банкомата.

Фактически, в части защиты сетевого взаимодействия все специфичное в требованиях к КИИ сводится к тому, что при взаимодействии с использованием сетей общего доступа каждый узел должен быть защищен СКЗИ высокого класса.

Все остальное – *следствия* из этого обстоятельства.

Рассмотрим на примере защиты банкоматов те из следствий этого требования, которые определяют необходимые свойства платформы средства защиты для КИИ.

4.2.1. Среда функционирования криптографии

Для оборудования каждого узла СКЗИ, сертифицированным на высокий класс, неприемлемо использовать установленный на технические средства программный VPN. Даже в случае, если для него создана и поддерживается СФК. Недопустимо потому, что при работах по обслуживанию в ПО этого компьютера могут быть внесены изменения, нарушающие СФК, а значит, после каждой из таких работ должны проводиться специальные проверки. Это, конечно, совершенно невозможно организационно. Более того, в случае с рядом специфических объектов КИИ вообще возможна ситуация, что непредсказуемые изменения – например, замена преступником штатного компьютера на свой, «улучшенный» – будут произведены, например, при работах вообще не с компьютером, а с какими-то другими техническими средствами объекта – например, с диспенсером банкомата: объекты КИИ зачастую обслуживаются большим количеством технического персонала, среди которого может скрываться злоумышленник (этот ход вы часто видели в кино – в форме обслуживающего персонала преступник никому не бросается в глаза, что бы он ни делал).

Ситуация выглядит несколько лучше при использовании аппаратного шлюза, однако, использование импортных устройств неприемлемо по причине их несоответствия требованиям регуляторов,

а отечественные сертифицированные устройства в этом качестве, как правило, не используются, потому что они очень дорогие и очень большого размера. Выглядят они так.

Рисунок 4.2. Внешний вид некоторых типичных российских аппаратных криптошлюзов

Установить такие машины в каждый банкомат, электричку, машину инкассации, скорую помощь и инфокиоск довольно сложно (поскольку они дорогие и велики по размеру), а кроме того, эти устройства избыточны по своим характеристикам и зачастую подвержены множеству уже хорошо разработанных и постоянно появляющихся новых атак.

4.2.2. Неизвлекаемый ключ

Еще одно требование, которое вытекает из того, что СКЗИ расположено вне контролируемой зоны и отсутствует доверенный оператор, – неизвлекамый ключ. Казалось бы, эта тема должна быть раскрыта в современных СКЗИ в полной мере, однако и здесь есть важные для применения в КИИ особенности.

«Неизвлекаемость» – свойство, описывающее связь ключа с некоторым его физическим хранилищем (из которого он не извлекается). То есть говоря о том, что ключ неизвлекаем, необходимо уточнять, откуда. Неизвлекаемые ключи как правило неизвлекаемы из

токена, который, как правило – USB-устройство, смарт-карта или «таблетка» Touch Memory. Читая документы на СКЗИ высоких классов сертификации для защиты канала, мы видим, что «требование неизвлекаемости ключа выполняется применением токена…». Это добросовестное выполнение требования, однако, токен с неизвлекаемым ключом – это инструмент решения совсем другой задачи, существенно отличающейся от защиты сетевого взаимодействия объектов КИИ. Токен предназначен для того, чтобы ключ *пользователя* был *отчуждаем от СВТ*, на котором пользователь осуществляет те или иные операции с ключом. Токен *может* обеспечивать и неизвлекаемость, но *назначение* его в том, чтобы обеспечить *отчуждаемость*. В описываемом же случае отчуждаемость не только избыточна, но и вредна: с одной стороны, она делает возможными сценарии атак с подменой или иными вариантами компрометации ключа за счет отчуждаемости (и стало быть – возможности замены) его носителя, а с другой, подключенное к порту USB-устройство резко снижает надежность решения – при вибрации, ударах, нагревании и прочих особенностях условий, в которых работают технические средства на объектах КИИ.

Модуль работы с неизвлекаемым ключом на технических средствах объектов КИИ должен быть реализован как часть резидентного компонента безопасности, размещенного непосредственно на плате компьютера, а не как отчуждаемый персональный носитель ключа.

4.2.3. Коммутация с СВТ

Задачи коммутации и использования широкого спектра каналов и протоколов связаны уже не с требованиями регуляторов, а с техническими особенностями объектов КИИ. В средстве защиты необходимо поддержать множество различных интерфейсов обмена

данными, которые тоже, естественно, поддерживаются именно аппаратно.

Отсюда недвусмысленно вытекает набор свойств, которыми должна характеризоваться платформа[35] средства защиты сетевого взаимодействия между объектами КИИ:

1. возможность создавать и поддерживать доверенную вычислительную среду,
2. возможность работы с неизвлекаемым ключом в автоматическом режиме,
3. возможность установки различных СКЗИ с соблюдением условий сертификации на высокие классы,
4. возможность работы с различными каналами связи по различным протоколам, в том числе, параллельно,
5. возможность коммутации с различным оборудованием объекта КИИ без модификации последнего.

Возможность коммутации без модификации самого технического средства – это крайне важная особенность, так как в отношении некоторых объектов КИИ модификацию ради установки СКЗИ нелепо даже теоретически рассматривать (оцените сами, насколько разумно звучит требование модифицировать объект АЭС или самолетостроительного предприятия?).

Всем этим требованиям отвечает специализированный компьютер с аппаратной защитой данных m-TrusT (это не совпадение, он разрабатывался специально для этого, по этим требованиям).

Его особенностями являются:

- Новая гарвардская архитектура, обеспечивающая вирусный иммунитет,
- аппаратная поддержка реализации доверенной загрузки,
- функциональная замкнутость среды,
- аппаратное обеспечение целостности,

[35] В этом месте вы можете задаться вопросом, почему «платформа», а не само средство защиты. Это правильный вопрос, чуть ниже к нему вернемся.

- аппаратное резидентное решение по неизвлекаемости ключа,
- аппаратный ДСЧ.

Как видите, эти особенности никак не затрагивают вопросов коммутации. За эти вопросы отвечают не архитектурные особенности, а форм-фактор и эксплуатационные требования, с соблюдением которых будет изготовлен компьютер.

Попробуем вывести эти требования.

Для этого сначала сформулируем, в чем проблема, почему для коммутации с объектами КИИ требуется что-то принципиально отличное от обычных средств защиты информации. Проблема в том, чтобы поддержать разнообразные технические средства, разнообразные цифровые каналы (WiFi, LTE, возможно, BlueTooth), разнообразную каналообразующую аппаратура (RS232, RS435 и др.), при этом минимизировав возможные сложности при вводе системы защиты в эксплуатацию. То есть СКЗИ, устанавливаемые на различные объекты, должны быть полностью совместимы и не требовать сложной интеграции и переучивания персонала.

Вариант с модернизацией объектов КИИ мы уже отбросили (очевидно, что неверно переделывать электрички или оборудование электроподстанции так, чтобы в них удобнее устанавливались СКЗИ – это очень дорого и долго). Что еще можно сделать?

Можно для каждого объекта КИИ разработать, изготовить и сертифицировать собственное множество аппаратных СКЗИ. Это дорого и очень долго (сертификация СКЗИ на КС2 и выше занимает несколько лет для каждого решения).

Остается вариант создать специальную аппаратуру, обладающую всеми необходимыми свойствами, и особенностью которой будет простейшая модернизация к любым объектам и каналам, не требующая проведения повторной сертификации. Адаптация СЗИ к техническим средствам объектов КИИ позволит сохранить инвестиции в КИИ.

Однако адаптация СЗИ, а особенно – СКЗИ – это повторная сертификация. Звучит как замкнутый круг, однако, по существу, это инженерная задача, причем теперь, когда она уже решена, она представляется даже не такой уж и сложной.

Решается задача путем декомпозиции: разделения СЗИ на то, что должно быть неизменным, чтобы не требовалось повторной сертификации, и то, что может меняться для того, чтобы интегрироваться с очередным техническим средством на очередном объекте КИИ.

Нужно выделить аппаратное ядро (оно будет неизменной средой функционирования СКЗИ), а встраивание выполнять за счет создания несложных интерфейсных плат, не связанных с выполнением криптографических преобразований, но обеспечивающих транспорт и необходимый форм-фактор.

Ядро проектируется как универсальное, множество интерфейсных плат может быть огромно, форм-факторы разнообразны и зависят только от особенностей объектов КИИ.

Именно таким решением и является платформа m-TrusT.

Платформа – это сам микрокомпьютер Новой гарвардской архитектуры m-TrusT, а решение на этой платформе при необходимости включает ту или иную интерфейсную плату для коммутации компьютера с сетевой инфраструктурой. А может и не включать, если микрокомпьютер включается в состав технического средства уже при проектировании – например, в состав терминала биометрического контроллера СКУД, «Сапсана» или дрона-беспилотника.

Изменения интерфейсной части, выделенной в отдельную плату, не влияют на вычислительную часть компьютера, а это снимает основные сложности, вызываемые адаптацией серийного продукта – возможное внесение новых ошибок или дефектов, необходимость повторных проверок или сертификации и т. п. Ядро универсально, а интерфейсные платы обеспечивают только транспорт.

Каждый микрокомпьютер «m-TrusT» является точкой сбора информационных и/или управляющих сигналов от объектов КИИ, их шифрования для передачи по каналам связи, а также приема зашифрованных сигналов из каналов связи и их расшифровки.

Типовые характеристики микрокомпьютеров можно увидеть на сайте[36].

Общий вид микрокомпьютера m-TrusT представлен на рисунке 4.3.

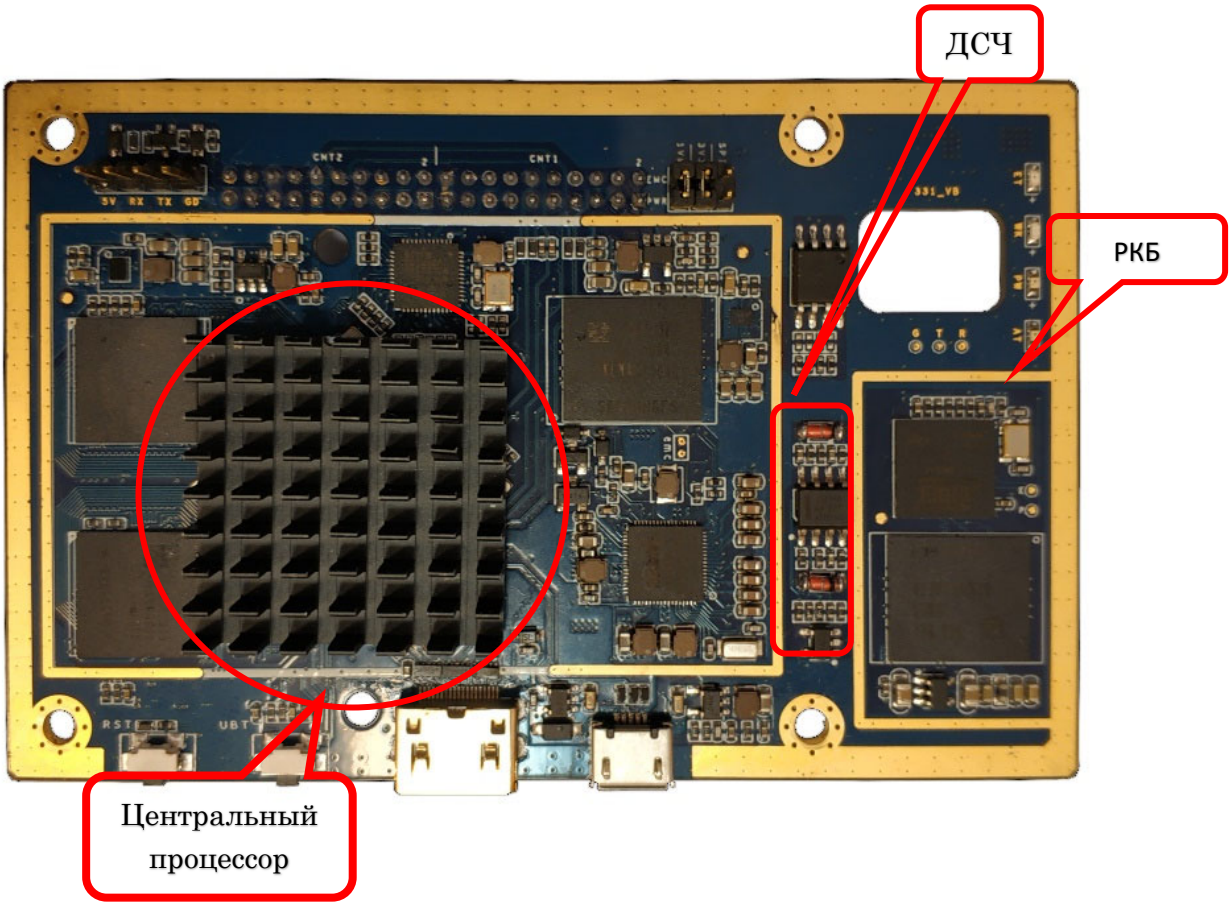


Рисунок 4.3. Общий вид микрокомпьютера m-TrusT

Микрокомпьютер не подключается напрямую ни к чему, кроме собственной интерфейсной платы, поэтому его состав не сложен и постоянен. Интерфейсная плата же нужна как раз для того, чтобы корректно подключиться к тому или иному конкретному

[36] https://www.okbsapr.ru/products/newharvard/m-trust/

подконтрольному объекту и каналообразующей аппаратуре различных типов.

Как уже упоминалось – разнообразие оборудования, взаимодействующего по сети (ПК, скорая помощь, банкомат, электричка, информационный киоск, машина инкассации, терминал оплаты etc), является ключевой характеристикой инфраструктуры, поэтому интерфейсные платы должны быть ***разными***, чтобы коммутировать ***одно и то же*** СЗИ (то есть не *совместимые*, не *похожие*, а именно *одинаковые* СЗИ) с разными ПКО. Например, она может быть такой, как на рисунке 4.4:

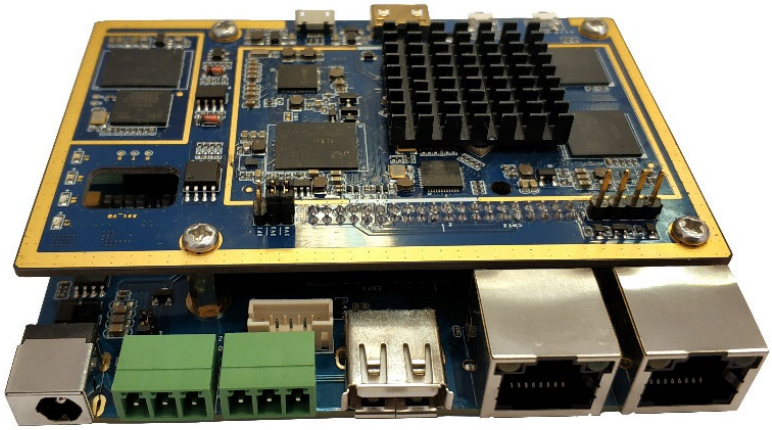


Рисунок 4.4. Микрокомпьютер m-TrusT, подключенный к интерфейсной плате

Другие фотографии, а также наборы характеристик различных интерфейсных плат также можно увидеть на странице продукта на официальном сайте разработчика и в [4].

Для некоторых объектов, как показала практика, удобным может быть исполнение в едином корпусе, например, если частого переоборудования не требуется, а техническое средство функционирует вне помещения, где внешние условия могут быть разнообразными и не всегда благоприятными. В этом случае корпус снижает возможное воздействие внешних условий.

Разумеется, за счет описанных особенностей, построенное на платформе m-TrusT решение может поддержать любой из вариантов

связи объектов, или даже все их одновременно, причем с дублированием каждого канала (несколько каналов Ethernet, несколько sim-карт для мобильного Интернета и т. д.), с тем чтобы во время работы использовать тот, что доступен в данный момент и в данном месте.

Описанная архитектура с интерфейсными платами обуславливает возможность построения на базе специализированного компьютера с аппаратной защитой данных m-TrusT широкого спектра инфраструктурных решений, которые могут очень существенно различаться между собой по функциональному наполнению. Именно в этом смысле m-TrusT – это платформенное решение, и все сформулированные требования к нему – это требования к платформе. А средство защиты на этой платформе может быть практически любым. В предыдущем разделе описано решение «TrusT Удаленка», о других решениях можно прочитать в Интернете, здесь ограничимся еще одним примером, а остальные вектора создания СЗИ на платформе m-TrusT зададим лишь в общих чертах.

4.2.4. Криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации fin-TrusT

С помощью криптошлюзов fin-TrusT защищаются коммуникации между подразделениями и офисами банков, банком и процессинговым центром, процессинговым центром и банкоматами. Выполняются требования законодательства, блокируются уязвимости во взаимодействии в финансовой сфере.

Рассмотрим банкомат как объект КИИ. В его составе есть диспенсер (в нем лежат деньги и из него деньги выдаются), компьютер и периферийное оборудование. Компьютер взаимодействует с процессинговым центром (например, по IP-протоколу), и USB-кабелями соединен с диспенсером и другим периферийным оборудованием.

При работе с банкоматом с пластиковой карты считывается ее номер, с клавиатуры – PIN, все это передается в процессинговый центр, где и выполняется авторизация. Если все в порядке – проверяется запрашиваемая сумма. Затем компьютером банкомата формируется команда на выдачу денег, которая передается в диспенсер. Из защитных механизмов здесь используется только один – диспенсер размещен в сейфе.

Напрашивается ряд очевидных направлений атак.

1. Атака на канал взаимодействия с процессинговым центром. Атака может быть реализована примерно так: вставляется любая карточка, вводится любой PIN, из процессингового центра приходит сигнал отказа в авторизации, но он подменяется сигналом успешной авторизации. При этом злоумышленнику достаточно иметь возможность вмешаться в работу канала, изменять логику работы банкомата необходимости нет.

2. Атака имитацией сигнала на выдачу денег. Команда на выдачу денег, которую исполняет диспенсер, формируется компьютером банкомата. А почему бы тогда злоумышленнику не использовать другой компьютер? Например, принести с собой ноутбук, отключить USB-кабель диспенсера от компьютера банкомата, подключить его к принесенному ноутбуку и подавать команды вида «дай 5000 рублей»? Естественно, диспенсер выполнит команду, если ее подать в нужном формате. Но это, конечно, дело техники и никакого труда не представляет. Эта же атака может быть реализована и по-другому. Так, злоумышленник может внедрить закладку в компьютер банкомата (это несложно сделать, например, во время выполнения профилактических работ). Логика работы вредоносной программы может быть любой: например, при предъявлении определенной легальной карты может запрашиваться подтверждение на выдачу 100 руб., а выдаваться вполне может значительно больше. Казалось бы, разные атаки, но они отличаются только нюансами реализации. Суть одна — на диспенсер подается команда, сформированная нештатными программными средствами.

3. Атака имитацией сигнала на прием денег. Можно смоделировать следующую несложную, но очень опасную атаку: предположим, клиент вносит 100 руб., а действиями закладки на его счет заносится значительно большая сумма, например 100 000 руб. Даже не ясно, можно ли будет этого клиента привлечь к ответственности (если поймают) — денег-то он не брал.

4. Сбор критичной информации пользователей. Если вредоносная программа внедрена, то что может помешать ей запомнить все номера карт и PIN в один день и все запросы на выдачу денег повторить в другое время по внешней команде — например, по предъявлении какой-то конкретной карты? Или просто передать эту информацию злоумышленникам?

Представляется, что такое перечисление возможных атак уже содержит ответ на извечный вопрос: «Что делать?». Надо защитить каналы с помощью СКЗИ высоких классов — как от процессингового центра к компьютеру, так и от компьютера к диспенсеру — и обеспечить целостность программно-аппаратной среды компьютера.

Применение СКЗИ высоких классов предписано и отраслевыми стандартами финансовой сферы. Так, согласно п. 3.1 Положения № 683-П [17], системно значимые кредитные организации, а также кредитные организации, значимые на рынке платежных услуг, должны реализовывать *усиленный уровень защиты информации* по ГОСТ Р 57580.1-2017 [18]. В данном ГОСТе *для усиленного уровня защиты информации предписывается использование СКЗИ, имеющих класс не ниже КС2*. Эти требования в первую очередь касаются именно контуров банковской инфраструктуры, предназначенных для банкоматов, взаимодействия с территориальными отделениями и других коммуникаций.

Защитить каналы – как от процессингового центра к компьютеру, так и от компьютера к диспенсеру, и обеспечить целостность программно-аппаратной среды компьютера по требованиям к СКЗИ высокого класса и при этом нетравматично для функционирования

системы и с сохранением инвестиций можно именно с помощью решения fin-TrusT на платформе специализированного компьютера с аппаратной защитой данных m-TrusT.

Криптошлюз fin-TrusT может быть как в форм-факторе, подходящем для банкоматов («fin-TrusT Банкомат»), так и в настольном и стоечном исполнении – для взаимодействия между отделениями, головным офисам и т. д., эта возможность обеспечивается платформой m-TrusT.

Далее – обещанные направления построения СЗИ на этой же платформе для различных отраслей деятельности.

4.2.5. Направления разработки других СЗИ на платформе m-TrusT

4.2.5.1. Безопасный город

Нас окружают камеры, данные с которых оказывают непосредственное влияние на принятие множества критически важных или просто значимых для конкретных граждан решений. Изображение с этих камер передается по каналам передачи данных общего пользования, вмешательство в этот процесс «человека посередине» не представляет для злоумышленника сложности. Называть такую инфраструктуру «Безопасным» городом – черный юмор.

Такая атака дает злоумышленнику возможность подменять данные на те, что позволят ему решить какие-то свои задачи, либо, что не менее опасно, особенно в условиях движения к биометрической идентификации, – накапливать данные о гражданах в целях дальнейшего использования в собственных целях.

Встраивание в камеры СКЗИ на платформе m-TrusT сделает процесс сбора данных с камер защищенным с максимально возможным сохранением инвестиций. Стоимость оборудования камер СКЗИ будет

ощутимо ниже замены всех камер на такие, в которые по умолчанию встроены средства шифрования аналогичного класса защиты.

4.2.5.2. Умный дом

«Умный дом» сейчас едва ли не в большей степени ассоциируется с опасностью, чем с прогрессом. Приборы, взаимодействующие по сети, в лучшем случае разовьют искусственный интеллект и взбунтуются (это оптимистический сценарий, потому что случится это очень нескоро), а в худшем – попадут под управление не собственного хозяина, а его недоброжелателя. Можно рисовать много сценариев развития этой ситуации – как смешных, так и страшных. Оставив эту задачу сценаристам, можно решить проблему радикально – защитить взаимодействие вещей, поскольку от этого взаимодействия зависят люди.

При этом сценарии m-TrusT со специализированной платой расширения становится концентратором потоков информационного взаимодействия в системах IoT (так называемого «Интернета вещей»). Преступник больше не сможет отключить ваш холодильник и включить кипяток в душе. Умный дом станет умнее – сможет отличать хозяина от преступника.

4.2.5.3. Безопасный транспорт

Представим себе железную дорогу как некоторый обобщенный эталонный макет транспорта вообще.

Если рассматривать ее с точки зрения сетевого взаимодействия объектов КИИ, то мы увидим три глобальных типа объектов: подвижные составы, станционное оборудование и некоторый центральный вычислительный центр.

Основное взаимодействие происходит между подвижными составами и центральным вычислительным центром (назовем его ЦВЦ).

Он рассылает расписание, аккумулирует данные от подвижных составов и рассылает сделанные на основании этих данных корректировки. Станционное оборудование также отправляет в ЦВЦ данные о движении подвижных составов и получает корректировки расписания, которые передает подвижным составам, а также выполняет различные вспомогательные функции, прописывать которые на уровне такой контурной обрисовки условной транспортной системы нет смысла. Подвижные составы также параллельно взаимодействуют со станционным оборудованием и с ЦВЦ, отправляя данные о своем движении и получая указания и корректировки. Очевидно, что нарушения этого взаимодействия может иметь крайне неприятные последствия, и так же очевидно, что средства защиты этого взаимодействия должны быть унифицированы, но в то же время адаптированы к работе в совершенно разных условиях. Бортовой компьютер подвижного состава работает в условиях вибрации и нагревания, и в целом он абсолютно не похож на ПК или сервер. На станциях оборудование представляет собой стойку серверов, ЦВЦ – это ЦОД с серверами огромной производительности. То есть это задача для платформы m-TrusT. Реализация СКЗИ на m-TrusT, с одной стороны, не имеет никаких ограничений по работе «навстречу» с реализациями этого же СКЗИ на любых других платформах, а с другой – позволяет организовать защищенное взаимодействие параллельно по разным каналам.

4.2.5.4. Умная энергетика

Объекты энергетики рассмотрим на примере электрических подстанций. Это объекты, предназначенные для приема, преобразования и распределения электричества. Многие из них расположены «в чистом поле» – на открытых пространствах, вдалеке от какой-либо инфраструктуры, и функционируют относительно автономно.

Такие объекты неизбежно вызывают повышенный интерес злоумышленников, о чем писал еще А. П. Чехов [19]. У электроподстанции нет ресурсов, позволяющих различать легальные и нелегальные запросы. Если ощутимо упростить, она постоянно отдает ток определенной мощности, а по сигналу (например, когда проезжает электричка) эту мощность существенно повышает. Подключение к подстанции с целью решения каких-то бытовых задач (получения бесплатного электричества, проще говоря) не только противозаконно, но крайне опасно – как для того, кто ворует (подача тока большей мощности может нанести ему различный вред, в зависимости от того, что именно и как он подключил), так и для всей инфраструктуры. Цифровые подстанции, имеющие в составе управляющего комплекса противоаварийную систему, могут расценить изменение нагрузки как аварию и включить противоаварийную автоматику – в этом случае целевые функции подстанции могут быть не выполнены в нужный момент, а к чему конкретно это приведет – зависит от того, в рамках какой инфраструктуры и для чего предназначена данная конкретная электроустановка.

Средство защиты, которое позволит отличать аутентифицированный и гарантированно неизмененный управляющий сигнал от воздействия «народных умельцев», позволит избежать этих негативных событий. Оно может быть построено на платформе m-TrusT. Для этого разработана специальная интерфейсная плата, позволяющая устанавливать м-траст в корпусе под DIN-рейку.

4.2.5.5. Умное производство

Сетевое взаимодействие технических средств объектов на производстве (классическое АСУТП – автоматизированная система управления технологическим процессом) характеризуется рядом важных особенностей.

Основной защищаемой информацией является технологическая (обеспечивающая управление технологическими или чувствительно важными процессами), программно-техническая (программы системного и прикладного характера, обеспечивающие функционирование системы), командная (управляющая) и измерительная информация (показания приборов). Это резко отличается от «офисных» информационных систем, где объектом защиты являются файлы и базы данных.

Во взаимодействие включены разнородные, территориально и пространственно распределенные элементы, в которых реализуются разнообразные информационные технологии, это взаимодействие предельно далеко от документооборота на офисных ПК.

Кроме того, в АСУТП предъявляются жесткие требования к времени и порядку выполнения автоматизированных функций. Эти параметры важны всегда, однако, намного более критичны для атомной электростанции, чем для МФУ, предположим.

Тем более крайне нежелательны отключения систем для проведения мероприятий по обеспечению безопасности информации.

Также крайне опасны последствия вывода из строя и (или) нарушения функционирования системы (и здесь уже речь идет об опасности для жизни и здоровья, а не просто ущерб каким-либо интересам пусть даже большого числа граждан).

Большая часть этих особенностей определяет, по существу, лишь одно требование общего характера к используемым СЗИ – они должны создаваться с повышенным вниманием к качеству на всех этапах – от проектирования для производства. Как правило, гарантия особенно высокого качества связана с более высокой ценой продукта, а значит, данный сегмент должен быть крайне привлекательным для производителя, что, в свою очередь, обеспечит конкуренцию, та повысит общий уровень качества и т. д.

Однако, иметь в своей продуктовой линейке варианты исполнения СЗИ с огромным разнообразием интерфейсов, в том числе довольно

экзотических, производителю сложно и не выгодно, ведь многотысячные продажи делают стандартные интерфейсы, свойственные офисным компьютерам. Аналогично обстоит дело с форматами данных, с файловыми системами, с поддержкой подключаемого оборудования. Поэтому эксплуатирующая или подрядная организация при создании проекта подсистемы защиты информации вынуждена использовать то, что есть, и за ту цену, которую назначит подчас единственных поставщик, а не то, что соответствует высоким требованиям к качеству, надежности и живучести.

Однако и это еще не все. Особенность многих производств сегодня состоит еще в одном очень существенном обстоятельстве: их управляющие инфраструктурные элементы находятся за рубежом. А это означает, что при неблагоприятных внешнеполитических обстоятельствах эти элементы могут стать рычагами управления не только производственными процессами. Система безопасности таких объектов должна строится в предположении, что центр управления может перестать быть доверенным источником, и его команды должны интеллектуально обрабатываться, а не просто без искажений передаваться на исполнение.

На платформе специализированного компьютера с аппаратной защитой данных m-TrusT можно построить такую систему.

4.2.5.6. Умный учет

Приборы учета всегда представляли собой цель для «улучшений» как со стороны недобросовестных пользователей учитываемых ресурсов, так и со стороны недобросовестных взимателей платы за эти ресурсы. Самого разного рода «скручивания» и «накручивания» самого разного рода счетчиков возникло, вероятно, одновременно с самими счетчиками. Каждый, кто брал в аренду автомобиль, который надо вернуть «с тем же количеством топлива», наверняка замечал, что датчик топлива ведет себя удивительно, ну а то, что Интернет полнится

советами по обходу любых счетчиков – от воды до трафика – и вовсе не секрет.

«Умные» приборы учета имеют два существенных отличия:

1) ими можно управлять удаленно, без непосредственного «личного» контакта с каждым, и

2) они несут в себе функциональность не только непосредственно учета, но и управления.

Это совершенно логично – закончился лимит, превышена просрочка по оплате, или наступило еще какое-то заранее назначенное граничным событие – и в установленном порядке отключается подача того, использование чего считает «умный» счетчик. Никакого произвола или человеческого фактора.

За исключением того, что подать эту команду может хакер. А учитывая природу учитываемых ресурсов, трудно преувеличить общественную значимость ситуации, которую сможет создать злоумышленник, буде в его планах резкое повышение уровня социальной напряженности.

Сделать «умный» учет безопасным можно за счет использования решений на платформе m-TrusT. Это та же, уже многократно упомянутая, задача аутентификации управляющих сигналов.

4.3. Функции защиты, связанные с перемещениями в пространстве

Как правило, процессы, протекающие в информационных системах (в цифровой среде) с пространством связаны крайне мало. Потому и возможны ноутбуки, планшеты, удаленка, дистанционное банковское обслуживание и т. п. В общем случае компьютер работает одинаково в любой точке пространства (с поправкой на то, что это не под водой и не в жерле вулкана, хотя бывают и те, что предназначены для таких условий). В рамках диапазона приемлемых для него условий компьютер работает одинаково в любом месте.

Но ведь, строго говоря, это не всегда так уж хорошо. Потому что на самом деле – для людей, а не для компьютеров – «места» различаются. Поэтому мы понижаем голос, разговаривая по телефону там, где нас слышат посторонние, можем оставить записку приклеенной к холодильнику дома, но складываем записку, которую оставляем адресату в общей комнате, и так далее.

С компьютерами все принципиально так же, даже очевиднее. Можно обсуждать, насколько защищенно работают сервисы ДБО, когда компьютер, реализующий функциональность банкомата, заперт в железном сейфе, но все явно становится совсем плохо, если его из этого сейфа кто-то вынул. Многие требования защиты информации, выполняющиеся с помощью организационных мер, перестают выполняться, когда компьютер (сервер, терминал, контроллер) перемещается (выносится из серверной или из контролируемой зоны, или вынимается из корпуса).

Для того чтобы научить компьютер ориентироваться в пространстве, обычно используются датчики. Для получения общего представления об этом можно прочитать, например, обзорную статью [20], написанную на основе реферата на кафедре.

Основная идея статьи в том, что, хотя для обнаружения различных видов инвазивных[37] атак используется множество видов датчиков[38], в большинстве случаев есть выбор, какой применить в каждом конкретном случае, поэтому набор необходимых датчиков при проектировании устройства можно минимизировать. Так, «использование фотодатчиков вместе с датчиком Холла и датчиком температуры способны обнаружить большинство инвазивных атак» [Там же. С. 369].

Надо заметить, что датчики принято считать инструментарием построения защиты именно от инвазивных атак, что отражено и в названии указанной статьи. Описанное же выше – перемещение из серверной или из здания, вынимание из сейфа – казалось бы, прямо с ними не связано, ведь инвазивная атака – атака с физическим проникновением в устройство, а «унесли» – это еще не «влезли внутрь». Однако при ближайшем рассмотрении легко обнаружить прямую связь, ведь «уносить» (а также, например, наклонять, снимать со стены, вынимать из шкафа) имеет смысл именно тогда, когда необходимо осуществить физическое воздействие на устройство – именно его невозможно осуществить в контролируемой зоне под видеокамерой, внутри стального сейфа или под крышкой стола. Если уносят – значит,

---

[37] Инвазивные – это такие, которые требуют физического проникновения внутрь атакуемого объекта. Это может быть проникновение внутрь корпуса железного шкафа при атаке на банкомат, или внутрь корпуса микросхемы памяти при атаке на блок хранения ключа.

[38] В статье перечислены и контурно рассмотрены

- группа датчиков перемещения и усилий (обнаруживают вскрытие корпуса устройства);
- датчики температуры (отслеживают инвазивные атаки с помощью экстремальных температур);
- датчики Холла и Виганда (отслеживают атаки по ошибкам вычислений с помощью переменного магнитного поля);
- Тамперы (определяют перемещение устройства с места фиксации);
- Аналого-цифровые преобразователи (фиксируют атаки по цепям питания);
- CSS (используется для обнаружения атак на тактовую частоту).

почти наверняка, будет не программное, а физическое воздействие. Исключением являются случаи, когда злоумышленнику требуется провести какие-то исследования, для которых необходим длительный доступ к устройству без помех и риска быть обнаруженным. Однако, строго говоря, этот сценарий весьма несущественно отличается от инвазивной атаки.

Так или иначе, датчики сами по себе не защищают ни от перемещения, ни от инвазивных атак, они могут дать возможность обнаружить обстоятельства, в которых должны включиться какие-то защитные механизмы.

Или не включиться, а отключиться – если защитить надо данные не *в устройстве*, а *от устройства*.

Сценарии, в которых человеку может быть желательно, чтобы его планшет или телефон работал по-разному в разных местах (например, отключал микрофон и камеру сам, без специальных действий со стороны пользователя), каждый может вспомнить много. Обрисуем те, что касаются не личных желаний или неловкостей, а регламентированного порядка работы. Речь о выделенных помещениях (ВП) и защищаемых помещениях (ЗП). Как и в отношении других понятий, введенных и описанных в грифованных документах[39], в отношении ВП и ЗП на профессиональных форумах в Интернете, в статьях и различных других материалах встречаются определения этих понятий, иногда почти прямо противоположные. Однако в данном случае это не важно – когда у вас возникнет необходимость, вы сможете, будучи специалистами, получить легальную возможность увидеть определения и требования в первоисточнике[40], а сейчас достаточно

---

[39] Так называют документы с грифами – например, ДСП (для служебного пользования), конфиденциально, секретно и так далее. Если вы слышите какие-то непонятные выражения типа «с собакой» или «две серьги» – то почти наверняка речь о грифе.

[40] Требования к ЗП определяет документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».

понимания, что в некоторых помещениях, предназначенных для разговоров, содержание которых должно остаться между собеседниками, смартфоны и планшеты могут представлять собой проблему, поэтому их при посещении таких мест, как правило, сдают в специальное хранилище.

Естественно, это вариант со всех точек зрения неудобный, поэтому предпринимаются различные попытки принять какие-то технические меры и сделать так, чтобы устройства проносить в такие помещения все же было можно, а если повезет – то и использовать их безопасным образом, а не просто проносить.

Этому посвящена дипломная работа одного из наших выпускников [21], где он предложил способ модификации мобильных устройств для возможности их применения в защищаемых помещениях без снижения защищенности этих помещений.

Помимо самого предложенного способа, в работе представлена интересная и полезная история вопроса, которая в числе прочего, обнаруживает любопытное обстоятельство, касающееся потенциальных каналов утечки, которые есть в мобильных устройствах (смартфонах, планшетах), и блокирование которых, собственно, является целевой установкой работы.

В качестве потенциальной основы построения каналов утечки автор рассматривает все модули ввода данных или модули, которые могут использоваться для ввода данных, что логично. Канал утечки, разумеется, не состоит только из модуля ввода, но так или иначе, данные, которые планируется украсть, сначала должны в смартфон попасть, а значит такие модули будут являться обязательной его частью. При этом оказывается, что канал утечки нельзя построить на очень небольшом числе модулей ввода: на сенсорном экране или сенсорной панели, клавиатуре и кнопках. И то в том случае, если мы рассматриваем сценарий, при котором пользователь не является злоумышленником –

Требования к ВП определяет документ «Требования по технической защите информации, содержащей сведения, составляющие государственную тайну».

потому что без ведома пользователя осуществить ввод с клавиатуры или через сенсорный экран представляется невозможным.

Все остальные же устройства ввода, имеющиеся во всех (или большинстве) мобильных устройств могут лечь в основу построения канала утечки: камера, микрофон и динамики, акселерометр и гироскоп, устройства беспроводной связи: WiFi, Bluetooth, GSM, 3G/4G, GPS и Глонасс модули.

Конечно, сразу обращает на себя внимание, что в этом списке есть датчики, которые, как упоминалось выше, являются общепризнанным инструментом построения защиты от атак на устройства и данные в них. Представляется весьма целесообразным ознакомиться с этой дипломной работой целиком (и это можно сделать, обратившись к архиву кафедры), однако фрагмент о датчиках имеет смысл привести целиком вместе со ссылками на источники, чтобы не создавать искусственной интриги. Нумерация источников сохранена без изменений, и их список приведен здесь же, в не в списке литературы к главе.

«1.2.3 Акселерометр и гироскоп

Гироскопом и акселерометром оснащены все современные мобильные устройства, смарт-часы и фитнес-трекеры — они используются для определения положения устройства в пространстве и фитнес-трекинга. Политика безопасности современных ОС устроена так, что показания акселерометра и гироскопа не считаются критическими данными [9] и доступ к ним имеет большинство приложений [9].

В работе 2014 года [10] американские и израильские исследователи показали, что гироскоп мобильных устройств достаточно чувствителен, что способен фиксировать и распознавать звук человеческого голоса. Аналогичный результат был получен российскими учеными в работе 2016 года [11].

Согласно другому исследованию [12], акселерометр совместно с гироскопом на мобильном устройстве, расположенном рядом с клавиатурой (например, в ситуации, когда на одном столе лежат ноутбук

и смартфон) могут анализировать вибрации от нажатия клавиш на клавиатуре и сопоставить вибрации с клавишами клавиатуры, определив вводимый текст. Похожей уязвимостью могут обладать смарт-часы или фитнес-браслет [12].

Показания гироскопа и акселерометра могут быть использованы для вычисления перемещений устройства в пространстве, раскрывая, таким образом, перемещения устройства и его владельца [13].

С одной стороны, ценность вибро-акустической информации в защищаемых помещениях и слабая защищенность показаний акселерометра и гироскопа делает этим модули привлекательной целью для атаки с точки зрения злоумышленника; с другой стороны, анализ полученных данных является сложной задачей сам по себе.

<…>

Список используемой литературы

<…>

9. Официальный сайт поддержки ОС Android source.android.com [Электронный ресурс]. URL: https://source.android.com/security/app-sandbox (дата обращения: 15.12.2019)

10. *Yan Michalevsky, Dan Boneh, Gabi Nakibly,* Gyrophone: Recognizing Speech From Gyroscope Signals // Proceedings of the23rd USENIX Security Symposium, August 20–22, 2014. — 12 p.

11. *Козлов Ю.Е., Евсеев В.Л.* // Экспериментальное определение речевого сигнала в показаниях акселерометра. Журнал “Вопросы кибербезопасности” №5(18) – 2016. — С. 12-16.

12. *Tony Beltramelli*, Deep-Spying: Spying using Smartwatch and Deep Learning. IT University of Copenhagen, Copenhagen, Denmark, 2015. – 13 p.

13. Пестов, Е. А. Распознавание движения мобильного устройства / Е. А. Пестов // International Journal of Open Information Technologies. — 2013. — Т. 1, № 3. — С. 5–10.

<…>».

Конечно, в том, что один и тот же компонент системы может в одном случае быть основой построения защиты, а в другом – канала утечки, нет решительно ничего парадоксального, это только еще один пример того, что не нужно присваивать техническим средствам ярлыков – ни положительных, ни отрицательных, чем шире вы можете на них смотреть, тем лучше вы как разработчик.

Более того, в обширно процитированной дипломной работе не рассматривается вопрос о том, как именно должен быть зафиксирован устройством тот факт, что оно оказалось в защищаемом помещении и должно отключить модули ввода предложенным дипломником способом. Думается, что если реализация будет предполагать автоматическое срабатывание этого механизма, а не произвольное – по осознанному действию пользователя, то без датчиков эта реализация тоже не обойдется.

В определенном смысле все, что описано в этой главе, и даже описанное в разделах 2.6 и 3.2 тоже можно интерпретировать, как связь между пространством и защитными функциями. Однако, думается, что выделенные ключевые акценты (отсутствие границ системы (2.6), доступ из разных вычислительных сред (3.2), расположение отдельных компонентов системы за пределами контролируемой зоны (4.1 и 4.2) и собственно перемещение, движение СВТ в пространстве (4.3)) должны помочь понять *особенности* этих различных с точки зрения технической защиты информации случаев более наглядно, ведь именно понимание тонкостей делает специалиста профессионалом.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования» [электронный ресурс]. URL: https://docs.cntd.ru/document/1200065692 (дата обращения: 23.06.2021).
2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 23.06.2021).
3. ГОСТ Р 56115-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования» [электронный ресурс]. URL: https://docs.cntd.ru/document/1200113336 (дата обращения: 23.06.2021).
4. *Конявский В. А., Конявская С. В.* Доверенные информационные технологии: от архитектуры к системам и средствам. М.: URSS. 2019. – 264 с.
5. Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 23.06.2021).
6. *Грунтович М. М.* О «двуличии» в алгоритмах цифровой подписи // itWeek. (334-335)16-17`2002 [электронный ресурс]. URL: https://www.itweek.ru/infrastructure/article/detail.php?ID=61554 (дата обращения: 23.01.2019).
7. Планшет СКЗИ ready «ПКЗ 2020» // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/accord/planshetSKZIreadyPKZ2020 (дата обращения: 16.04.2021).
8. TrusTPad // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/newharvard/istoriya-nga/trustpad/ (дата обращения: 23.06.2021).
9. СОДС // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/storage/compute/sods/ (дата обращения: 16.04.2021).
10. Aladdin LiveOffice // Официальный сайт Аладдин [электронный ресурс]. URL: https://www.aladdin-rd.ru/catalog/liveoffice (дата обращения: 16.04.2021).
11. С-Терра Пост 4.2 // Официальный сайт S-Terra [электронный ресурс]. URL: https://www.s-terra.ru/products/catalog/s-terra-post-4-2/ (дата обращения: 16.04.2021).

12. M-TrusT // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/newharvard/m-trust/ (дата обращения: 23.06.2021).

13. Федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 23.06.2021).

14. Приказ ФСТЭК России от 11 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236 (дата обращения: 23.06.2021).

15. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60) [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 23.06.2021).

16. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1702-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 23.06.2021).

17. Положение Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» [электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/72146408/ (дата обращения: 23.06.2021).

18. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [электронный ресурс]. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 23.06.2021).

19. *Чехов А. П.* Злоумышленник // Полное собрание сочинений и писем в 30-ти томах. Сочинения. Том 4. М., «Наука», 1984.

20. *Маркин И. М.* Обзор датчиков для обнаружения инвазивных атак // Комплексная защита информации. Материалы XXVII международной научно-практической конференции (Минск, 25–27 мая 2021 г.). Минск, 2021. С. 365–369.

21. *Шагапов А. И.* Разработка способа реализации защищенного мобильного устройства для использования в защищаемых помещениях. Дипломная работа (на правах рукописи). Кафедра защиты информации ФРКТ МФТИ. М., 2020.

ГЛАВА 5. СОБЫТИЯ БЕЗОПАСНОСТИ

Наличие подсистемы регистрации событий – это естественное и закрепленное в нормативных документах требование к любому относительно самостоятельному компоненту информационной системы и к информационной системе в целом. Меры, связанные с регистрацией событий безопасности указаны в приложениях «Меры…» к Приказам ФСТЭК России [1–3], методических документах «Профиль защиты…» для всех типов средств защиты (как тех, что выпускает ФСТЭК России[41], так и отраслевых или корпоративных[42]).

Реализация этой подсистемы может представлять некоторые сложности, но как правило, они исчерпываются техническими задачами.

Два аспекта, которые целесообразно здесь рассмотреть – это централизованный сбор данных и мониторинг, с одной стороны, а с другой – хранение и архивирование журналов. Первый аспект касается выстраивания системы оперативного и адекватного реагирования, полноты представлений управляющего персонала о состоянии системы, а второй – напротив, создания условия для того, чтобы вернуться к событиям прошлого можно было через продолжительное время.

---

[41] С теми из них, что являются общедоступными, можно ознакомиться, например, в [4].

[42] В соответствии с п. 6.3.2.3 ГОСТ Р 57628-2017 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» [5] профили защиты (ПЗ) могут разрабатываться уполномоченным федеральным органом исполнительной власти (ФСТЭК России), крупными организациями, группами организаций, ведомствами и т.д. На практике, как правило, все используют ПЗ, разработанные и утвержденные ФСТЭК России, ничего в них не добавляя, но, в принципе, такая возможность предусмотрена, требования ФСТЭК России могут быть расширены требованиями, специфичными для отрасли или организации. Предусмотрен даже порядок создания иерархии связанных ПЗ. Подробнее про это будут рассказывать в других курсах.

Вообще говоря, между этими задачами нет какой бы то ни было противопоставленности, они могут быть одинаково актуальны в какой-то системе, могут иметь различную актуальность, но главное – они разные и решаются разными средствами, которые не могут рассматриваться как взаимозаменяемые.

5.1. Системы удаленного централизованного мониторинга событий безопасности

В первую очередь, необходимо провести границы того явления, которое мы будем рассматривать, как сейчас принято говорить, «отстроиться» от смежных явлений. И первое, на что нужно обратить внимание, это то, что класс решений носит обобщенное название «Системы мониторинга и управления информационной безопасностью». Нет как-то особенных причин для того, чтобы систему централизованного мониторинга событий нельзя (или неверно) было бы реализовать и без компонентов управления, однако практика такова, что заказывается (то есть востребована) эта функциональность именно в комплексе. В значительной мере это связано с тем, что оперативный контроль, анализ событий и обеспечение механизмов реагирования позволяют не только выявить факт атаки или нарушения работоспособности, но и подготовить комплекс превентивных мер и мероприятий по устранению последствий нарушения безопасности. Смежные же действия удобно выполнять с помощью единого инструмента, без промежуточных этапов, поэтому их и реализуют в одной подсистеме.

Так и будем рассматривать, опираясь в этом разделе, преимущественно, на [1].

5.1.1. Общая характеристика систем мониторинга и управления информационной безопасностью

Мониторингом и управлением ИБ называют подсистемы, контролирующие общее функционирование ИС, системы передачи данных, средства и механизмы защиты. Требования к этим подсистемам определены в документах, устанавливающих общие требования к соответствующим системам в целом, и не имеют особенно радикальных

различий. Особенности реализации этих требований стандартизированы, и дальше будет очевидно, почему это важно.

Предпосылки к созданию систем *удаленного* мониторинга и управления информационной безопасностью появились в тот момент, когда возникла необходимость отслеживать состояние компьютерной системы, локальный доступ к которой отсутствует или затруднен [2].

Вообще говоря, представить себе систему, которой было бы по-настоящему удобно управлять локально – довольно сложно. Попробуем.

В процессе функционирования система мониторинга и управления (как локальная, так и удаленная) осуществляет сбор первичных данных мониторинга информационной безопасности с наблюдаемых подконтрольных объектов (ПКО) и их анализ. Для этого разрабатываются специальные приложения – компоненты системы мониторинга и управления, выполняющие удаленный сбор журналов аудита с подконтрольных объектов: рабочих станций (РС) сотрудников и серверов контролируемой информационной системы.

Подобно другим многокомпонентным распределенным системам, эта система нуждается в управлении и конфигурировании со стороны администратора системы.

Конфигурирование заключается в задании параметров, в соответствии с которыми система должна выполнять свои функции. В случае выходов значений параметров за пределы, определенные как «нормальные», администратор предпринимает шаги для устранения этой ситуации и нормализации параметров. Например, администратор может ограничить доступ пользователя к ресурсам подконтрольного объекта теми или иными способами, например, с помощью систем контроля поведения (в частности, приостановить или частично заблокировать работу процесса) [3]. На это и направлены основные типы функций управления:

- определение текущего состояния компонентов,
- формирование управляющего воздействия (команда управления),

• предоставление администратору системы результатов обработки управляющего воздействия, переданных со стороны компонента.

То есть получаются данные для оценки их «нормальности», при необходимости, формируется команда на корректировку, затем получаются данные о том, произведена ли корректировка. То, каким именно образом будет произведена корректировка ситуации, зависит от того, чем именно – какими средствами – управляет система. Как уже не раз было показано, одни и те же задачи могут решаться совершенно разными инструментами, и, если система управления и мониторинга предоставляет возможность решить задачу разными способами, выбор, так или иначе, за администратором. Либо он определяет правила автоматического выбора инструмента в зависимости от совокупности условий, либо этот выбор осуществляется вручную по факту.

Теперь представим себе, что все это осуществляется локально. Как минимум, это точно не персональный компьютер – потому что представить себе, что за компьютером сидят рядом пользователь и администратор, управляющий ИБ, можно было, наверное, только в антиутопии в 80-х годах прошлого века. С другой стороны, если функции управления не должны непременно осуществляться прямо в сеансе работы пользователя, а могут осуществляться отдельно, в другом сеансе, ситуация выглядит менее абсурдно. Еще менее абсурдно выглядит локальное управление сервером.

И тут мы приходим к точке, где нужно очень точно развести понятия – о чем мы говорим, используя слово «локальный»? Локальный доступ управляющего персонала и локальная система – это совершенно разные вещи. Локальная система управления – это когда управляющее ПО находится прямо на ПКО, а не на другой, отдельной машине. Как при этом получает к нему доступ администратор – совершенно не имеет значения.

То есть при затрудненности доступа к ПКО требуется не удаленная система управления, а удаленный доступ к управлению. А удаленная

система управления требуется тогда, когда возникает потребность в *централизации*.

Одной из основных целей создания *централизованной* системы мониторинга и управления информационной безопасностью является повышение эффективности соответствующих процессов. Рассмотрим, что это означает на практике.

Зачастую в рекламных описаниях пишут о том, что централизованный мониторинг и управление позволяют администраторам работать на одном рабочем месте, а не «бегать по этажам». Вспомним, что не бегать по этажам можно и при удаленном доступе к локальным подсистемам. В этом случае процесс будет выглядеть так: администраторы (системный и безопасности информации) каждый со своего рабочего места будут подключаться к соответствующим подсистемам на ПКО и производить необходимые действия. При этом на разные мониторы или на разные окна на одном экране могут параллельно выводиться и оперативные журналы с разных ПКО – дальше вопрос только в том, хватит ли внимания администратора – во всяком случае, он точно не бегает по этажам.

Однако при этом у управляющего персонала остается необходимость производить большое количество однотипных (а как правило и просто одинаковых) настроек, вручную следить за тем, как соотнесены сотрудники с пользователями различных ПКО (один и тот же человек может иметь разные права на разных компьютерах, и при этом его учетные записи могут выглядеть совершенно по-разному, хотя справедливости ради нужно заметить, что обычно организационными мерами обеспечивается «узнаваемость» сотрудника по учетной записи (она называется его фамилией и инициалами, например), но в то же время исключать, что user1 с ПКО_N и user3 с ПКО_K – это один и тот же человек – нельзя). Казалось бы, ну и что, ведь правила заданы для пользователей, по заранее продуманной политике, и так далее. Так-то оно так, однако при живом функционировании системы изменения,

вносимые «на живую нитку», могут увести фактически реализованную политику довольно далеко от изначально описанной и утвержденной.

Получается, что конфигурация подсистемы защиты информации развивается спонтанно, а в ИС большого объема, где управляющего персонала много, может вообще не быть никого, кто представлял бы себе общее состояние подсистемы в целом.

Владение частью информации, невозможность сопоставить данные разных участков системы (или возможность их сопоставить только вручную), не дает системе мониторинга и управления стать по-настоящему эффективной.

5.1.2. Система централизованного управления и мониторинга средствами защиты информации от несанкционированного доступа

Система управления и мониторинга средствами защиты информации от несанкционированного доступа (СЗИ от НСД) предоставляет возможность централизованного управления и конфигурирования СЗИ от НСД, функционирующих на подконтрольных объектах системы.

В качестве примера будем рассматривать ту же систему СУЦУ, управляющую ПАК СЗИ от НСД «Аккорд-Win64», о которой уже шла речь в 3 главе. Там же уже говорилось о том, что СЗИ от НСД «Аккорд» осуществляет контроль целостности своего программного обеспечения (ПО) и настроек, а также программного обеспечения, указанного как «объекты контроля» системы, системных областей диска, файлов ОС, а также прикладного ПО объектов защиты, имеет собственную систему разграничения доступа. В комплексе реализована подсистема регистрации и учета, предназначенная для регистрации в системном журнале СЗИ от НСД событий информационной безопасности.

Журнал событий СЗИ содержит информацию о дате и точном времени регистрации события, детальности журнала, установленной на момент регистрации события, имени рабочей станции, типе операции, наименовании объекта доступа (файла, каталога, диска, устройства), имени процесса и результате события. При положительном завершении события в журнал записывается результат «ОК», а при отрицательном – регистрируется несанкционированный доступ (НСД) или ошибка доступа (в случае нарушения целостности сообщается об изменении контролируемых параметров).

Для просмотра журнала событий СЗИ существует специальная программа, входящая в состав ПАК СЗИ НСД «Аккорд», которая позволяет осуществить не только просмотр журнала, но и его вывод на печать и архивацию. Журнал отображается в виде таблицы, каждая строка которой соответствует одному событию, зарегистрированному в журнале.

Для управления правами пользователей в состав ПАК входит другая программа. И так на каждом защищенном компьютере.

Необходимость централизации функций управления и мониторинга становится очевидной даже в системе из нескольких сотен компьютеров, если их администрирование производится постоянно и интенсивно. Такие случаи встречаются на практике довольно часто и могут быть связаны как с недостаточной продуманностью администрирования и желанием подразделения информационной безопасности показать свою необходимость, так и с какой-нибудь объективной целесообразностью.

Структурно система удаленного централизованного управления и мониторинга СЗИ от НСД состоит из:

- сервера управления (сервер реализован в виде терминального сервера и АРМ управляющего персонала, которые подключаются к серверу по протоколу терминального доступа, однако, в принципе, можно управлять и с консоли, если это для чего-то нужно);

- подконтрольных объектов (АРМ и серверов, на которых установлены и функционируют СЗИ от НСД).

Функционально данная система включает:

- средства централизованного управления учетными записями пользователей и СЗИ от НСД (включая доступ к коммуникационным портам и съемным носителям) на объектах защиты;
- средства централизованного сбора журналов событий ИБ с подконтрольных АРМ и серверов;
- средства оперативного оповещения о событиях ИБ.

Программное обеспечение, входящее в состав данной системы, включает в себя серверную и клиентскую часть, устанавливаемые соответственно на сервер управления и подконтрольные объекты.

В системе управления и мониторинга СЗИ от НСД реализована собственная подсистема управления доступом персонала этой системы к функциям мониторинга и управления. Управление правами доступа персонала заключается в выделении ролей, уровней их иерархии и объектов доступа [4]. Персонал системы имеет доступ к той и только к той части информации, которая ему необходима и достаточна для выполнения своих обязанностей, этому был посвящен раздел «Победить супербезопасника» в 3 главе.

В результате при внимательном и профессиональном подходе подразделения информационной безопасности к формированию политик безопасности и распределению задач между управляющим персоналом на базе описанного средства можно создать эффективную систему контроля, позволяющую собирать исчерпывающий материал для последующего анализа.

Однако средства анализа как таковые в эту подсистему не входят, так как анализ не является ее функцией. Но, как правило, события СЗИ НСД вполне поддаются анализу «вручную», и зачастую специальные средства только для этого на предприятиях не применяются.

Наряду с этим нужно иметь в виду и тот факт, что при комплексном подходе к управлению системой, скорее всего, предприятие внедряет не только систему мониторинга и управления СЗИ НСД, но и аналогичные средства для мониторинга и управления другими важными подсистемами (ОС, антивирусы, ЛВС и прочие). В силу своей специфики, эти средства часто разрабатываются разными компаниями, агрегируют данные в разных форматах.

То есть ситуация с децентрализованным управлением, описанным выше, переходит на новый виток спирали. Теперь у предприятия есть разрозненные данные, собранные разными системами в разных форматах, анализируемые сотрудниками разных отделов.

Очевидно, что следующий шаг централизации управления системой – корреляция, для которой требуется управляющая система над всеми системами мониторинга и управления. Такие системы относятся к классам SIEM или BI. SIEM – это Security Information and Event Management, а BI – это Business Intelligence. BI – это более масштабная система, обрабатывающая, коррелирующая и визуализирующая не только данные, связанные с безопасностью, а самые разнообразные данные о состоянии системы. SIEM обычно входит в состав BI (но используется и отдельно, если BI избыточна).

В свою очередь SIEM – это SIM и SEM – Security Information Management и Security Event Management. SIM автоматизирует сбор данных журнала событий с различных СЗИ (межсетевые экраны, прокси-серверы, системы обнаружения вторжений и антивирусное программное обеспечение) и приведение этих данных в коррелированные и нормализованные форматы, а затем отображает отчеты, диаграммы и графики с этими данными.

SEM также собирает события, но кроме этого их анализирует и позволяет выделять данные о событиях определенных типов. Зачастую SEM также включают в себя функции «обратной связи» – управления настройками СЗИ.

Очевидно, что эти два типа систем настолько близки, что не могли не соединиться в один новый (некогда новый, сейчас уже нет) тип – SIEM.

Для примера можно рассмотреть BI от IBM – «IBM Tivoli», она включает в себя SIEM – TSIEM. Кроме этого в Tivoli входит система сбора и анализа оперативных журналов TSOM, и другие модули, позволяющие выполнять операции с информационными ресурсами в области управления доступом, управления техническими средствами и пр.

При совместном применении Tivoli и системы централизованного управления и мониторинга СЗИ от НСД последняя используется в качестве единого консолидированного источника данных о событиях ИБ, зафиксированных СЗИ от НСД на подконтрольных объектах, и выступает в качестве объекта управления со стороны соответствующих компонентов Tivoli. То есть Tivoli (или другая BI система) получает от СУЦУ данные для корреляции и анализа, а СУЦУ получает от Tivoli управляющие воздействия, сформированные на основе анализа или на основе решений управляющего персонала вручную.

В связи с этим необходимо отдавать себе отчет в одном существенном обстоятельстве (впрочем, тот факт, что в нем отдает себе отчет разработчик, не очень помогает эксплуатирующим организациям, однако наш долг хотя бы постараться им объяснить). В реальных системах журналы событий – как СЗИ, так и любой другой программы, полученные в результате работы пользователя, состоят из огромного количества строк, описывающих возникшие события. Для того чтобы сделать психологически более приемлемой задачу сбора статистики или иные задачи, связанные с обработкой данных журналов, администраторы используют возможность снижения их детальности. Уровень детальности журнала настраивается практически во всех продуктах, имеющих подсистему регистрации событий (то есть, иными словами, практически по всех программных продуктах). Самый высокий

уровень детальности – записываются все события, самый низкий – записываются только события НСД (в случае с журналом СЗИ).

Желание минимизировать объем данных для анализа, ограничившись «только действительно важными» – хорошо понятно. Однако, эти действия уместны только в том случае, если анализируются события вручную, а данные разных подсистем не агрегируются в целях корреляций, поскольку в общем случае невозможно предположить, какие данные точно не окажутся значимыми для воссоздания некоторой картины инструментами класса BI.

Эти инструменты, получив данные от подконтрольных систем, структурируют их определенным образом, анализируют их согласно заданным правилам, формируют на основе этого анализа описание процессов, протекающих в системе (в том числе визуализацию этих процессов), и предоставляют пользователям (руководителям, аналитикам, администраторам) доступ к данным того виды, который интересует пользователя – как просто к агрегированным и структурированным, так и к результатам анализа, визуализациям и так далее.

Например, в состав Contour BI [5] входит программа, предназначенная для быстрого создания интерактивных отчетов. Эти отчеты уже анализируются пользователями этой системы. Входными данными для программы, как правило, являются суммированные в один большой журнал несколько сотен или даже тысяч журналов событий от различных подразделений организации, выходными же данными являются графики и диаграммы, на основании которых можно отфильтровать нужные данные или выполнить сортировку по выбранному событию, выделить N лучших или худших событий. Это пример агрегации.

Корреляция же в данном случае – это наложение данных о событиях разных подсистем и анализ этого наложения. Такими подсистемами, могут быть, например, подсистемы, регистрации доступа пользователей

в помещение (возможный эффект от сквозного анализа событий СЗИ и СКУД уже упоминался в 3 главе, вернитесь к разделу 3.1.2.4, чтобы вспомнить), антивирусной защиты, подсистема обновления операционной системы или какого-либо прикладного программного обеспечения. Рассмотрим на простом примере, как, используя BI и журналы событий различных подсистем, можно провести более глубокий анализ происходящего в системе. Например, в одном из подразделений организации, судя по журналам событий СЗИ, каждую неделю в определенный день и время происходят попытки НСД, связанные с попыткой доступа к какому-либо ресурсу. Проанализировав журнал антивирусной защиты можно понять, что как раз в этот день и время происходит обновление антивирусных баз. И уже на основании полученной из обоих журналов информации можно сделать вывод о том, легальное ли это обновление и имеет место ошибка настройки СЗИ, или СЗИ настроено правильно, а антивирус обновляется нештатно (такое может быть по разным причинам). Ручной анализ таких событий сложно выполнить быстро и качественно, а BI позволяет это сделать без особых временных затрат, используя фильтры и диаграммы событий.

В примере рассмотрена корреляция всего двух очень простых событий, а если события более сложные и их не два, а гораздо больше, к тому же все они между собой переплетены, то при выполнении их анализа без BI не обойтись. И тут становится хорошо понятно, что, если использовать журналы не самой высокой детальности, информативность корреляционного анализа существенно снизится, множество «совпадений», которые могли бы выстроиться в понятную картину происходящего, не будет выявлено из-за того, что для одной из подсистем событие будет отфильтровано как неважное. Этот факт нужно хорошо понимать и как можно тщательнее объяснять эксплуатирующей или внедряющей организации, если им он не очевиден.

Более подробное описание работы Contour BI можно прочитать в [6].

5.2. Хранение и архивирование журналов событий

В начале главы уже упоминалось, что требования к журналам событий вполне понятны и достаточно просто реализуемы, поэтому мы в ОКБ САПР, возможно, никогда не задумались бы о том, чтобы создать какое-то отдельное решение для работы с журналами, ограничиваясь стандартным выполнением требований к регистрации событий в своих продуктах. Однако решение пришло в ходе обсуждения с администраторами безопасности информации наших защищенных флешек «Секрет». В результате этого разговора возник замысел, а затем и само решение ПАЖ, которое уже упоминалось в 3 главе в связи с его ролевой структурой.

Оказывается, флешка с управляемым доступом, различающая не только людей, но и компьютеры — это как раз то, что нужно, чтобы упростить жизнь в части организационных мер по работе с журналами и в то же время не снизить, а наоборот повысить их защищенность, а значит, и доказательность.

Журналы нужны для того, чтобы «если что» восстановить, как было дело. Это довольно очевидно.

Для того чтобы это предназначение реализовывалось без оговорок, журнал должен:

1. Быть доступным для изучения в случае необходимости,
2. Быть недоступным для изменения для кого-угодно с какими-угодно целями.

Что может быть не так, за счет чего журналы могут оказаться недоступными для изучения или измененными?

• Журналов много, и это файлы. Большого объема, в большом количестве. Они занимают очень много места, и память, отведенную под журналы — будь то память СВТ или память СЗИ — время от времени освобождают. Все без исключения. При этом их обычно архивируют, записывают на какой-то носитель и куда-то убирают. В

какой-то шкаф. И там они, конечно, штабилируются. Это первая причина, по которой журнал может оказаться не доступен в нужный момент.

- Вторая причина — это повреждение файла журнала. С этим сталкивались большинство администраторов систем и большинство служб технической поддержки. Конечно, файл журнала может быть поврежден и из-за ошибок того устройства или приложения, которое регистрирует событие. Но чаще, объективно, случается так, что он повредился при хранении. Эта причина затруднений смежна с проблемой изменения журнала.
- Журнал может стать недоступным из-за того, что кто-то его специально повредил. А может оставаться доступным, но «улучшенным». И необязательно действовал злоумышленник. Возможно, администратор просто «убрал лишнее», чтобы не засоряло. Ну или, конечно, чтобы что-то скрыть. Так или иначе, если нет возможности доказать, что журнал не изменен, то использовать его при «разборе полетов», конечно, можно, но.

И чтобы не было «но», нужно каким-то способом обеспечить доказанную целостность информации.

Однако, согласитесь, что подписание журналов ЭП (или защита с помощью кодов аутентификации (КА)) — решение не то что бы нереализуемое, но немного странное.

Тем более, оно никак не предотвратит порчу журнала, а еще в меньшей степени поможет его просмотреть в случае необходимости.

Не будем забывать, что все журналы — это не просто файлы, это еще и *разные* файлы, и выработать надо механизм для работы сразу со всеми.

Значит, логично перенести фокус с защиты файла на защиту его носителя.

Итак, нам потребуется носитель:

- удобный в хранении,
- совместимый со всеми или с большинством СВТ
- не требующий от пользователя специальных навыков
- способный обеспечить неизменность своего содержимого после того, как оно на него попало.

Получается неперезаписываемый (add only) USB-накопитель, чтобы данные нельзя было ни удалить, ни модифицировать умышленно или по ошибке.

При этом жизнь подсказывает еще ряд функциональных требований, например:

- различение СВТ — чтобы журналы не путались, иначе неудобно;
- различение пользователей, например, чтобы читать журналы мог только специальный аудитор, а тот, кто настраивает носитель (администратор) и тот, кто записывает на него журналы (пользователь) — не могли.

Все эти выкладки мы и положили в основу «Программно-аппаратного журнала» — неперезаписываемого хранилища на базе служебных носителей семейства «Секрет».

Теперь посмотрим, что привносят в этот контурный замысел требования документов.

Требования к хранению журналов и к работе с ними фигурируют во множестве нормативных и методических документов разных типов – от приказов ФСТЭК России до отраслевых стандартов. Рассмотрим для примера следующие:

- ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [7];
- положение Банка России № 316-П «Об обеспечении информационной безопасности автоматизированных систем Банка

России, предназначенных для обработки, хранения и (или) передачи информации ограниченного доступа» [8];

- методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» [9].

В стандарте [7] предъявляются следующие требования к хранению журналов:

- информация, содержащаяся в журналах аудита, должна быть защищена от несанкционированного доступа и несанкционированного изменения;
- необходимо применять меры по обеспечению конфиденциальности данных, хранящихся в журнале.

Положение Банка России [8] требует архивировать содержащуюся в журналах информацию перед их очисткой. При этом архивы журналов могут уничтожаться только администратором информационной безопасности и не ранее чем через три года с момента появления последней записи в данной архивной копии.

Методический документ ФСТЭК России [9] задаёт срок хранения информации о зарегистрированных событиях безопасности (не менее трех месяцев). При этом объём памяти для хранения информации о событиях безопасности определяется с учетом:

- типов событий безопасности, подлежащих регистрации;
- составом и содержанием информации о событиях безопасности, подлежащих регистрации;
- прогнозируемой частоты возникновения подлежащих регистрации событий безопасности;
- срока хранения информации о зарегистрированных событиях безопасности.

Для повышения уровня безопасности в информационной системе документ [8] требует хранить журналы в изолированном хранилище,

физически отделенном от технических средств, входящих в состав информационной системы.

На основе этих выкладок можно сформулировать следующие требования к средству архивации журналов СЗИ:

- возможность дописывания событий в существующие архивы журналов;
- невозможность удалить содержимое архивной копии журнала до истечения срока хранения;
- доступность архивных копий журнала для просмотра только уполномоченными субъектами;
- большой размер дискового пространства, достаточный для хранения архивных копий журналов;
- изолированность хранилища от технических средств, входящих в состав информационной системы;
- контроль целостности содержимого архива;
- простая интеграция с системами защиты информации;
- возможность использования хранилища только на компонентах контролируемой информационной системы.

Таким и разработан ПАЖ. На высоком уровне абстракции сценарий его работы такой:

- настройка устройства уполномоченным лицом (какие журналы работы СЗИ необходимо архивировать, установка лиц, имеющих прав на просмотр и экспорт журналов, установка сроков хранения журналов);
- сотрудник организации, имеющий право на экспорт журналов, подключает средство архивации к компоненту информационной системы, откуда автоматически выгружаются журналы работы СЗИ. При этом в устройстве сохраняется дата и время последнего зарегистрированного события для каждого СЗИ, вычисляется сумма контроля целостности для каждого журнала работы СЗИ;

- сотрудник организации, имеющий право на просмотр журналов, проверяет работу СЗИ за истекший период;
- по истечении установленного времени хранения журнал работы СЗИ в устройстве автоматически очищается.

Подробнее ролевая структура ПАЖ описана и обоснована в 3 главе.

Внутренняя память устройства разделена на три части [10]:

1. Открытый диск. Он всегда появляется при монтировании устройства на компьютере, доступен только для чтения. На нем находится внешнее ПО ПАЖ, которое записывается туда при изготовлении изделия или его обновлении;
2. Диск архива журналов. На нем сохраняются файлы журналов, доступные для просмотра и экспорта с помощью ПО ПАЖ;
3. Диск внутреннего журнала ПАЖ [11]. На нем сохраняется журнал событий самого устройства (подключение ПАЖ к рабочей станции, успешное или ошибочное выполнение регистрации, авторизации, настройки политик и т. д.).

ПАЖ может использоваться по двум различным сценариям:

- архивирование журналов: в память архива ПАЖ записывается информация из журналов СЗИ. После этого происходит очистка журналов СЗИ на рабочей станции. Копирование журналов в архив ПАЖ осуществляется по расписанию или по достижению журналом СЗИ заданного объёма;
- регистрация событий СЗИ: СЗИ осуществляют регистрацию событий, сразу помещая их в архив ПАЖ [12].

Подробнее в целом о решении, как всегда, можно прочитать на сайте ОКБ САПР.

В заключение этой темы рассмотрим, как может строиться сценарий работы ИС, в которой совмещены так или иначе решения двух

рассмотренных классов, чтобы более наглядно осознать, насколько различны их задачи, и в какой мере они могут быть смежны.

Представим себе, какие возможности по манипуляциям представлениями о состоянии информационной системы у руководителей и аналитиков располагает персонал, обслуживающий BI систему. Корректируя данные, используемые системой для анализа, можно самым разнообразным образом искажать картину. Поэтому такие системы должны очень тщательно защищаться. И, как мы уже знаем, крайне желательно дублировать защиту критичных участков, реализуя ее разными способами и механизмами.

Значит, имеет смысл, например, дополнительно сохранять журналы где-то вне системы BI, с тем чтобы потом, в случае возникновения подозрений сравнить данные с эталонными. Здесь в дело вступает ПАЖ, с помощью которых организуется архивирование и упорядоченное хранение архива. Если BI показывает на архивных данных ту же самую картину, значит, все в порядке.

При этом может быть целесообразно настроить журналирование так, чтобы события вообще не записывались на жесткий диск подконтрольного объекта (иногда это просто невозможно, если речь идет о бездисковых терминалах), а только передавались в систему мониторинга и сохранялись на ПАЖ. В этом случае не придется устанавливать отдельных регламентов по работе с журналами на ПКО – режима доступа к ним, очистки и так далее.

СПИСОК ЛИТЕРАТУРЫ:

1. Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 23.06.2021).
2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 23.06.2021).
3. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1702-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 23.06.2021).
4. Профили защиты // ISO 27000.ru. Искусство управления информационной безопасностью [электронный ресурс]. URL: http://www.iso27000.ru/standarty/iso-15408-obschie-kriterii-ocenki-bezopasnosti-informacionnyh-tehnologii/profili-zaschity (дата обращения: 17.07.2021).
5. ГОСТ Р 57628-2017 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» [электронный ресурс]. URL: https://docs.cntd.ru/document/1200146707 (дата обращения: 17.07.2021).
6. *Сухарева С. В., Лыдин С. С., Макейчик Ю. С.* Особенности системы централизованного управления и мониторинга средствами защиты информации от несанкционированного доступа // Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15–18 мая 2012 года, Суздаль (Россия). М., 2012. С. 226–228.

7. *Сильнов Д. С.* Современные системы удаленного мониторинга вычислительных ресурсов: состояние, проблемы, перспективы // Безопасность информационных технологий. М., 2011. № 3. С. 57–60.

8. *Васильев Н. П., Сильнов Д. С.* Программные средства защиты систем удаленного мониторинга вычислительных ресурсов // Безопасность информационных технологий. М., 2011. № 3. С. 140–142.

9. *Пестунова Т. М., Родионова З. В.* Об одном подходе к управлению правами доступа // Материалы XVIII всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы». М., 2011. С. 119–121.

10. Contour BI // Официальный сайт Contour Components [электронный ресурс]. URL: https://www.contourcomponents.com/ru/contour_bi (дата обращения: 03.07.2021).

11. *Некрасов В. А.* Business Intelligence и информационная безопасность // Национальный банковский журнал. М., 2012. № 3 (март). С. 104–105.

12. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности [электронный ресурс]. URL: http://docs.cntd.ru/document/1200103619 (дата обращения: 03.07.2021).

13. Положение Банка России № 316-П от 11.01.2008. Об обеспечении информационной безопасности автоматизированных систем Банка России, предназначенных для обработки, хранения и (или) передачи информации ограниченного доступа.

14. «Меры защиты информации в государственных информационных системах». Методический документ. Утвержден ФСТЭК России 11 февраля 2014 [электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 24.04.2015).

15. *Конявский В. А., Щербаков А. Ю.* Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. № 15.

16. *Конявский В. А.* Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013, бюл. № 20.

17. *Конявская С. В., Кравец В. В., Батраков А. Ю.* Безопасный Интернет: видимость как необходимое и достаточное // Вопросы защиты информации: Научно-практический журнал. М.: ФГУП «ВИМИ», 2014. Вып. 4

ГЛАВА 6. ВОПЛОЩЕНИЕ РАЗЛИЧНЫХ ИДЕЙ, ПОДСКАЗАННЫХ ЖИЗНЬЮ, ИЛИ ХОД МЫСЛЕЙ РАЗРАБОТЧИКА

Так или иначе по тексту этой книги, а также в лекциях по другим базовым предметам вам много раз встречалась мысль о том, что решения получаются полезными тогда, когда они создаются в результате (или хотя бы с учетом) понимания того, как *на самом деле* (а не в теории) протекает тот или иной процесс в *настоящих* информационных системах. Вообще говоря, едва ли можно сформулировать более очевидную мысль. Идея о том, что делать надо то, что нужно людям, поражала своей новизной только при советской власти. Однако на практике так делается крайне редко, так как удобнее делать то, что умеешь, а не то, что нужно. В этой главе описаны случаи, когда мы (ОКБ САПР) не просто руководствовались здравым смыслом (так мы стараемся поступать всегда), а буквально создавали решения «по просьбам трудящихся» – по мотивам рассказов пользователей о своих задачах и проблемах. Особенность этих решений в том, что они не «заказные», а «инициативные», то есть это не разработка по техническому заданию некоторого решения в интересах некоторого заказчика, а собственная инициатива разработчика, поэтому некоторые из них не были доведены до промышленной серии, а существуют в виде макета или даже проекта. Однако наличие этого багажа существенно повышает оперативность разработки новых решений, поэтому мы благодарны нашим пользователям за все идеи и подсказки. Задача этой главы – показать на примерах, как рассуждает разработчик, создавая новое решение. Это должно помочь вам не испытывать «страх чистого листа» при начале работы над новым проектом.

6.1. Идеи и решения на основе технологии «Секрет» и устройств «Секрет»

Выше уже были описаны два решения на базе технологии «Секрет»: «Идеальный токен» и «ПАЖ». Их замыслы возникли из рассуждений безопасников, узнавших о «Секретах», о том, как можно применить такую флешку к тем или иным специфическим задачам, где чувствуется польза от различения компьютеров.

6.1.1. Как возник сам «Секрет»

Интересно отметить, что замысел самого «Секрета» сложился, в свою очередь, не от задачи, а «от парадигмы». После того, как был придуман и спроектирован «МАРШ!», мысль разработчиков шла по двум направлениям. Первое, очевидное – какие еще продукты можно сделать на базе этого же устройства. Второе – не очевидное ни для кого, кроме ученых с их привычкой к рассуждению в соответствии с научной методологией – как еще можно применить логику, в соответствии с которой получено это решение?

Для того чтобы в принципе было возможно пойти по второму пути, необходимо четко понимать, что это за «логика». «МАРШ!» – это память с управляемым доступом, разбитая на разделы с разными атрибутами доступа. То есть в устройстве есть два объекта контроля – субъекты доступа (кому можно) и действия (что можно).

Проектируя «МАРШ!», мы сформулировали, что

1) некоторые данные должны быть неизменяемыми (RO, это ОС),

2) некоторые – изменяемыми (RW, это данные пользователя, конфигурационные данные),

3) некоторые – быть перезаписываемыми, но при этом доступными только определенным процессам, а не пользователям (RW

Hidden, это ключи VPN – их надо менять, но не должно быть возможно использовать бесконтрольно),

4) а некоторые – можно добавлять, но нельзя удалять (Add only, это журналы событий).

Из трех типов сущностей, включенных в работу на АРМ с «МАРШ!»[43], этим описанием охвачены два: пользователи, и память. Пользователь типа «администратор» имеет доступ к конфигурациям и журналу, может перезаписывать ключи VPN, но не имеет доступа к пользовательским данным, может иметь или не иметь доступ к загрузке с «МАРШ!а». Пользователь, напротив, может использовать свои данные и загружаться, но не просматривать журнал и не менять конфигурационные данные. Компьютер же – *может быть любой*. Этот рекламный слоган отражает ситуацию достаточно верно – все, что касается компьютера – это есть ли проблемы совместимости с ним.

А что если сделать наоборот – если компьютер НЕ МОЖЕТ быть любой? В каком случае «любой» компьютер – это проблема? Есть ли польза от того, чтобы разрешить устройству самому определять, «свой» ли компьютер? Оказывается, что есть – именно так можно решить проблемы утечек через флешки.

Это рассуждение о полноте парадигмы вообще является крайне продуктивным в проектировании, целесообразно всегда задавать себе вопрос «а как еще можно?», и проверять, не осталось ли еще что-то полезное без внимания. Как правило, при перебирании вариантов комбинаций окажется, что часть из них решительно ни на что не годится[44], однако, при наклеивании этого ярлыка не следует спешить. Так, может показаться, что решительно бесполезной является комбинация «только запись», когда пользователь может писать данные в память, но не может их оттуда читать. На лекции, дойдя до этого

---

[43] Эти три взаимодействующие сущности – а) пользователи, б) память (сам «МАРШ!») и в) компьютеры, к которым подключаются «МАРШ!и».

[44] Так называемый «ночной горшок с ручкой внутри» – прикидывая размещение ручки у ночного горшка, вы рассмотрите и этот вариант, но, вероятно, его отклоните.

варианта, студенты неизменно задают вопрос о том, зачем такое может быть нужно. Действительно, нет толку от записанных данных, если их *никто* не может прочитать. Однако, смысл появляется, когда пользователей становится несколько (при работе пользователя события записываются в журнал, который он не может прочитать, но может читать администратор), а тем более полезным это становится при разграничении доступа к устройству компьютерах, это дает возможность ограничить не только то, кто может ознакомиться с журналами или записать ключи, но и то, в какой вычислительной среде он сможет это сделать. Еще один случай полезности такого ограничения будет описан в разделе про другой продукт, лишь косвенно связанный с технологией «Секрет».

Однако все изложенное описывает «теоретический» путь создания решений. Вернемся к обещанным примерам проектирования на основе высказанных пользователями идей и просьб.

Напомню вкратце, каковы были запросы, и как они трансформировались в продукты ПАЖ и «Идеальный токен».

6.1.2. Программно-аппаратный неперезаписываемый журнал

Выпустив «Секреты», мы включили их в программу наших ознакомительных семинаров и рассказов на выставочных стендах и начали рассказывать посетителям этих мероприятий – безопасникам и информатизаторам – о том, какова идея и в чем заключается принципиально новый на тот момент подход к решению задач защищенной работы с флешками. После прохождения всех обычных стадий восприятия новой идеи те из специалистов, которые оказывались в принципе готовы к смене парадигмы и осознанию того, что можно не учить компьютер различать флешки, а научить флешки различать компьютеры, начинали думать о том, какую еще пользу они могут извлечь из такой новой особенности устройства. Не надо ожидать

этого от каждого собеседника, но настоящие профессионалы, как правило, всегда задают себе вопрос «а что еще можно с этим сделать».

И вот администраторы, ответственные за сбор и архивирование журналов увидели в возможности «привязывания» носителя к компьютеру перспективу снижения путаницы в файлах журналов событий с разных рабочих мест. Обычно за этим нужно следить вручную, привязывая флешки к компьютерам через маркировку и записи в каком-либо реестре (тетради или файле). Следить за тем, чтобы журналы записывались в соответствии с назначенным порядком, нужно, разумеется, тоже вручную. Использование для этой цели «Секретов» позволит менее пристально следить за тем, чтобы не перепутать носители – журналы не перемешаются.

Вообще говоря, этой подсказки достаточно для того, чтобы позиционировать эту задачу как удачный пример применения «Секретов». Однако рассуждение о том, что еще специфичного в журналах, кроме того, что их нужно не смешивать, позволяет специализировать решение еще сильнее и спроектировать ПАЖ. В данном случае не потребовалось заново изобретать велосипед, так как раздел памяти «Add only» для хранения журналов уже был предусмотрен в «МАРШ!е». Осталось собрать пазл. Пользователь ПАЖ (это администратор, который должен собирать журналы, информатизатор) может их записывать (только с заданных компьютеров), но не может их читать (нигде). Администратор ПАЖ (это администратор безопасности информации, безопасник) – может их читать на заранее заданном компьютере, аудитор ПАЖ (обычно должность так и называется – аудитор безопасности информации, безопасник) – может просматривать настройки ПАЖ и его собственный журнал, но не журналы, заархивированные на нем. Или как-либо еще, как определит политика безопасности информации организации. Распределение полномочий по ролям пользователей в ПАЖ, конечно, должно настраиваться.

6.1.3. «Идеальный токен»

Идея идеального токена подсказана нам обращением в нашу службу технической поддержки. Обращение было за консультацией – можно ли использовать «Секрет» как хранилище ключей для одного определенного СКЗИ. У нашей службы технической поддержки, как и у любой другой, есть моральная установка «отвечать пользователю “нет” только в крайнем случае», поэтому пришлось всесторонне изучить этот вопрос, и ответить, «да, можно, но лучше…». Для того чтобы было что-то лучше «Секрета», пришлось разработать и запатентовать [1] токен, который является идеальным, так как его невозможно применить на произвольном компьютере, даже зная PIN-код. Других таких токенов нет до сих пор.

Здесь нужно заметить, что поскольку то самое СКЗИ, о котором задавался вопрос, допускало на тот момент хранение ключей практически где угодно – на жестком диске компьютера, на ТМ-идентификаторе, на флешке и даже на дискетке (которые уже в то время мало где можно было найти, и еще меньше было компьютеров с дисководами, в которые их можно было бы вставить), то, строго говоря, не было причин отвечать «нет». Хранить ключи в «Секрете» точно защищеннее, чем на флешке. Однако, не вполне рационально использовать для хранения объекта в 32-64 байта хранилище на 8-64 Гб.

Подробнее рассуждения о ключевых хранилищах и их идеальности можно прочитать в статьях об этом [2–5], а о самом «Идеальном токене» – в 3 главе, в разделе 3.2.1.

Еще два продукта, построенных на технологии «Секрет», были спроектированы также по запросу от эксплуатирующего персонала информационных систем – «Система Ниппель» и «Секрет Администратора».

6.1.4. «Система Ниппель»

Запрос на создание «Системы Ниппель» поступил не от обычного пользователя наших продуктов (насколько вообще безопасников можно считать обычными – как правило, это люди с заметной технической смекалкой), а от ученого, кандидата наук, работающего на стыке медицины и информационных технологий. Это важно потому, что толчком к предложению о создании такого решения могло послужить только то самое «рассуждение о парадигме», пример какового приведен в начале главы. Однако рассуждали не мы, а представитель эксплуатирующей организации, принимавший у нас проект, в котором одновременно применялись и «МАРШ!и», и «Секреты». Ясно поняв, что мы можем управлять состоянием памяти устройства в зависимости от некоторого внешнего условия, и можем различать компьютеры, к которому подключено устройство, он предложил нам сделать так, чтобы в зависимости от того, к чему флешка подключена, она могла бы быть либо WO, либо RO, иными словами, спроектировать однонаправленный шлюз в форм-факторе USB-устройства.

Сегодня есть достаточный выбор средств, которые контролируют только информационные потоки. Однако, они, как правило, контролируют только те потоки, которые проходят по каналам, предназначенным для их передачи. Подобный подход оставляет возможность обмена информацией посредством скрытых каналов (СК) – непредусмотренных коммуникационных сред, которые могут быть использованы для нарушения политики безопасности. Например, такой «непредусмотренной коммуникационной средой» могут быть съемные носители информации.

Одним из методов противодействия опасным СК является применение однонаправленного канала — механизма, позволяющего в целях обеспечения безопасности информации осуществлять передачу данных только в одном направлении. Этого эффекта можно добиться, например, настройкой мандатного механизма разграничения доступа в

СЗИ НСД и применением «Секретов». Разграничение доступа должно обеспечить режим, в котором будет исключено «перетекание» данных между сегментами разного уровня доступа (можно настроить, что на данном ПК с данной флешки – только читать, и так далее), но они никак не помогут предотвратить вынос информации на флешке вообще за пределы системы – за это будет в этом случае отвечать «Секрет».

Система получается довольно сложная, можно вынести эту задачу в отдельное решение. Таким и является ПАК «Система Ниппель». Это отчуждаемый шлюз, построенный по технологии «Секрет» и предназначенный для организации однонаправленного канала передачи данных конфиденциального характера. Канал создается так. На каждом устройстве задается режим доступа к памяти («только чтение», «только запись», «чтение и запись») для каждого компьютера или сегмента сети. В результате при подключении «Системы Ниппель» в сегменте сети с низким уровнем защищённости доступ к памяти открывается в режиме «чтение и запись» или «только запись», а при регистрации в сегменте сети с высоким уровнем защищённости — «только чтение». При таких параметрах доступа у пользователя не будет возможности копировать информацию высокого уровня доступа и переносить её в сегмент сети с низким уровнем доступа.

Рассмотрим на примере.

Пусть в некоторой информационной системе имеется два сегмента сети: с высоким и низким уровнем защиты. В сегменте сети с высоким уровнем защиты обрабатывается и хранится информация высокого уровня доступа, а в сегменте сети с низким уровнем защиты – низкого уровня доступа. Пользователь с низким уровнем доступа к информации в рамках своих должностных обязанностей должен получать некую информацию из СВТ, расположенного в сегменте сети с низким уровнем защиты, и переносить ее (информацию) на СВТ из сегмента сети с высоким уровнем защиты. Реализация этих действий с применением «Системы Ниппель» выглядит следующим образом (рисунок 6.1):

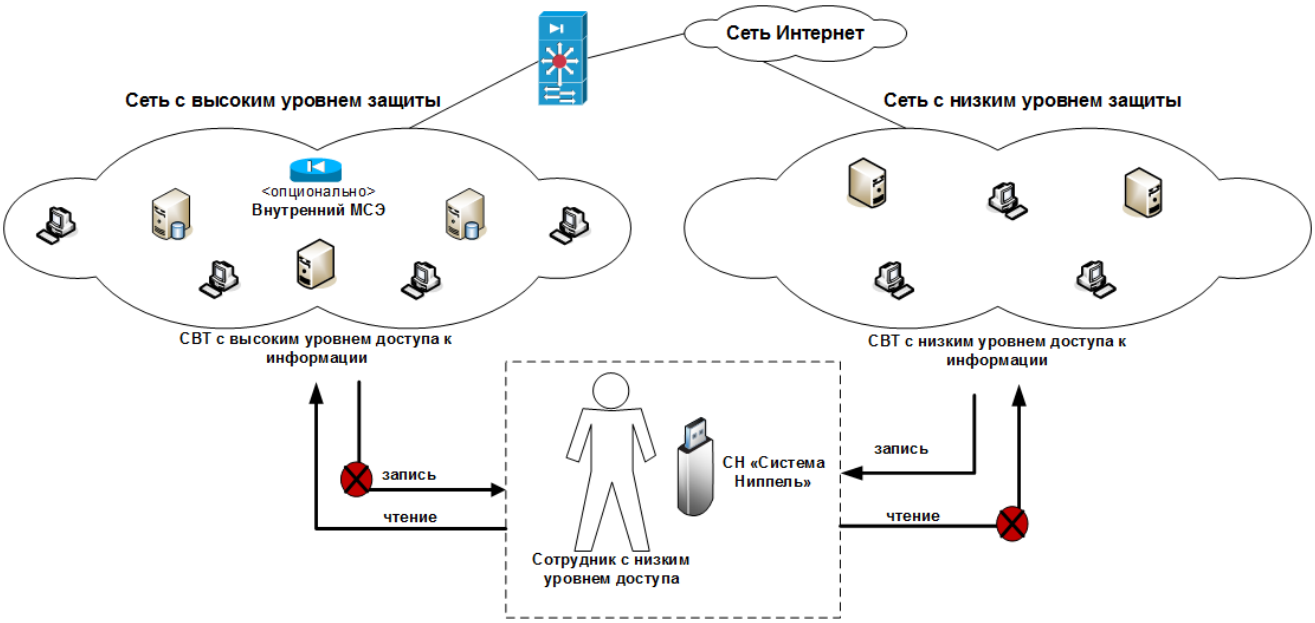


Рисунок 6.1 – Пример организации одностороннего канала передачи данных посредством «Система Ниппель»

Общая схема работы:

1) пользователь выполняет подключение «Системы Ниппель» к СВТ с низким уровнем доступа к информации;

2) блок идентификации/аутентификации проверяет, относится ли СВТ к разрешенным для работы; опционально может проводиться идентификация/аутентификация пользователя;

3) если да (относится), то блок контроля доступа, разрешает обращение к flash-памяти в рамках режима доступа, заданного для этого СВТ. Поскольку мы рассматриваем пример, где «Система Ниппель» подключен к СВТ в сегменте сети с низким уровнем защиты, пользователь получает только в режиме «запись»;

4) далее пользователь копирует на устройство необходимую информацию с СВТ низкого уровня доступа к информации и переносит информацию в сегмент сети с высоким уровнем защиты;

5) на СВТ с высоким уровнем доступа выполняются такие же проверочные действия;

6) блок контроля доступа «Системы Ниппель» разрешает обращение к памяти в режиме «только чтение».

Разумеется, если проверки на СВТ какого-либо сегмента сети (с высоким или низким уровнем доступа) не увенчались успехом, то в доступе будет отказано: блок идентификации/аутентификации не направит в блок контроля доступа команду, разрешающую обращение к устройству со стороны интерфейса USB.

Таким образом, пользуясь случаем передачи нужной информации на СВТ с высоким уровнем доступа к информации, записать заодно на устройство информацию конфиденциального характера пользователь не сможет.

6.1.5. «Секрет Администратора»

Идея «Секрета Администратора» сформировалась более стандартным путем – информатизаторы, услышав про «Систему Ниппель» поняли, что это почти то, что им нужно, только требуется слегка сместить акценты (в некотором смысле может показаться, что сместить их пришлось вплоть до «наоборот»).

Одна из задач системных администраторов (информатизаторов) – поддерживать бесперебойное функционирование рабочих мест, в том числе, оперативно устранять неполадки и сбои в работе программного обеспечения на подконтрольных рабочих местах. Для этого администраторы как правило носят с собой флешку (или иной съемный носитель, жесткий диск) с эталонными дистрибутивами необходимого ПО, чтобы в случае необходимости быстро установить его там, где внезапно «сломалось».

Администратор заинтересован в том, чтобы эталоны ПО на этой флешке не повреждались случайно или намеренно, а на флешку не записывались вирусы (которые, вполне возможно, есть на рабочих местах пользователей, ведь сбои так или иначе происходят по каким-то причинам – возможно, как раз из-за вирусов). В то же время на своем собственном компьютере администратору нужно иметь возможность записывать на флешку все то, что ему нужно установить пользователям,

включая обновления ПО (то есть иметь возможность и перезаписывать, а не только записывать). Владелец системы при этом заинтересован, чтобы администратор устанавливал ПО только в рамках его системы, а не распространял бесконтрольно на свое усмотрение.

Таким образом, требуется съемный носитель, который на одном компьютере будет работать на чтение и запись, на остальных компьютерах системы – на чтение, а на компьютерах вне системы не будет работать совсем.

Разберем на примере.

Пусть в некоторой информационной системе администратор работает на своем АРМ, где записывает на «Секрет Администратора» эталонное ПО для установки на СВТ пользователей. Порядок работы с «Секретом Администратора» выглядит следующим образом (рисунок 6.2):

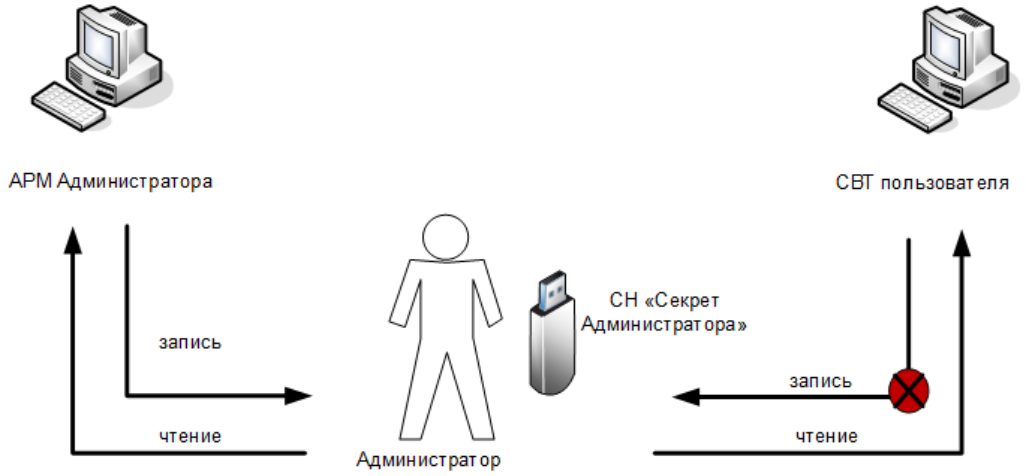


Рисунок 6.2 – Пример работы СН «Секрет Администратора»

Общая схема работы:

1) Администратор подключает носитель к АРМ Администратора;

2) Блок идентификации/аутентификации выполняет проверку СВТ, опционально – пользователя (в это время блок контроля доступа запрещает обращение к носителю со стороны интерфейса USB, то есть вирусы не записываются);

3) В случае положительного завершения проверок данные об успешной и/а передаются блоку контроля доступа, который разрешает обращение к flash-памяти в рамках заданного для данного СВТ режима доступа. В соответствии с рисунком 6.2 доступ к flash-памяти СН на АРМ Администратора предоставляется на «чтение и запись»;

4) Администратор копирует заранее подготовленный набор образов ПО на «Секрет Администратора» и переносит это ПО на СВТ пользователя;

5) После подключения носителя к СВТ пользователя блок идентификации/аутентификации выполняет проверку СВТ, опционально – пользователя[45] (в это время блок контроля доступа запрещает обращение к носителю со стороны интерфейса USB);

6) В случае успешного завершения проверок блок и/а передает управляющее воздействие блоку контроля доступа, который разрешает обращение к flash-памяти СН в рамках заданного для данного СВТ режима доступа. В соответствии с рисунком 6.2 на СВТ пользователя доступ к flash-памяти носителя, на которой хранится набор образов эталонного ПО, предоставляется только на «чтение».

Если же проверки на АРМ Администратора ИБ и/или на СВТ пользователя не увенчались успехом, то в доступе будет отказано: блок и/а не направит в блок контроля доступа команду, разрешающую обращение к памяти со стороны интерфейса USB.

Действуя таким образом, при копировании образов эталонного ПО на СВТ пользователя Администратор ни умышленно, ни случайно (например, посредством скрытых каналов) не сможет повредить эталонные образы или заразить флешку вирусами с пользовательского

---

[45] Здесь важно не упустить из виду, что «пользователь» «Секрета Администратора» – это тот самый Администратор, пользователь СВТ, на котором Администратор что-то чинит, здесь не при чем. Эта проверка может устанавливаться, если предполагается, что сотрудники (или иные злоумышленники) почему-либо попытаются несанкционированно воспользоваться носителем эталонного ПО. Большого смысла в этой предосторожности нет, поэтому это опциональная возможность, а не обязательная функция.

компьютера. Также он не сможет (хотя, конечно, хорошие администраторы так никогда и не делают) установить принадлежащее компании ПО кому-то другому в качестве подарка или подработки.

Легко заметить, что эти продукты – «Система Ниппель» и «Секрет Администратора» очень похожи. Логика реализации из основной защитной функции одинакова – контролируется направление передачи данных: в одном направлении данные передавать можно, а в другом – нельзя). Одинакова и примененная технология – управление атрибутами доступа к разделу в зависимости от СВТ, к которому подключен носитель. Все, что в этих продуктах различно, касается вещей, которые для разработчика второстепенны, но крайне важны для пользователя: ролевой структуры, сценариев работы, предусмотренных как основные, возможностей настройки того, что нужно, и отсутствия необходимости настройки того, что для данного применения неважно и не интересно. Разберем на этом примере подробнее, чтобы, самостоятельно анализируя другие решения, вы могли не упускать из виду такие нюансы.

В таблице 6.1 сравним наборы функций, реализованных в «Системе Ниппель» и «Секрете Администратора», помимо собственно управляемого доступа к памяти с заданными атрибутами доступа.

Таблица 6.1 – Сравнение наборов функций носителей

№	Характеристики специальных носителей	Специальные носители (СН)	
		«Система Ниппель»	«Секрет Администратора»
1)	регистрация администратора	+	+[46]
2)	настройки PIN-кода администратора (длина PIN-	+	+

[46] Это единственный пользователь «Секрета Администратора», но он обладает полными правами по установке изменению всех доступных для управления настроек, поэтому в контексте сравнения с другим устройством, где есть привилегированный и непривилегированный пользователь, корректно называть его администратором.

	кода, число неверных попыток доступа к СН)		
3)	смена PIN-кода администратора	+	+
4)	идентификация и аутентификация администратора при доступе к СН	+	+ <опционально>
5)	идентификация и аутентификация пользователя при доступе к СН	+	-
6)	механизм контроля доступа к flash-памяти СН	+	-
7)	настройки PIN-кода пользователя (длина PIN-кода, число неверных попыток доступа к СН)	+	-
8)	регистрация пользователя	+	-
9)	аннулирование регистрации пользователя	+	-
10)	ведение журнала работы СН	+	+
11)	разблокирование СН	+	+
12)	сброс СН	+	+
13)	создание списка СВТ, на которых разрешено использован СН	+	+
14)	<опционально> настройка размера диска СН	+	+
15)	настройка временного интервала работы с СН	+ <опционально>	-

16)	возможность проверки целостности эталонных образов ПО	-	+ <опционально>

Когда различия уже визуализированы, они очевидны, и, кажется, не требуют комментирования. Основное из них – разная ролевая структура, обусловленная разницей в сценарии применения. «Секрет Администратора» применяется Администратором, сотрудником, относящимся к управляющему персоналу информационной системы. Выделять для работы с его узкоспециализированным инструментом еще одного отдельного администратора, который будет задавать настройки для этого устройства, представляется нецелесообразным. Если же в организации установлен регламент, в соответствии с которым управлять настройками безопасности (к которым относятся параметры PIN-кода и допустимого число его вводов, разблокировка и тому подобные) должны исключительно Администраторы ИБ (безопасники, а не информатизаторы), то администратором «Секрета Администратора» можно зарегистрировать безопасника, но при этом снять режим и/а пользователя при работе с устройством (он опциональный). Тогда PIN-код будет запрашиваться только для настроек, и при работе не требоваться, и Администратору (информатизатору) знать его будет не нужно, таким образом и будут разделены функции управления устройством и функции его использования.

В «Системе Ниппель» же функции управления и использования безо всяких сомнений будут в большинстве случаев использоваться разными сотрудниками, и ролевая структура необходима.

15 и 16 пункты – опциональные возможности, целесообразные для одного или другого решения – приведены в качестве примеров, они могу быть дополнены еще рядом аналогичных по запросу потенциальных пользователей или на основании соображений

продающих подразделений (которые они формируют, изучая требования конкурсов на поставки средств защиты).

6.1.6. Случаи, когда второстепенная функция становится главной

В этом параграфе объединены продукты, возникшие в результате того, что какая-то из функций «Секретов» оказалась для кого-то важнее их основного назначения (флешка, которая работает на разрешенных компьютерах и не работает на всех остальных).

Это продукты «Транзит» и «Мобильный носитель лицензий» (МНЛ). Первый был создан в результате взаимодействия с Заказчиком, а во втором мы решили свою собственную задачу (сделали продукт для себя, в каком-то смысле).

6.1.6.1. Неперепрограммируемая флешка «Транзит»

Когда получили широкую огласку (в узком кругу специалистов) уязвимости, связанные с Intel ME, те специалисты, которые оказались способны посмотреть на ситуацию системно, придали гораздо больше значения, чем раньше, и другим уязвимостям различных устройств, которые в свете возможностей IME «заиграли новыми красками».

С подсистемой IME связаны угрозы двух видов:

- получение несанкционированного удаленного управления
- несанкционированная передача конфиденциальных данных за пределы основного СВТ [6].

Каналами реализации угроз обоих видов может быть как Ethernet, так и USB. Подключаемые к USB-портам устройства (флешки, клавиатуры, мыши, токены, сканеры, принтеры, плоттеры, телефоны, фотоаппараты, жесткие диски) могут быть как каналом несанкционированного управления, так и приемником для

несанкционированной передачи данных. Причем выполнять нештатные действия они могут в теневом режиме, незаметно для пользователя, подключившего их к USB-порту, параллельно с основным функционалом. Фактически даже самая простая флешка представляет собой компьютер с собственным процессором и собственной памятью. Известен целый класс атак, называемый BadUSB, в основе которого лежит модификация firmware USB-устройств для выполнения несанкционированных действий процессором этих самых USB-устройств. Кроме того, существуют варианты реализаций штатных протоколов взаимодействия USB-устройств [7] с нештатными расширениями, которые могут быть использованы и как скрытые каналы управления, и как нелегальные хранилища для конфиденциальной информации.

При этом важно понимать, что IME имеет прямой доступ к периферии (в том числе и к USB-контроллерам), минуя приложения и драйвера ОС, а программные агенты DLP-систем, функционирующие в ОС, могут определять наличие подключенных к портам устройств только с некоторой задержкой, необходимой ОС для проведения работ по инициализации стека драйверов и извещения соответствующих агентов о подключении устройств к портам. И последующий контроль за обменом данными с устройством агенты DLP-систем могут проводить не ниже драйверов ОС. IME же может взаимодействовать с подключенными USB-устройствами напрямую через firmware USB-контроллера. То есть DLP-системы в этом случае решительно бесполезны.

Для блокирования уязвимости требуется доверенный вычислитель между компьютером и USB-устройством, или прямо в составе USB-устройства.

Понимая ситуацию именно таким образом, к нам обратилась одна компания разработчик и интегратор средств защиты и защищенных информационных систем (одна из старейших и наиболее авторитетных на рынке). Специалисты компании, построив описанную выше логику,

решили использовать в качестве USB-накопителей в одном проекте, требующем высокой степени защищенности, не обычные флешки, а ШИПКИ (персональные СКЗИ разработки ОКБ САПР, включавшие в состав устройства диск масстoрадж). Действительно, это USB-устройство, в котором есть доверенный вычислитель, который делает невозможным перепрограммирование firmware устройства, и диск, который можно использовать, как накопитель. Надо сказать, что компания просто не знала о «Секретах», так как продукт был еще достаточно новый, иначе они бы несомненно остановили свой выбор на них.

Обсудив задачи и то, в какой мере подходят ее решения ШИПКИ и «Секреты», мы пришли к выводу, что функциональность «Секрета» хоть и заметно ближе к искомой, но все же ощутимо избыточна, и целесообразно реализовать устройство, которое не будет иметь ненужной для данного проекта подсистемы и/а и разграничения доступа, а будет только неперепрограммируемой флешкой. Если firmware нельзя будет перепрошить, организовать канал утечки не получится. Была создана такая флешка, ей дано название «Транзит», так как она предназначена *только* для переноса данных с места на место и ни для чего иного.

6.1.6.2. Мобильный носитель лицензий

Долгое время (десятки лет) ОКБ САПР разрабатывало и производило исключительно программно-аппаратные комплексы. Сначала, если вспомнить дела давно ушедших дней, мы вообще не заботились о том, чтобы как-то лицензировать ПО, просто продавали наборы «Аккорд-АМДЗ + диск с ПО», потом, когда обнаружили, что все чаще покупают 1 комплекс и пару сотен Аккордов-АМДЗ, догадались, что столкнулись с бытовым пиратством, и ввели лицензионные ключи, которые «привязывали» ПО к контроллеру по его серийному номеру. Это было очень удобно, так как даже в тех редких случаях, когда

контроллеры покупались отдельно, а ПО отдельно, посмотреть в формуляре или в «Инфо» контроллера его серийный номер, передать его нам и получить лицензию – было легко.

Однако со временем в номенклатуре продуктов появились программные, и вопрос о лицензировании встал гораздо более остро. Основным способом продажи ПО на сегодняшний день является именно продажа лицензий. Для организации этого процесса необходимо решить две задачи, одна из которых коммерческая, а вторая техническая:

1. разработка схемы лицензирования продукта;
2. разработка механизма распространения лицензий.

После того, как владелец ПО продумал схему лицензирования, ему необходимо решить, каким образом лицензии (представляющие собой файл лицензии, ключ лицензии или что-либо иное) будут попадать к конечному пользователю. При этом во главу угла зачастую ставится вопрос защиты от тех, кто желает получить лицензии бесплатно. Однако это не все, важно соблюсти баланс между защищённостью и удобством, ведь если выдавать лицензию на листе бумаги с печатью под роспись в центральном офисе компании, то количество желающих воспользоваться продуктом резко сократится. Наоборот, покупатели, особенно, интеграторы, которые покупают продукт для установки в систему Заказчика, как правило хотят, чтобы лицензии попадали к ним мгновенно в любое время, а устанавливались и активировались без усилий.

Наиболее распространёнными механизмами передачи лицензий в настоящее время являются:

1. Передача покупателю не привязанного к рабочей станции ключа лицензирования (набора символов, который активирует ПО). Ключ может быть указан в коробке с ПО (на отдельном вкладыше или на самом диске). Это одноэтапный процесс, после получения ключа пользователь сразу может активировать ПО.

2. Формирование привязанного к рабочей станции ключа лицензирования. В данном случае ключ — это тоже набор символов для активации ПО, но теперь в нём указан идентификатор рабочей станции. Отличием от предыдущего способа распространения является многоэтапность процесса: необходимо считать данные с рабочей станции, передать их продавцу и затем передать готовый код обратно покупателю. Этот процесс может быть реализован, например, при помощи центрального сервера лицензирования, или путём общения по почте/телефону между сотрудниками организации-покупателя и организации-продавца.

3. Передача USB-ключа (такого как HASP) — устройства, на котором хранится информация, проверяемая при старте ПО, или некие данные, необходимые для работы программы, или, в некоторых случаях, часть кода программы. Обычно передаётся заказчику от продавца вместе с дистрибутивом. Ключ должен быть постоянно подключен к рабочей станции, чтобы ПО работало. Соответственно, для каждой копии ПО нужно отдельное устройство.

Это именно самые распространенные способы, есть и более экзотические, в том числе предложенные когда-то и нами [8].

У всех этих способов есть свои недостатки. Слабая защищённость, сложность и длительность процесса, наложение дополнительных условий (например, наличие интернета у конечного пользователя) и необходимость поддержки сервера в случае передачи лицензий через центральный сервер лицензирования, увеличение цены продукта в случае использования аппаратных ключей (например, цены на Guardant ~1-4,5 тыс. рублей, и на эту сумму повысится стоимость одной копии продукта).

Мы выбрали второй способ, но он нам, разумеется, не нравился. Вот как выглядит процесс получения лицензии в этом случае (без учета того факта, что в некоторых организациях передать данные о компьютерах наружу крайне сложно, и в эту схему добавляются еще внутренние согласования).

Для формирования лицензионного ключа производственный отдел должен получить сведения о рабочей станции, стало быть, клиент их должен передать. Рассматриваем идеальный случай, когда приобретается ПО для себя конечной эксплуатирующей организацией, и рабочая станция, для которой оно покупается уже есть (а не планируется к приобретению), и уже известно, какая. В этом случае получить уникальные идентификационные признаки рабочих станций (UID) в принципе реально. Для этого эксплуатирующая организация получает специальную утилиту, она запускается на будущем подконтрольном объекте и формирует набор данных, необходимый для генерации лицензии. Тогда при оформлении покупки у клиента запрашивают этот UID, передают в производственное подразделение, и клиент получает лицензии сразу вместе со всей покупкой.

Хуже, если приобретаются СЗИ для компьютеров, которые еще тоже только покупаются. В этом случае обратиться за лицензионным ключом покупатель должен тогда, когда у него будет в распоряжении рабочая станция и он сможет получить ее UID.

Ситуация еще более неудобна, если покупатель – интегратор, и он ведет работы по вводу системы в эксплуатацию в условиях сжатых сроков. Лицензии ему почти наверняка понадобятся ночью из-за разницы во временных поясах.

Еще одно существенное обстоятельство заключается в том, что запрос на лицензию генерируется для каждой отдельной машины, и в ответ именно на него приходит лицензия для нее. Этот процесс выглядит впечатляющим, если представить себе работы на тысячах машин.

Решение пришло нам в голову, когда мы заметили, что сбор данных о машине для создания UID для лицензии напоминает сбор данных о машине «Секретом» для проверки, входит ли этот компьютер в список разрешенных.

У нас уже есть устройство, которое может собирать сведения о компьютере, почему бы не научить его и генерировать лицензии, а затем устанавливать их в нужную папку?

По существу, предметом продажи являются не сами лицензии, а количество допустимых установок ПО. Значит, устройство должно иметь счетчик лицензий, значение которого задается при покупке лицензий и уменьшается на 1 при каждой установке.

Так была сформулирована идея «Мобильного носителя лицензий» (МНЛ). Затем она «доводилась до ума» учетом различных нюансов распространенных сценариев – например, оказалась необходимой возможность загружать новое значение счетчика при докупке лицензий, передавать лицензии с устройства на устройство (чтобы разделить их между объектами или между администраторами для организации параллельных работ). Подробнее можно прочитать о МНЛ на сайте ОКБ САПР или в документации на продукт [9, 10].

6.2. Продукты и решения, возникшие на основе ПСКЗИ ШИПКА

Для того чтобы изложенное в этом параграфе было понятно, необходимо рассказать в нескольких словах о самом ПСКЗИ ШИПКА, хотя этот класс продуктов сейчас не выпускается, а семейство ШИПКА представлено персональным идентификатором (ПИ) ШИПКА.

Однако разрабатывалась ШИПКА как ПСКЗИ (персональное средство криптографической защиты информации), и название его было аббревиатурой: Шифрование – Идентификация – Подпись – Коды Аутентификации. ПСКЗИ ШИПКА было сертифицировано как СКЗИ КС3 и СЭП КС3. При желании погрузиться в историю этого продукта, можно ознакомиться с подборкой публикаций о нем на сайте ОКБ САПР [11]. Ключевое свойство ШИПКИ состояло в том, что криптография в ней была реализована полностью аппаратно. Такую возможность давало использование микроконтроллера (в отличие от смарт-карточных чипов, которые сделать это не позволяют), был физический датчик случайных чисел, с которым работал процессор устройства, и таким образом все криптографические процедуры от получения случайного числа для генерации ключа, до собственно криптографического преобразования производились строго аппаратно, внутри устройства, без передачи каких-либо данных в память компьютера (который считаем по умолчанию не доверенным).

Продукт имел определенный спрос, но со временем от него решено было отказаться из-за слишком высокой себестоимости (однако в некоторых информационных системах федерального масштаба ШИПКИ до сих пор используются (на момент написания этой книги) именно в качестве СКЗИ, о том, как организован там обмен зашифрованными видео-данными, вам расскажут на семинаре, здесь не будем уходить настолько далеко в сторону.

Итак, ПСКЗИ ШИПКА было разработано как USB-устройство с аппаратной криптографией, включая физический ДСЧ и генерацию ключей.

Это дало толчок к творческому осмыслению возможностей применения этого устройства для разнообразных задач, которые будут описаны ниже. Здесь стоит упомянуть, что в рамках совершенствования собственной функциональности ШИПКИ однажды в нее был добавлен диск масстoрадж, с тем чтобы на нем пользователь мог носить с собой персональную вычислительную среду и работать в ней на произвольном компьютере. Из этого, как теперь, читая ретроспективу, совсем не сложно догадаться, выросла идея «МАРШ!а».

6.2.1. Физический датчик случайных чисел с USB-интерфейсом

Впервые мы поняли, что ДСЧ – это самоценная функциональность, когда к нам за ШИПКАМИ обратилась компания, которой нужны были случайные числа для проведения лотереи. Количество необходимых им устройств было невелико, а их стоимость компанию не смутила, поэтому как отдельное устройство USB-ДСЧ возник позже, когда другому заказчику понадобился специфический форм-фактор – для установки внутрь корпуса компьютера, со штырьковым разъемом.

В отличие от ПСКЗИ ШИПКА, где было пользовательское программное обеспечение с утилитами для генерации ключей, самоподписанных сертификатов, шифрования и подписания ЭП с помощью сертификатов и непосредственно на ключах, в USB-ДСЧ ничего этого не требуется, это устройство только выдает по запросу случайную последовательность, и ничего более.

Для запроса случайной последовательность можно использовать библиотеку CCID, входящую в состав операционной системы ПЭВМ (это рекомендованный вариант) или запрос напрямую через порт USB (для случаев, когда библиотека работы с CCID недоступна).

Поскольку использование USB-ДСЧ может быть самым разным, устройство реализуется с различными типами разъема USB: тип А или штырьковый с прямым разъемом, либо штырьковый с разъемом под углом 90 градусов, а также с разъемом PBS.

6.2.2. KeyMaker – Мастер ключей

Одной из функций ШИПКИ, как уже упоминалось, была генерация ключей с использованием российских и зарубежных алгоритмов и случайных чисел, сгенерированных физическим ДСЧ. Тем, кто изучает техническую защиту информации на материале устройств ОКБ САПР, наличие в устройстве физического датчика случайных чисел на шумовых диодах кажется естественным и прозаическим обстоятельством. Однако, например, в европейских странах нам не раз на сообщение об этом отвечали – «да ну что Вы говорите, такого не бывает». Дело тут, конечно, не только в том, что ОКБ САПР гораздо лучше всех в Мире умеет делать устройства. Есть и другие причины.

Одна из самых значительных, и она упоминалась в самых разных разделах этой книги, заключается в том, что работа с криптографическими ключами требует развертывания ключевой инфраструктуры. Для работы с асимметричной криптографией давно существует, хорошо развита и описана инфраструктура открытых ключей (ИОК, или Private Keys Infrastructure – PKI). В нашей стране используется ИОК вертикального типа, с Удостоверяющими центрами, а «сеть доверия» (web-of-trust) не распространена и официально не признана как альтернатива Удостоверяющим центрам. При этом Удостоверяющие центры, которые, вообще говоря, должны выполнять одну функцию – удостоверять принадлежность ключа проверки подписи и его связь с ключом подписи, то есть выдавать сертификат ключа подписи (СКП), на деле «выдают электронную подпись», то есть генерируют ключевую пару, записывают ее и СКП на носитель (чаще всего токен), и выдают все это вместе клиенту. Это воспринимается

большинством клиентов как единственно возможный и правильны вариант, хотя это далеко не так. Подробнее об этом можно прочитать здесь [12]. Однако обо всех этих тонкостях вы узнаете в рамках других дисциплин, здесь же вернемся к тому, как получилось, что в таких условиях именно функция генерации ключа стала основной для нового продукта, разработку которого заказала компания, имевшая представление о ШИПКЕ и ее функциях. Им было нужно устройство, которое могло бы генерировать ключи.

Дело в том, что, хотя инфраструктура открытых ключей позволяет решать огромное количество прикладных задач криптографии, она накладывает существенные ограничения, которые зачастую вызваны самыми базовыми принципами технологии. Камнем преткновения в этой истории стал принцип сохранения в тайне ключа подписи. В большинстве систем ключ подписи знает и может использовать только владелец этого ключа. Противное является нарушением условий эксплуатации, компрометацией ключа и должно приводить к немедленному принятию мер.

У обратившейся к нам компании появилась задача, в которой использовать ключ должен был не его владелец, а кто-то другой (пусть это будет условный подрядчик), естественно, при наличии некоторого контроля со стороны владельца. На первый взгляд задача кажется невыполнимой: никто не должен знать чужой ключ подписи. Однако в основе кажущегося парадокса лежит лишь несколько слишком образное восприятие связанных с криптографическими ключами понятий, а отнюдь не объективное противоречие.

Дело в том, что «знать» ключ для того, чтобы его использовать, вообще говоря, не надо. Более того, в большинстве случаев ключи никто и не «знает». Словом «знать» разработчики жаргонно выражают смысл «иметь возможность произвести операцию».

Теперь задача звучит менее философски и более решаемо: необходимо, чтобы *строго определенную операцию* с ключом мог совершать *не* его владелец. При этом ему не должны быть доступны ни

одна *другая* операция с этим ключом, кроме разрешенной, а разрешенные операции должны учитываться (в зависимости от сценария работы это может производиться по-разному, в той конкретной системе это был контроль кратности операции, но могли бы быть и просто записи о каждом факте операции или тех или иных ее параметрах).

Для решения этой и подобных задач было создан продукт KeyMaker, который позволяет сгенерировать мастер-ключ (или записать, если необходимо, чтобы ключ был сгенерирован каким-то другим образом) и производить с ним необходимые криптографические операции (в данном случае – генерацию производных ключей) прямо внутри устройства. Мастер-ключ неизвлекаем, в KeyMaker нет функции его экспорта.

KeyMaker имеет встроенный журнал работы с ключами. Журнал находится во внутренней памяти устройства и доступен пользователю только на чтение. При необходимости всегда можно отследить, сколько раз мастер-ключ использовался, в каких функциях и, опционально, с какими данными.

Опционально устройство может содержать встроенные часы реального времени, что позволяет ввести ограничение на время использование ключа.

Владелец мастер-ключа при записи ключа в устройство может задать максимальное количество операций с ключом.

Таким образом получаем следующую логику работы. Владелец мастер-ключа хочет передать своему агенту полномочия по реализации некоторых криптографических функций. И не хочет, чтобы агент распоряжался мастер-ключом сверх делегированных ему полномочий. Владелец записывает мастер-ключ в устройство и передает устройство агенту. Агент выполняет необходимые функции в пределах ограничения по количеству использований мастер-ключа и времени его использования. Владелец мастер-ключа при необходимости или по

регламенту проверяет журнал устройства. Таким образом агент выполняет криптографические функции, но не «знает» мастер-ключ.

Также в устройство можно добавить функцию «идеальности»: в этом случае устройство будет работать только на тех АРМ, которые были в нем предварительно зарегистрированы. Проверка соответствия АРМ списку разрешенных будет выполняться процессором устройства, список разрешенных АРМ – содержаться во внутренней памяти устройства, аналогично тому, как это реализовано в «Идеальном токене» или «Секрете Особого Назначения». В этом случае агент сможет выполнять только доверенные ему криптографические операции только на тех АРМ, которые ему заранее разрешены. Но конкретно тому заказчику, который поручил нам эту разработку, эта функциональность не понадобилась.

6.2.3. Центр-Т: централизованная работа с терминальными образами

Функции ПСКЗИ ШИПКА – генерация и хранение ключей, вычисление хеш-функций, а также функция персонального идентификатора пользователя как в ОС, так и в Аккордах (и Аккорде-АМДЗ, и СЗИ Аккорд, в том числе в клиентской части – Аккорд ТК) – обусловили ее применение в составе решения КАМИ-терминал компании «Ками». Решение было предназначено для обеспечения контролируемой загрузки целостного образа ОС терминальной станции. Из микросхемы памяти аппаратного бездискового терминала, который изготавливался также компанией «КАМИ», после и/а пользователя в ПСКЗИ ШИПКА стартовала загрузочная ОС, которая инициировала терминальную сессию с сервером хранения и загрузки (также компании «КАМИ»), с которого терминал получал образ ОС, предназначенный для пользователя данной ШИПКИ. Целостность образа проверялась вычислением хеш с помощью ШИПКИ и его

сравнением с записанным в ШИПКУ эталоном. Затем, когда проверенный образ загружался в оперативную память терминала, стартовала терминальная сессия с терминальным сервером, и в ПАК СЗИ НСД «Аккорд», установленном на терминальном сервере, пользователь идентифицировался и аутентифицировался также с помощью той же ШИПКИ.

Решение было революционным, так как до тех пор никто не пытался всерьез озаботиться защитой ОС терминальной станции. Однако, оно было не очень удобным в администрировании – в частности, когда загружаемые образы обновлялись, чтобы начать их применять, нужно было собрать все ШИПКИ и переписать в них эталонные значения хеш. А главное, оно привязывало эксплуатирующую организацию к одному производителю терминалов, так как никакие аппаратные терминалы, кроме «КАМИ», это решение не поддерживало, и поддержку других моделей компания «Ками» оценивала достаточно высоко (откровенно говоря, просто называла заградительную цену).

Выход был подсказан самой архитектурой решения – терминалы не имели жестких дисков, а образ начальной загрузки загружался с микросхемы памяти NAND. В линейке ПСЗКИ ШИПКИ, как уже упоминалось, как раз было устройство ШИПКА-2.0, в состав которого входила микросхема памяти NAND, на которой был реализован диск «массторадж». Решение напрашивалось – что, если загружать образ начальной загрузки с NAND из ШИПКИ, а не из терминала?

В результате нам заказали комплекс «точно такой же, но с перламутровыми пуговицами». А именно:

- чтобы образ начальной загрузки загружался с ШИПКИ;

- чтобы он допускал использование различных СВТ в качестве терминальных станций;

- чтобы он допускал использование различных СВТ в качестве сервера хранения и сетевой загрузки;

- чтобы было возможно централизованное администрирование загружаемых образов без необходимости сбора ШИПОК и перезаписи хешей;

- чтобы пользователь не заметил разницы.

Таким и был разработан «Центр-Т», подробнее о котором можно прочитать в [13, 14, 15]. Способ загрузки терминальных станций, реализованный в ПАК «Центр-Т» был запатентован [16].

6.3. Продукты и решения сложного генезиса

Не всегда, разумеется, новые идеи и новые продукты возникают таким легко фиксируемым путем (подчеркнем, этот пусть легко зафиксировать и описать пост-фактум, это не значит, что сам процесс выведения логики так уж тривиален). В качестве примера более замысловатых, но все же прослеживаемых ходов мысли можно привести еще несколько продуктов и проектов совершенно различного плана.

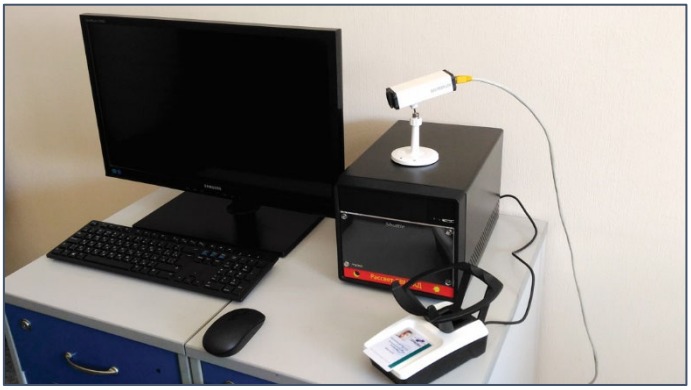
6.3.1. Очень маленький универсальный хаб «Рассвет» (МКТ-card long)

В главе 3 – про разграничение доступа – в разделе 3.1.2.4 упоминалось решение для интеграции системы защиты от НСД и СКУД – СВМиКД на основе комплекса «Рассвет-СВМиКД».

История создания этого решения сама по себе небезынтересна, но тут она является скорее предысторией. Дело в том, что задача, изначально поставленная нам в общем виде нашим постоянным заказчиком, сводилась примерно к тому, чтобы за счет использования контроллеров Аккорд создать отдельную сеть передачи данных, независимую от основной и не влияющую на нее. Эту сеть будет использовать СКУД и централизованная система СЗИ НСД. Это было связано не столько с тем, чтобы сделать более надежной или защищенной передачу данных, связанных с безопасностью (то есть тех, что надо было отделить от основной сети), сколько наоборот, с требованиями к передаче данных по основной сети. В той информационной системе они таковы, что никаких данных, кроме целевых (платежных) по ней передаваться не должно. Потом уже эта задача обрастала большим количеством подробностей, в ряду которых этот изначальный контрапункт стал практически незаметен даже

самому интересанту. Однако, для нас это было очень существенной архитектурной особенностью системы. Постепенно заказчик входил во вкус и подсистем, данные которых стало необходимо «передавать через Аккорды» стало много: видеокамера, считыватель биометрических данных, кард-ридер, граббер (это средство захвата изображения с экрана (так как необходим был видеопоток, а не скриншоты, пусть даже и раз в секунду)) и так далее. Стало очевидно, что подключить все это прямо на борт Аккорда уже невозможно, и надо делать какой-то «хаб». Это устройство получило внутреннее название (то есть мы так его звали между собой) «Универсальный хаб “Рассвет”», или сокращенно УХР.

Затем выяснилось, что необходимо также минимизировать число подключений, поэтому нужно все, что можно, соединить в одном корпусе. Чтобы все поместилось, корпус пришлось взять довольно большой (как маленький системный блок), а соответственно, называться он должен был уже «Большой Универсальный хаб “Рассвет”», или сокращенно БУХР. Разумеется, официальное название было другим – Комплекс «Рассвет-СВМиКД», а БУХРом мы и по сей день ласково зовем его между собой.



Самый большой по размеру компонент БУХР – граббер, устройство для захвата изображения с экрана монитора. Поэтому для тех подконтрольных объектов, у которых нет мониторов, мы сделали МУХР – «Маленький Универсальный хаб “Рассвет”».

На этом предысторию можно закончить (вы сможете узнать детали этого крайне интересного решения у разработчиков ОКБ САПР в рамках стажировок и семинаров) и перейти к истории – истории создании совершенно другого решения в рамках плановых работ по развитию ПАК «Центр-Т».

Специалисты крупной организации, много лет эксплуатирующей «Центр-Т», во время обсуждения очередного набора пожеланий, которые нам было бы хорошо реализовать в очередной версии, высказали мнение, что было бы замечательно совсем отказаться от аппаратных терминалов, которые в этом решении работают только как переходник для периферии и источник проблем с совместимостью. Сделайте «кубик», посоветовали нам, к которому будет подключаться периферия и ШИПКА (как носитель ПО «Центр-Т», хранилище ключей и идентификатор пользователя в «Аккорде» на терминальном сервере). Идея особенно нравилась безопасникам тем, что рабочее место становилось при таком решении персональным устройством, за которое отвечает пользователь, то есть требования к организационным мерам защиты информации могут быть выполнены ощутимо проще.

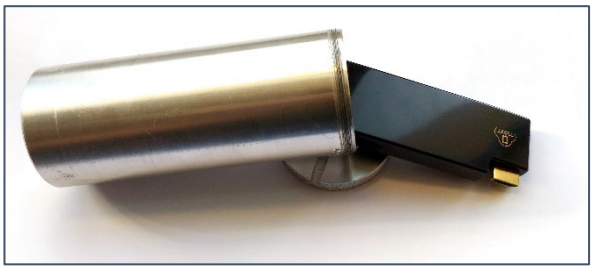
Мы провели параллель с СВМиКД (так как получался очевидный хаб) и назвали этот будущий кубик «очМУХР» («Очень маленький универсальный хаб «Рассвет»). Разумеется, этот «кубик» должен был или сам стать маленьким терминалом (как минимум, ему понадобилась бы оперативная память и сеть), или должен был измениться носитель ПО «Центр-Т», так как у ШИПКИ ни собственной сети, ни собственной оперативной памяти также не было.

В это же время мы занимались разработкой микрокомпьютеров Новой гарвардской архитектуры, семейства МКТ – естественно, такой компьютер, в формате стика, стал очевидным кандидатом на роль будущего очМУХРА.

Одной из проблем, которую мы ощущали в идее микрокомпьютера в форме стика – была именно необходимость подключения к нему всего разнообразия периферии, превращавшая изящное решение в какого-то ежа (из которого все торчит во все стороны). И задумка с «кубиком» оказалось прекрасным решением – из нее вырос форм-фактор компьютеров «МКТ-card»: док-станция, стационарно

размещаемая на столе, к которой подключается периферия, и отчуждаемый мобильный компьютер – персональное защищенное устройство.

Затем, в развитие идей упрощения организационных мер, заказчик захотел иметь возможность закрывать эти отчуждаемые компьютеры в пенал для ключей, опечатывать и сдавать в шкаф на посту охраны, и появился «МКТ-card long» – точно такой же только его физические размеры позволяли пометить его в пенал [17].



6.3.2. Решение «два экрана»

В одной крупной территориально распределенной организации был запрещен Интернет на рабочих местах.

Электронная почта была организована через внутреннюю сеть, а использовать, например, браузер можно было на отдельных компьютерах, не подключенных ко внутренней сети и специально отведенных для работы с Интернетом. Это позволяло получать из сети данные через специально организованные санитарные зоны и с применением разных других полуорганизационных мер. Получить их можно было только после того, как их безопасность была подтверждена (ошибочно или нет – другой вопрос). Это было решение и вполне безопасное, и неудобное для пользователей.

Время от времени эта организация возвращается к поиску других вариантов, но любой другой способ избежать негативных влияний Интернета, кроме его полного запрета в корпоративной сети, как правильно тоже оказывается не вполне эффективным. В лучшем случае (при наличии ощутимых инвестиций в такие технические средства, как межсетевые экраны и системы обнаружения вторжений, значительных усилий по принятию организационных мер, систематически

обновляемых антивирусов, желательно нескольких разных, а также профессиональных и ответственных сотрудников, все это тщательно настраивающих и ответственных пользователей, не старающихся все это обойти) удается добиться того, что инциденты, связанные с атаками из сети Интернет становятся редки и не приносят значительного урона (и это очень хороший результат).

Однажды с предложением продумать какой-то качественно новый подход к этому вопросу, который сочетал бы в себе плюсы полной изоляции корпоративной сети от сети Интернет с плюсами наличия Интернета на каждом рабочем месте, и в то же время лишенный минусов обоих подходов, обратились и к нам.

В поисках подхода к реализации такого решения мы обратились к истории.

На заре своего развития интернет был безопасным. Это достигалось не за счет того, что были установлены мощные межсетевые экраны и серьезное антивирусное ПО. Все проще — Интернет просто технологически не предоставлял возможности загрузить вирус, выполнить вредоносный код, или как-то обмануть пользователя. Но Интернет развивался, «осваивая» все больше и больше различных технологий — javascript, Java-апплеты, свободная возможность скачивать файлы.

Идеально было бы вернуться в светлое прошлое, когда все эти технологии еще только зарождались и не могли нанести вред пользователям, но так, чтобы Интернет не потерял свой привычный вид.

Слово «вид», на наш взгляд ключевое. Визуальная информация — это 90% всей воспринимаемой человеком информации. Что если ею и ограничиться? Тогда задачу защиты пользователя от всех возможных угроз можно свести к защите передачи изображений. Изображение не может нести с собой угрозу безопасности (на самом деле может, но в рамках решаемой задачи этим весьма специфическим случаем можно и пренебречь). Значит, достаточно организовать пользователю

безопасный канал, по которому он может получать изображения — и безопасный Интернет у нас в кармане. Практически, серебряная пуля.

В качестве прикладной реализации описанного подхода мы предложили технологию одновременной изолированной работы пользователя с корпоративной сетью и сетью Интернет на одном рабочем месте в рамках двух независимых терминальных сессий с их одновременным отображением на экране одного монитора в разных «окнах». Естественно, чтобы пользователям было удобно, при работе в обеих сессиях они должны были иметь возможность использовать один и тот же комплект элементов управления и отображения (клавиатура, мышь, монитор, принтер).

Взаимовлияние между корпоративной сетью и сетью Интернет в предложенной технологии исключено с 1 по 4 уровень модели ISO/OSI.

Это было основным, системообразующим требованием. Однако для комфортного и «бесшовного» введения технологии в систему, которая уже работает, и ее работа не должна быть нарушена, необходимо выполнение еще и ряда дополнительных требований:

1) активные компоненты системы, обеспечивающие работу в режиме двух терминальных сессий, должны вести журналы событий,

2) события должны фиксироваться в аппаратном журнале, память которого доступна только для операции дополнения (то есть события нельзя удалить или перезаписать),

3) должны быть предусмотрены программные средства обработки журналов событий и описан порядок их использования,

4) должна быть предусмотрена возможность отправки оперативных оповещений Администратору ИБ в случае наступления критичных с точки зрения безопасности событий,

5) порядок работы пользователя в режиме двух терминальных сессий не должен требовать специальных навыков и знаний или оказывать негативное влияние на производительность его труда.

Корпоративная сеть, для которой предлагалось решение, представляла собой терминальную систему, в которой пользователь

работает с терминальным сервером по RDP и ICA. Терминальные серверы и терминальные клиенты, а также их взаимодействие — защищены надлежащим образом, этот аспект не будет рассматриваться, чтобы не запутывать описание решения.

На терминальном сервере — будем называть его «функциональный терминальный сервер» (ФТС) — нет ни браузера, ни каких-либо других средств и инструментов работы с сетью Интернет.

Предложение заключалось в том, чтобы к той же локальной сети, через которую взаимодействуют терминальные клиенты с ФТС, подключить другой терминальный сервер, но не напрямую, а через специальный фильтр, как показано на рисунке 6.3.

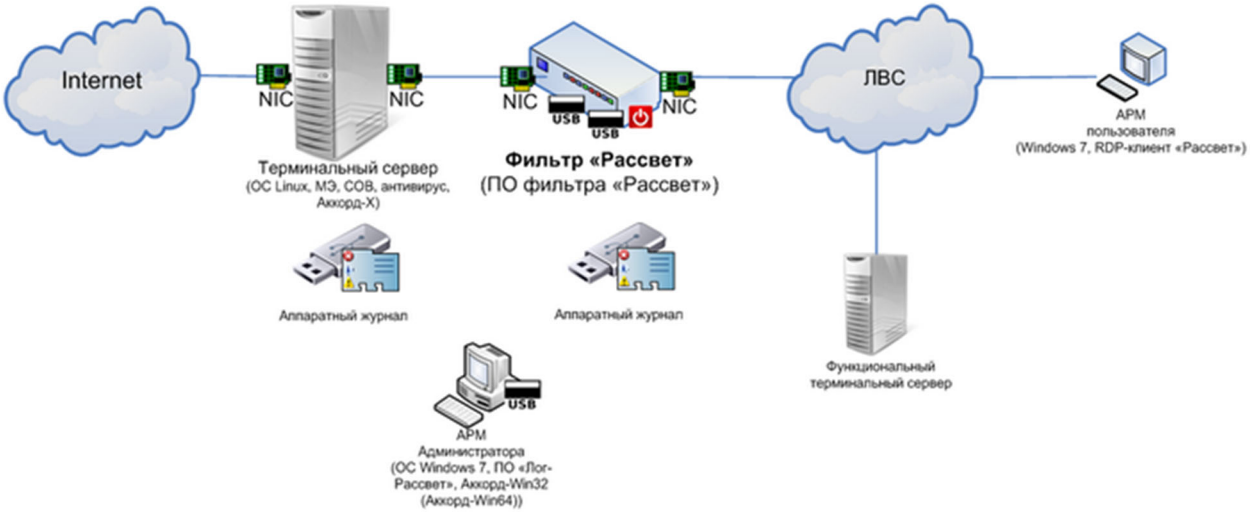


Рисунок 6.3. Структурная схема комплекса технических средств решения

Это терминальный сервер (далее — ТС) под управлением ОС Linux, имеющий соединение с сетью Интернет. На терминальном сервере опубликован браузер.

На рисунке в качестве терминального клиента показана ПЭВМ с ОС Windows, однако с тем же успехом может быть тонкий клиент под управлением ОС Linux, в том числе, загружаемой по сети (или локально с отчуждаемого устройства).

Обмен данными между ТС и сетью Интернет производится в штатном порядке, без ограничений и/или изменений. Для соединения с Интернет у ТС предусмотрена отдельная сетевая карта.

На терминальный сервер установлен полный комплект средств защиты информации: средства защиты от воздействия вредоносных кодов, средство обнаружения вторжений, межсетевой экран, ПАК СЗИ НСД «Аккорд-Х».

Через отдельный сетевой интерфейс (вторую сетевую карту) ТС взаимодействует с аппаратным комплексом с функциональностью фильтра (Фильтр «Рассвет»).

Фильтр также оборудован двумя сетевыми картами. Через одну из них Фильтр взаимодействует с ТС. В фильтр передаются все команды и данные от ТС, которые не были заблокированы МЭ, СОВ, СЗ ВВК или ПАК СЗИ НСД «Аккорд-Х».

От фильтра на ТС передаются только нажатия клавиш клавиатуры и движение мыши. Все команды и данные, не являющиеся нажатиями клавиш клавиатуры и/или движениями мыши, не передаются на ТС, а попытка их передачи фиксируется в журнале событий.

Через другой сетевой интерфейс (вторую сетевую карту) фильтр взаимодействует с ЛВС предприятия. От фильтра в ЛВС передаются только изображения рабочего стола. Все команды и данные, не являющиеся изображениями рабочего стола, не передаются в ЛВС, а попытка их передачи фиксируется в журнале событий.

От ЛВС в фильтр передаются все данные и команды без ограничений.

Взаимодействие пользователя с ЛВС производится через установленный на АРМ пользователя модифицированный RDP-клиент (далее RDP-клиент «Рассвет»). Для пользователя взаимодействие происходит обычным порядком, без изменений, все изменения взаимодействия от него скрыты. Он работает параллельно в окне браузера и в окне сессии с ФТС.

Схематично взаимодействие компонентов системы показано на рисунке 6.4.

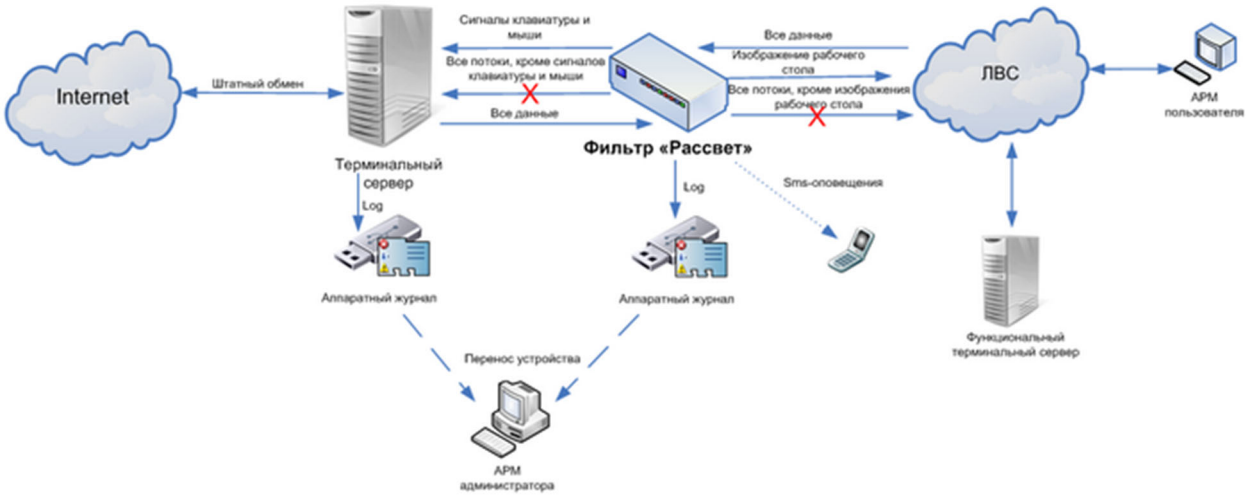


Рисунок 6.4. Функциональная схема решения

Фильтр «Рассвет»

Очевидно, что главной активной частью решения является Фильтр, поэтому на его описании остановимся подробнее.

Фильтр представляет собой устройство серверного типа с двумя сетевыми картами, минимум двумя USB-портами для подключения аппаратных неперезаписываемых журналов и кнопкой выключения коммутации на внешней стороне корпуса.

Эта кнопка необходима для того, чтобы в случае возникновения нештатной ситуации администратор информационной безопасности (АИБ) (или иное уполномоченное лицо) мог физически, одним действием отключить сетевое взаимодействие корпоративной сети и сети Интернет.

Наличие кнопки отключения на внешней стороне корпуса детерминирует размещение фильтра в помещение, для которого обеспечен контроль доступа и приняты меры, не допускающие несанкционированного нажатия этой кнопки.

В состав фильтра входит предустановленное ПО «Фильтр-Рассвет», обеспечивающее фильтрацию RDP таким образом, чтобы от ЛВС на ТС передавались только нажатия клавиш клавиатуры и движения мыши, а от ТС в ЛВС передавались только изображения рабочего стола. Любые

другие команды и/или данные блокируются, а информация об этом заносится в журнал событий Фильтра.

Дополнительно данное ПО реализует сервис оперативных оповещений (например, в форме sms-оповещений) о событиях безопасности на телефон АИБ с целью обеспечения возможности безотлагательного принятия мер в случае возникновения необходимости. Перечень событий и способ оповещения настраивается. Одним из событий, о котором настроено оповещение по умолчанию — заполнение журнала на N % (количество процентов заполнения — настраивается).

Также ПО реализует порядок фиксации событий фильтра таким образом, чтобы события сохранялись только на аппаратный неперезаписываемый журнал.

Работа с журналами

Все события, трактуемые любым из средств, установленных на ТС, как события безопасности, фиксируются в журналах событий. Настройками ПАК СЗИ НСД «Аккорд-Х» обеспечен режим, при котором журналы событий записываются не на жесткий диск или иное хранилище, а только на подключенный к ТС аппаратный неперезаписываемый журнал (ПАЖ, о котором вы читали в предыдущей главе и в начале этой).

Все события Фильтра «Рассвет» также записываются не на жесткий диск или иное хранилище, а только на подключенный к ТС аппаратный неперезаписываемый журнал. Это обеспечивается настройками ПО «Фильтр-Рассвет».

Для чтения и анализа журналов, записанных на аппаратный неперезаписываемый журнал на ТС или Фильтре, АИБ (или иное лицо, в обязанности которого входит анализ журналов) использует АРМ, на котором установлено специальное ПО «log-Рассвет».

Рекомендуется, чтобы в качестве разрешенных для работы с ПАЖ регистрировались на запись – только сами ТС и/или Фильтр «Рассвет»,

а на чтение – только специальный АРМ работы с журналами, и больше никакие.

Дополнительно, на случай возникновения событий, требующих незамедлительной реакции от АИБ, в системе предусмотрено оповещение АИБа о событиях Фильтра и/или ТС.

С помощью ПО работы с журналами на ТС и Фильтре реализуется порядок, который предусматривает переход к сохранению событий на последнее подключенное устройство. Когда необходимо обработать данные с одного аппаратного неперезаписываемого журнала, АИБ подключает к свободному USB-порту второе устройство, и записи о событиях автоматически начинают сохраняться на него, а первое устройство можно отключать и переносить на АРМ работы с журналами для анализа.

Для реализации такого порядка работы на ТС и Фильтре должно быть доступно не менее 2-х USB-портов.

RDP-клиент «Рассвет»

Это модифицированный RDP-клиент, имеющий только 3 функции:

1. передача позиции курсора мыши,
2. передача нажатий клавиш клавиатуры,
3. прием и визуализация изображения рабочего стола.

Он лишен возможности расширения функций за рамки перечисленных.

Такая система позволяет построить технологию работы с двумя терминальными сессиями с обеспечением ключевых требований:

- не снижается защищенность работы пользователей с корпоративной сетью (в описанной модели — с защищенным ФТС),
- повышается комфортность работы пользователей,
- предоставлена возможность аудита и анализа инцидентов.

Таким образом, защищенность решения обеспечивается изолированностью сессий друг от друга на уровнях модели ISO/OSI с 1 по 4 включительно (1 уровень — физический — 2 отдельные сетевые

карты у ТС и фильтра, 2-й уровень — канальный — преобразование Ethernet-пакетов, 3-й уровень — сетевой — использование МЭ, 4-й уровень — транспортный — фильтр протокола RDP).

Пользователь работает в привычном режиме и при этом без необходимости переходить на выделенное рабочее место для работы с сетью Интернет.

На первый взгляд, решение выглядит несколько экзотически. Однако оно в полной мере воплощает мечту о «старом добром безопасном Интернете», сохраняющим в то же время все столь дорогие пользователю возможности. В зависимости от выбранной политики можно так настроить среду работы пользователя с Интернетом в описанной системе, чтобы создать видимость работы вообще без каких-то особых ограничений. Например, пользователь не сможет «прицепить» к веб-форме файл, находящийся на ФТС, однако, если возможность прицеплять файлы действительно нужна пользователю, то можно позволить ему создавать файлы на ТС и прицеплять их, куда необходимо. То же со скачиванием файла — он не сможет скачать его на свою флешку или на ФТС, но если владелец системы сочтет такую возможность уместной и полезной для работы, пользователю может быть позволено скачивать файлы на ТС. Это никак не нарушит безопасность функциональной системы, так как все эти файлы будут всегда оставаться за Фильтром, а на терминальный клиент будут передаваться только изображения. Пользователь будет его видеть, а этого ему более чем достаточно.

К сожалению, решение так и осталось на уровне макета, договор на его реализацию не был заключен.

6.3.3. USB Guard

Особенность организации процесса закупок на момент написания этого раздела такова, что в качестве необходимого требования в

техническое задание может быть вписано практически что-угодно, если это представляется потом возможном оправдать, если будет эскалировано разбирательство об ограничении конкуренции. Поэтому большую ценность имеют с одной стороны, редкие или уникальные функции, а с другой – способность разработчика быстро добавить такую редкую функцию в свой продукт, чтобы обеспечить ему возможность поучаствовать в конкуренции.

Однако, такое включение налету в продукт новых функций имеет и оборотную сторону – необходимость пересертификации продукта, что и долго, и дорого. Нежелание заниматься сертификацией функций, которые не относятся к выполнению каких-либо требований регулятора, а являются просто полезными, привело к идее создания функциональных модулей UEFI, например, USB Guard. Задачу он решает следующую.

В ряде операционных систем имеются встроенные инструменты безопасности такие, как, например, функция управления USB-портами. «Управление» в отношении этого механизма – некоторое преувеличение, в общем случае, у него есть два состояния:

1) он включен, и тогда все USB-порты компьютера работают в режиме «только чтение»

2) он отключен, тогда все USB-порты работают штатным образом.

Как правило, такого «грубого» управления достаточно, так как используются эти механизмы для запрета записи данных на любые USB-устройства, а при необходимости более тонкой настройки правил используются не встроенные, а наложенные средства (средства разграничения доступа, DLP-системы, защищенные съемные носители информации и т. д.).

Однако, как и любая функция или настройка, реализованная в ОС, функция контроля USB-портов может быть несанкционированно отключена (специально, или из-за системного сбоя, или действия вредоносных программ, например). Значит, для того чтобы

использование такого механизма имело смысл, в системе должно быть какое-то средство, которое контролировало бы, включен ли механизм, и сигнализировало, если отключен.

Важно отметить одну особенность – эта задача отличается от контроля целостности. Не достаточно убедиться, что механизм не удален и не изменен, нужно убедиться, что он *включен*.

Такое средство, несомненно, должно быть запущено на исполнение раньше, чем контролируемый механизм (т.е. до загрузки ОС). Именно таким средством и является USB Guard. А поскольку к такого рода функциональности не предъявляются требования со стороны регуляторов, он не подлежит сертификации, но включен в Реестр отечественного ПО.

Приведенные в этой главе истории призваны показать, что новые решения могут быть придуманы практически любым путем, главное – и, в общем, практически единственное, что для этого нужно – это все время (без преувеличения) об этом думать, и во всем видеть причину и повод придумать какую-нибудь штуку для защиты информации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Батраков А. Ю., Конявская С. В., Счастный Д. Ю.* Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014, бюл. №31.
2. *Батраков А. Ю.* Обзор защищенных ключевых хранилищ // Комплексная защита информации. Безопасность информационных технологий. Материалы XVII Международной конференции 15–18 мая 2012 года, Суздаль (Россия). М., 2012. С. 37–38.
3. *Ладынская Ю. П., Батраков А. Ю.* Хранение данных СКЗИ: выбор носителя // Информационная безопасность. Материалы XIII Международной конференции. Таганрог 2013. Часть. 1. С. 129–134.
4. *Бирюков К. А.* Средства безопасного хранения ключей // Безопасность информационных технологий. М., 2013. № 3. С. 50–53.
5. *Кравец В. В.* Идеальный токен // Комплексная защита информации. Материалы XX научно-практической конференции. Минск, 19–21 мая 2015 г. Минск: РИВШ, 2015. С. 114–115.
6. *Счастный Д. Ю.* К вопросу о защите от Intel Management Engine // Вопросы защиты информации. М., 2018. № 2 (121). С. 37–40.
7. *Кравец В. В.* Клавиатура — устройство вывода? [Электронный ресурс]. URL:https://habrahabr.ru/company/pm/blog/352868/ (дата обращения: 08.04.2018).
8. *Счастный Д. Ю.* К вопросу защиты авторских прав // Информационные технологии управления в социально-экономических системах. М., 2008. С. 156–159.
9. Мобильный носитель лицензий // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/storage/data/mnl/ (дата обращения: 23.08.2021).
10. МНЛ. Документация // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/support/docs/sluzhebnye-nositeli/mnl-doc/ (дата обращения: 23.08.2021).
11. МНЛ. Подборка публикаций. // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/library/?year_from=&year_to=&tags=%D0%A8%D0%98%D0%9F%D0%9A%D0%90&authors=&type_pub= (дата обращения: 23.08.2021).
12. *Конявский В. А.* Смысл и безопасность // Information Security/Информационная безопасность. М., 2020. № 5. С. 54–56.

13. ПАК «Центр-Т» // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/management/PAKTSENTRT/

14. Специальные носители ПО «Центр-Т» // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/storage/compute/center-t/ (дата обращения: 23.08.2021).

15. Центр-Т. Документация // https://www.okbsapr.ru/support/docs/sluzhebnye-nositeli/tsentr-t-doc/

16. Счастный Д. Ю., Бажитов И. А., Конявская С. В. Способ защиты от несанкционированного доступа к информации, хранимой в компьютерных системах. Патент на изобретение № 2470349. Опубликовано 20.12.2012, бюл. № 35.

17. MKT-card и MKT-card long // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/newharvard/istoriya-nga/mkt-card-long/ (дата обращения: 23.08.2021).

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Для проверки усвоения представленного материала предлагаем ответить на несколько вопросов и решить практические задачи. Не на все вопросы ответы можно найти в тексте напрямую. Но если вы совершенно не представляете себе ответ, значит, какую-то часть материала усвоить не удалось и следует вернуться к нужному разделу.

ВОПРОСЫ

1. В чем Вы видите следствия из различий между понятиями «атака» и «угроза»? Какое следствие на Ваш взгляд самое важное и почему?

2. В чем различие между понятиями «защищенность» и «безопасность»?

3. Какие меры защиты необходимы для доверенного старта СВТ?

4. Почему нельзя выполнять процедуры контроля целостности до загрузки ОС для всех подлежащих контролю ресурсов?

5. Какие меры защиты необходимо применять для предотвращения несанкционированной модификации функционального ПО?

6. В каких случаях невозможно выполнение процедур идентификации/аутентификации до загрузки ОС?

7. Как можно исключить нежелательное взаимное влияние процессов в ОС?

8. Выполнение каких процедур требуется для блокирования атак на каналы связи?

9. Назовите известные вам варианты реализаций загрузки ПО на клиентские СВТ в системах удаленного доступа.

10. Как удостовериться в том, что на рабочем месте установлено только необходимое для работы пользователей ПО?

ПРАКТИЧЕСКИЕ ЗАДАЧИ

Для решения практических задач может быть целесообразно обращаться к эксплуатационной документации на продукты, она доступна на официальном сайте разработчика.

1. Как вы считаете, возможны ли ситуации, когда для контроля внешних носителей требуется одновременное использование СЗИ, позволяющих:

- определить, с какими носителями может работать пользователь на этом компьютере;

- определить, на каких компьютерах пользователь может работать с этим носителем?

Если да, то приведите примеры таких ситуаций. Если нет, то объясните, почему.

2. В каких случаях может быть полезным использование:

- только «Секрета Фирмы»;

- только «Секрета Особого Назначения»?

Возможно ли совместное использование «Секретов» разного типа?

3. Когда может оказаться полезным наличие двух ОС на СВТ в защищенном исполнении? Приведите примеры, когда две ОС = два контура, и когда ≠.

4. Приведите примеры данных, для хранения которых удобно использовать «ПАЖ». Как в этих случаях следует настроить политики использования устройства?

5. Чем, по Вашему мнению, обусловлено разделение функциональных обязанностей между ролями «ПАЖ»? На какую роль Вы бы назначили администратора системы, а на какую – администратора информационной безопасности? Кто может быть «пользователем» ПАЖ? Каким образом можно реализовать политику «четырех глаз» (когда какая-либо функция может выполняться пользователем определенной роли только в присутствии другого сотрудника) для функции установки настроек доступа ПАЖ? А для выполнения просмотра записанных на ПАЖ данных?

6. В каких случаях может потребоваться использование функции временного отключения ограничительных политик использования СН в «Секрете Руководителя», а в каких наоборот – временного *включения* этих политик?

Возможно ли с Вашей точки зрения обнаружить манипуляции с системным временем в журнале обыкновенного «Секрета Особого Назначения», и для чего такие манипуляции могут понадобиться недобросовестному пользователю?

Если Вам было интересно подумать над этими вопросами, книга удалась.

Спасибо за внимание!

Конявская-Счастная Светлана Валерьевна

Начала технической защиты информации

Подписано в печать: 20.03.2025
Формат 60×90/16. Печать цифровая.
Бумага офсетная №1.
Усл. печатных л.: 21
Усл. авт. л.: 13
Тираж 500 экз.
Тип. заказ № 734205

ISBN 978-5-6053673-0-7

Типография «Вишневый пирог»
115114, Москва, 2-й Кожевнический пер., 12
Тел: +7 495 994 49 94