Защита сетевой коммуникации: «зоопарк» с человеческим лицом

Статья посвящена одному из «узких мест», в которых могут возникать сложности при приведении систем в соответствие требованиям к критическим информационным инфраструктурам (КИИ) или, например, к осуществлению переводов денежных средств. Эти задачи влекут за собой изменение уже функционирующих систем, что повышает риски, связанные с «зоопарком» технических средств. Этих рисков можно избежать, если использовать средства защиты информации, адаптирующиеся к разным типам средств вычислительной техники.

Ключевые слова: АСУ ТП, КИИ, защита сетевого взаимодействия, коммутационные интерфейсы

En **Protection of Network Communication: «Zoo» with a Human Face**

S. V. Konyavskaya,
PhD (Philology)
OKB SAPR, MIPT
cd@okbsapr.ru

The article is devoted to one of the» bottlenecks «in which there may be difficulties in bringing systems in line with the requirements for critical information infrastructures or, for example, to the implementation of money transfers. These tasks entail changing already functioning systems, which increases the risks associated with the «zoo» of technical means. These risks can be avoided if you use information security tools that adapt to different types of computer equipment.

Keywords: automated process control system, critical information infrastructure, network communication protection, switching interfaces

Светлана Валерьевна Конявская,
кандидат филологических наук
ЗАО «ОКБ САПР», МФТИ
cd@okbsapr.ru

Периодическая смена терминологии в отношении инфраструктуры информационного взаимодействия очень полезна. Она заставляет посмотреть на многие вещи свежим взглядом, актуализирует их (хотя при этом по существу может ничего и не меняться). Значение этого «свежего взгляда» трудно преувеличить, поэтому ворчание о том, что все новое (например, КИИ) – это еще даже не вполне хорошо забытое старое (в значительной части – АСУ ТП), нам кажется напрасным. Безусловно, специалистам важность и исключительность объектов информатизации разных типов понятна, как бы эти объекты ни назывались. Но невозможно не отметить, что новое разделение предмета – выделение частного из знакомого и потому утратившего остроту общего – всегда повышает не только уровень общественного интереса к задачам, но и возможности в части затрачиваемых на решение этих задач ресурсов. Это касается и КИИ, в отношении которой принят федеральный закон и целый комплекс подзаконных актов[1], и финансовых коммуникаций, в отношении которых выпущено и вступило в силу Указание[2] Банка России.

[1] *Федеральный закон от 26 июля 2017 года 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановление Правительства Российской Федерации от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», Приказ ФСТЭК России от 11 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».*

[2] *Указание Банка России от 7 мая 2018 года № 4793-У «О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П „О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств“».*

Возможным негативным следствием из этой оптимистической картины могут стать разного рода «перегибы», которых вполне можно, на наш взгляд, избежать.

Главный «перегиб», которому (а точнее, противодействию которому) посвящена эта статья, имеет вполне понятную природу.

Итак, под влиянием новой нормативной базы предприятие поставлено перед необходимостью изменения организации защиты своих сетевых коммуникаций. Как правило, инфраструктура одного из тех типов, о которых упомянуто выше, связанная с переводом денежных средств или подпадающая под параметры КИИ, – это не вся информационная инфраструктура предприятия, а лишь ее часть, хотя, конечно, и ключевая. Естественно, в связи с этим предпринять усилия к тому, чтобы провести сегментирование и выделить для изменений *минимально* необходимую часть системы.

Желание минимизировать изменения и не трогать то, что «и так работает», глубоко понятно каждому. Однако эта игра может не стоить свеч в том случае, когда *обязательно* подлежит изменению именно *наиболее сложный* в технологическом смысле сегмент инфраструктуры.

И плюсы, и минусы тут очевидны. Плюс: необходимо переоборудовать, в частности, в плане защиты сетевой коммуникации (такова тема номера) не всю систему, а только ее часть. Это дешевле во внедрении, сохраняет хотя бы некоторые инвестиции, требует меньше единовременных трудозатрат на переоборудование и настройку. Минус: возникает (или умножается) «зоопарк» применяемых средств защиты. Это умножает проблемы совместимости с функциональным ПО, трудозатраты на сопровождение, повышает требования к квалификации персонала и/или его численности, усложняет проект системы, наконец.

Таков взгляд на ситуацию с той точки зрения, при которой средство защиты информации является «вещью в себе», а поддается (и подлежит) адаптации защищаемая система, что не совсем логично. Предполагаю, что здесь может возникнуть возражение: мол, выбирают все же СЗИ для системы, а не наоборот. Это, безусловно, так, и лишь в редких случаях (хотя известны и такие) доходит дело до изменения инфраструктуры под нужды, например, конкретного СКЗИ. Однако использование в различных сегментах системы разных СЗИ одной и той же функциональности – это явление того же порядка: компромисс, при котором система подстраивается под СЗИ. Уже на стадии проектирования она становится «зоопарком» просто потому, что СЗИ не способны адаптироваться ко всем типам применяющихся в ней технических средств.

Я бы не рискнула эскалировать вопрос именно под таким углом, если бы сама не имела отношения к компании-разработчику СЗИ, являясь таким образом и адресатом собственной критики.

Мы попробовали изменить привычное положение вещей, и оказалось, что это вполне возможно. Рассмотрим контуры такого решения, не углубляясь в детали.

К основным особенностям, которые существенно влияют на обеспечение защиты сетевой коммуникации, в частности, при осуществлении переводов денежных средств, относятся следующие:

- жесткие требования к времени и порядку выполнения автоматизированных функций;
- наличие разнородных, территориально и пространственно распределенных элементов (мобильных и стационарных) с сочетанием разнообразных информационных технологий (банкоматы, терминалы оплаты, информационные киоски, фронт-офисы, системы ДБО, подвижные составы, станционное оборудование и пр.);
- неприемлемость отключения систем для проведения мероприятий по обеспечению безопасности информации, а также другие требования аналогичного плана.

При этом КИИ в «классическом» смысле и особенно в части АСУ ТП характеризует также следующее.

- основной защищаемой информацией в АСУ ТП является технологическая (обеспечивающая управление технологическими или чувствительно важными процессами) информация, программно-техническая (программы системного и прикладного характера, обеспечивающие функционирование АСУ ТП), командная (управляющая) и измерительная;
- опасность последствий вывода из строя и (или) нарушения функционирования АСУ ТП (риски для благосостояния клиентов – это тоже крайне негативный результат нарушения функционирования системы, однако опасности для жизни и здоровья объяснимо стоят в этом смысле особняком).

Структурно в таких системах может быть выделена совокупность подконтрольных объектов (ПКО) и совокупность каналов связи, по которым передаются информационные и управляющие сигналы. Все информационные и управляющие сигналы, сформированные ПКО, должны защищаться на месте выработки, доставляться в защищенном виде и расшифровываться перед обработкой (использованием) другим ПКО. Это требует внедрения в уже *функционирующие* инфраструктуры средств защиты, которые должны обеспечивать:

- криптографическую защиту информации о состоянии ПКО и управляющих сигналов для ИС;
- информационное взаимодействие с ПКО (USB, Ethernet и др.);
- возможность использования стандартных цифровых каналов (BlueTooth, Wi-Fi и др.);
- информационное взаимодействие с каналообразующей аппаратурой (RS232, RS435 и др.).

Очевидно, что большая часть имеющихся в настоящее время на рынке средств защиты информации при их внедрении потребуют, в лучшем случае, некоторой доработки отдельных ПКО, а в худшем – изменения функциональной структуры и замены ПКО на совместимые со средствами защиты. Хорошо понятно, почему это так: если сделать аппаратную базу СЗИ такой, чтобы она поддерживала все возможные интерфейсы во всех комбинациях, получится самое большое, дорогое, сложно настраиваемое и ненадежно работающее СЗИ в мире.

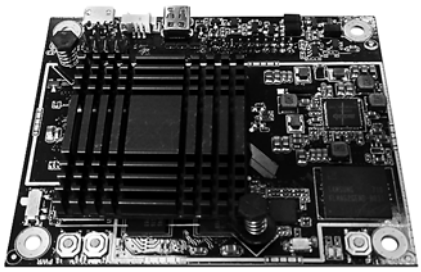

Рис. 1. ***Микрокомпьютер «m-TrusT»***

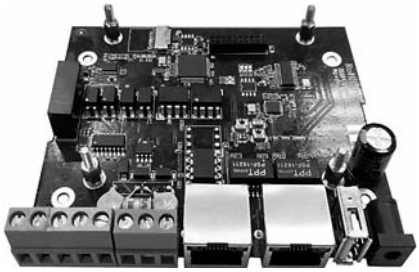

Рис. 2. ***Интерфейсная плата***

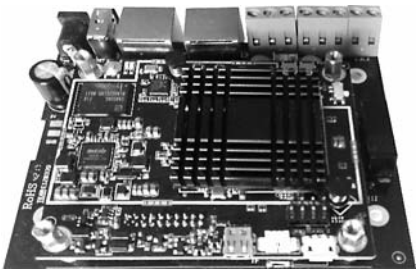

Рис. 3. ***Интерфейсная плата с подключенным «m-TrusT»***

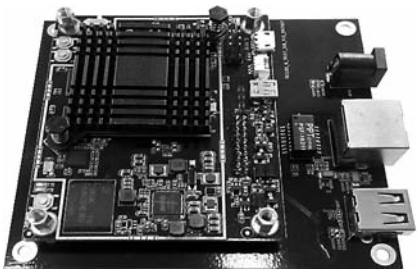

Рис. 4. ***Интерфейсная плата («облегченный» вариант)***

Все три варианта (доработка ПКО, замена ПКО, использование «огромного» СЗИ) связаны с существенными финансовыми и временными затратами, вплоть до приостановки функционирования, что зачастую неприемлемо. Альтернативным вариантом является гибкая адаптация СЗИ под различные типы оборудования самого различного назначения. Это вариант очевидно менее хлопотный для эксплуатирующей (внедряющей) организации, так как адаптация СЗИ выполняется не ими, а вендорами СЗИ.

Примеров таких СЗИ пока не много, но они есть. Для защиты сетевой коммуникации в инфраструктуре, включающей то или иное оборудование, взаимодействующее разнообразным образом по различным каналам, можно использовать интеграционную платформу «МК-И».

Эта интеграционная платформа представляет собой комплекс распределенных одноплатных микрокомпьютеров «m-TrusT» Новой гарвардской архитектуры, обладающих «вирусным иммунитетом», и интерфейсных плат для них. Каждый микрокомпьютер «m-TrusT» является точкой сбора информационных и/или управляющих сигналов от ПКО, их шифрования для передачи по каналам связи, а также приема зашифрованных сигналов из каналов связи и их расшифровкой.

Типовые характеристики микрокомпьютеров:

- габаритные размеры: 65×80 мм;
- процессор: Quad-core ARM Cortex-A17, up to 1,8 GHz;
- ОЗУ: 2 Гбайта DDR3;
- ПЗУ: 16 Гбайт NAND-flash;
- microUSB;
- microHDMI.

Общий вид микрокомпьютера «m-TrusT» представлен на рис. 1.

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 корректного подключения к тому или иному конкретному ПКО и каналообразующей аппаратуре различных типов.

Наличие собственной операционной системы и вычислительных ресурсов позволяет обеспечить необходимую производительность и высокий уровень защищенности. Особенностями «m-TrusT» является наличие датчика случайных чисел и размещение ПО в памяти с физически устанавливаемым доступом *read only* (только чтение), что исключает вредоносное воздействие на ПО и обеспечивает неизменность среды функционирования средств криптографической защиты информации. Встроенные средства защиты информации имеют сертификаты соответствия ФСБ России и ФСТЭК России.

Итак, коммутировать микрокомпьютер «m-TrusT» в «разрыв» между ПКО различного назначения и каналом связи позволяет интерфейсная плата. Как уже упоминалось, разнообразие оборудования, взаимодействующего по сети (ПК, подвижной состав, станционное оборудование, банкомат, терминал оплаты и пр.), является ключевой характеристикой инфраструктуры (будь то КИИ, АСУ ТП или информационная система финансовой организации), 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 показано на рис. 2:

Интерфейсная плата № 1:

- габаритные размеры: 90×105 мм;
- соединитель типа «розетка» 87758-2016 MOLEX;
- разъем USB Type A;
- разъем Ethernet;
- разъем питания от источника постоянного напряжения 5 В.

Интерфейсная плата № 2:

- габаритные размеры 90×110 мм;
- соединитель типа «розетка» 87758-2016 MOLEX;
- USB-хаб;
- разъем USB Type A;
- 2 разъема Ethernet;
- разъем RS-232, подключенный через преобразователь USB-RS-232;
- разъем RS-485, подключенный через преобразователь USB-RS-485;
- разъем для карты micro-SD;
- разъем питания от источника постоянного напряжения 5 В.

На рис. 3 изображен «m-TrusT», подключенный к интерфейсной плате.

На рис. 4 показан другой вариант интерфейсной платы с меньшим количеством интерфейсных разъемов:

- габаритные размеры: 90×105 мм;
- соединитель типа «розетка» 87758-2016 MOLEX;
- разъем USB Type A;
- разъем Ethernet;
- разъем питания от источника постоянного напряжения 5 В.

Возможна разработка интерфейсных плат для других типов разъемов. Учитывая уже имеющийся опыт их внедрения на транспорте,

мы уверенно говорим о том, что эта задача решается с положительным результатом в разумные сроки.

Разумеется, не всегда уместно использование СЗИ именно такого форм-фактора. Как правило, оборудование, обрабатывающее данные с ПКО, представляет собой обычные серверы в серверных стойках, размещенные стационарно и не имеющие каких-либо значительных конструктивных особенностей. И для этого элемента инфраструктуры финансовой организации больше подойдет исполнение «в стойку» (рис. 5).

Рис. 5. ***Стоечное исполнение того же самого СЗИ***

При этом технически – не считая корпуса – это одно и то же оборудование, оно работает, эксплуатируется и обслуживается одинаково.

Таким образом, применение микрокомпьютеров «m-TrusT» для защиты сетевого взаимодействия финансовой организации, различных специфических КИИ и АСУ ТП позволит построить подсистему защиты для разнообразного оборудования с использованием одного и того же СЗИ, «подогнанного» под каждый инфраструктурных элемент. Каждый, кто проектировал или внедрял подсистему защиты информации, понимает, насколько это значимо во всем – от обучения эксплуатирующего персонала до проведения ремонтных работ: перекоммутировать интерфейсную плату не требуется, просто заменяется подключенный к ней модуль, то есть операция становится элементарной.

В таких условиях ограничиваться модернизацией исключительно той части инфраструктуры, что подпадает под действие нормативных документов, не имеет смысла. Наоборот, представляется логичным унифицировать защиту сетевого взаимодействия, сократив «зоопарк» технических средств без затрат на адаптацию собственной инфраструктуры. Ведь при появлении возможности без ощутимых издержек и ограничений действительно сделать что-либо лучше по сравнению с текущим положением вещей, никто в здравом уме не станет минимизировать объем изменений, улучшая только самое необходимое. ■

НОВОСТИ

Учебный центр «Информзащита» отпраздновал свой 20-летний юбилей!

В истории Учебного центра «Информзащита» 2 сентября произошло значимое событие – ему исполнилось 20 лет!

Оценивая работу по подготовке и повышению квалификации специалистов в сфере информационной и экономической безопасности, можно с уверенностью сказать – огромный скачок в развитии отрасли в целом стал, с одной стороны, залогом непрерывного роста Учебного центра, а, с другой стороны, был обеспечен и подкреплен теми специалистами, которые получили подготовку в его стенах.

За 20 лет Учебный центр «Информзащита» выпустил более 70 000 слушателей!

В 1998 году Учебный центр «Информзащита» был создан на базе компании НИП «Информзащита» в целях подготовки специалистов к работе с поставляемыми продуктами нескольких компаний, а за последующие 20 лет линейки курсов, разработанные специалистами Центра в содружестве с отечественными и зарубежными вендорами, охватили фактически все сферы информационной безопасности!

Хотелось бы отметить самые важные достижения Учебного центра за 20 лет:

- в арсенале Центра более 200 курсов и комплексных программ обучения по информационной, экономической и кадровой безопасности;
- свидетельства и дипломы Учебного центра признаются регуляторами отрасли: ФСБ России, ФСТЭК России, Минкомсвязи России;
- в 2016 году УЦ «Информзащита» был признан лучшим центром в сфере обучения информационной безопасности;
- Учебный центр является крупнейшим в сфере обучения по информационной, экономической и кадровой безопасности – более 15 штатных преподавателей, 11 учебных аудиторий;
- за 20 лет здесь прошли обучение специалисты 5200 государственных и коммерческих структур 19 государств;
- в Центре реализованы самые передовые учебные технологии, включая возможности дистанционного обучения на базе виртуальных лабораторий и реконфигурируемых стендов.