Доверенные системы как средство противодействия киберугрозам. Базовые понятия

Валерий Конявский, *заведующий кафедрой "Защита информации" МФТИ (Физтех), научный консультант ОКБ САПР*

В статье формулируются определения основных понятий, связанных с доверенностью вычислительных систем, и намечаются основные направления рассуждений об их построении. Доверие к системе в общечеловеческом понимании формируется либо доказательством корректности ее работы в заданных условиях, либо продолжительным положительным опытом ее эксплуатации. Наличие сертификата способствует формированию доверия, но не равносильно ему — и свидетельство тому недавняя критически опасная уязвимость, найденная в одном из широко известных сертифицированных средств защиты от НСД.

Информационные системы развиваются так быстро, что очень немногие из них могут похвастаться продолжительным положительным опытом эксплуатации. Остается понять, при каких верифицируемых условиях систему можно считать доверенной.

Что такое доверенная система

Доверенность – относительно новое понятие, которое при этом, на мой взгляд, носит характер категории. Именно поэтому его часто трактуют слишком расширительно, размывая до спекулятивного уровня. Именно поэтому я попытаюсь выработать конструктивные определения, минимально отличающиеся от определений, принятых в материальном производстве. Полагаю, что такой подход принесет гораздо больше пользы, чем попытки смешать в одном котле технику, ментальность, ошибки ПО и криптографию.

Понятие "доверенная вычислительная система" (ДВС) было введено в [1] в развитие понятия "изолированная программная среда" (ИПС) [2]. Было показано, что ДВС – это система, все узлы которой аутентифицированы, и целостность их установлена. Также было показано, что обеспечение целостности и аутентификация должны выполняться специальным средством, который получил название "резидентный компонент безопасности" (РКБ), для которого были перечислены свойства и доказана лемма о размещении РКБ в ДВС.

Система – это ее элементы и связи между ними. Чтобы точно описать систему, лучше перечислить то, что относится к ней, и то, что к ней не относится. Начнем со второго.

Доверенная и проверенная – разное.

Доверенная и защищенная – разное.

Доверенная и надежная – разное.

Доверенная и устойчивая – разное.

Разное, но не противоположное. И во многом близкое.

Материальное производство

Рассмотрим определения, касающиеся отношений в сфере материального производства.

1. Производство – процесс создания какого-либо продукта.

2. Технология, технологический процесс – последовательность операций преобразования материалов в продукцию.

3. Технологическая операция – это законченная часть технологического процесса, выполняемая на одном рабочем месте.

Если производство не кустарное, то совершенно необходимы вспомогательные операции.

4. Вспомогательные операции – действия по транспортировке, измерению, маркировке продукции и т.п.

Деятельность осуществляется не в чистом поле. Есть среда выполнения операций. Не на любом рабочем месте можно выполнить любую операцию. Должны быть организованные цепочки оборудования, транспорта, складов и так далее.

5. Производственная среда – совокупность материально-пространственных условий деятельности людей в производственной сфере, складывающаяся из имеющихся в наличии промышленных зданий и сооружений, оборудования, транспорта и др. компонентов.

Информационные технологии

Перейдем теперь к информационным технологиям. На мой взгляд, они не сильно отличаются от технологий в материальном производстве. Можно, конечно, информационной технологией называть совокупность методов, способов и средств обработки информации, как это часто делают, но я смысла в этом не вижу. Есть точные понятия в сфере материального производства, ну и почему бы не пользоваться ими в сфере информационного производства?

Мы возьмем за основу традиционные определения, проверенные временем и опытом и точно описывающие объекты и процессы информационного производства.

6. Информационное производство – производство электронных документов (ЭлД), в смысле [3].

Здесь мы трактуем ЭлД несколько расширительно, но близко к пониманию, что информационные системы могут производить документы, влияющие на отношения в своем секторе действенности, а могут производить спам. Вряд ли стоит говорить о доверенных системах, производящих спам.

Конечно, доверенные системы должны использоваться и в АСУ ТП. В этой зоне наши рассуждения тем более необходимы – так как речь идет о технологии, предназначенной для управления технологией. Управляющие сигналы, конечно, не являются ЭлД в полном смысле, но имеют с ними много общего – в частности то, что управляющие сигналы оказывают влияние на технологические подсистемы, аналогичное тому, которое ЭлД оказывает на свой сектор действенности. Поэтому данное выше определение представляется довольно точным.

7. Информационная технология – последовательность информационных операций преобразования данных в документы.

Как и ранее, принципиальным в определении является слово "последовательность". Очевидно, что изменяя последовательность вычислительных операций, из любых данных можно получить любой результат. Вряд ли такое преобразование можно считать технологией. Видимо, последовательность операций нужно зафиксировать, создать нечто, что в информационной технологии соответствует "технологической карте" в материальном производстве.

Отметим, что такая зафиксированная последовательность очень похожа на то, что мы обычно называем "алгоритм". Но только похожа. Все мы знаем, что алгоритм можно реализовать по-разному. То есть он не фиксирует последовательность операций. А для нас фиксация важна – нужно установить "последовательность", как сказано в определении.

8. Защищенная информационная технология – информационная технология, обладающая свойством сохранять последовательность операций.

9. Среда функционирования ИТ – совокупность аппаратных и программных (технических) средств (узлов обработки, автоматизированных рабочих мест (АРМ), абонентских пунктов (АП) и др.) исполнения информационных операций.

10. Доверенная среда функционирования – взаимодействующая совокупность доверенных узлов обработки данных.

11. Доверенная вычислительная система – система, в которой в доверенной среде функционируют защищенные информационные технологии.

В доверенной системе все должно быть доверенным – показано в [1]. Эту позицию по прошествии ряда лет я хочу уточнить. Сейчас понятно, что 20 лет назад защищенная система воспринималась как локальная или корпоративная. И для корпоративной системы практически всегда это утверждение верно. Но появление открытых систем существенно изменило ситуацию, и нам приходится задуматься о транспортных каналах, влиять на которые мы далеко не всегда можем. Но и здесь есть ассоциации со сферой материального производства.

Транспортная среда

Каналы связи в полном соответствии с определением 4 будем считать вспомогательным элементом, предназначенным для "транспортировки" данных между узлами обработки. Вспомогательные элементы редко бывают доверенными и – поскольку обычно они принадлежат другим собственникам с другими целями – совсем не обязаны быть доверенными.

Как сделать доверенной транспортную среду? Или как ее использовать в доверенной системе без снижения уровня доверия? Как минимум, нужно знать ответ на вопросы "откуда" и "куда", а это значит, что точки подключения к транспорту должны быть аутентифицированы.

Соответственно:

12. Каналы связи в ДВС должны быть аутентифицированы и могут быть защищены.

В перечне наших определений нет только одного – определения доверенного узла обработки. Теперь его проще сформулировать. Узел – локальный и относительно простой. Для уверенности в том, что свои функции узел выполнит правильно, мы должны убедиться в том, что его не подменили, а сам он сохранил свой состав и структуру – то есть он целостный, и проверенное программное обеспечение не изменилось. Ограничимся минимальными требованиями.

13. Доверенный узел обработки – выделенная совокупность аутентифицированных и целостных технических средств с проверенным программным обеспечением.

Как сделать доверенными недоверенные технические средства?

Обеспечить целостность. Обеспечить аутентификацию.

Это и делает РКБ.

Таким образом, каждый элемент ДВС должен включать РКБ.

14. Резидентный компонент безопасности – это встроенный в технические средства вычислительной системы объект, способный контролировать целостность технических средств, включая их аутентификацию (так как не аутентифицированный защитным механизмом объект уж точно не может быть целостным).

Компьютер – дополним аппаратным модулем доверенной загрузки или выберем компьютер, в котором целостность обеспечивается архитектурно [4]. Периферия – подменить мышь, клавиатуру или принтер ничего не стоит. А они – подмененные – вполне могут выполнять функции, не входящие в состав защищенных информационных технологий. Сделать их доверенными, если это актуально, можно, вставив в них небольшой специализированный блок РКБ. Это сделает их активными на этапе аутентификации и защитит систему от подмены.

Отчуждаемые носители – как правило, они пассивны. Значит, невозможно понять, можно с ними работать или нет. Специализированные отчуждаемые носители со встроенным РКБ выпускаются [5] и могут использоваться в составе доверенных систем.

Ключевые характеристики РКБ:

- это устройство памяти с очень высоким уровнем защищенности (его внутреннее программное обеспечение должно быть немодифицируемым),
- примитивное (иначе обеспечение его собственной защищенности эквивалентно задаче защиты компьютера, который он защищает),
- встроенное в контролируемую систему и стартующее до старта основной ОС (иначе его функционирование будет бессмысленным),
- не зависимое от контролируемой системы (функционирующее автономно),
- перестраиваемое (то есть предполагающее функционирование в режиме управления и в пользовательском режиме – режиме контроля).

Доверенные узлы обработки состоят из доверенных элементов. А в магазинах продаются недоверенные. Что же делать? Как из недоверенного СВТ сделать доверенное?

Теперь ответ очевиден – в недоверенное средство нужно внедрить РКБ. Доверенное средство всегда активно – и это важнейший признак.

Еще несколько вопросов остались за бортом. Мы не рассмотрели клиента как источник угроз и блокирование этой угрозы с помощью подхода "One Touch Security", не рассмотрели также доверенность не как постоянную характеристику, а как ограниченную во времени функцию – так называемый "доверенный сеанс связи" – ДСС. Может быть, рассмотрим в дальнейшем. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Литература

1. Конявский В.А. Управление защитой информации на базе СЗИ НСД "Аккорд". М., 1999. – 325 с.

2. Щербаков А.Ю. Хрестоматия специалиста по современной информационной безопасности. Palmarium academic publishing. 2016. – Том 1. – 265 с.

3. Конявский В.А., Гадасин В.А. Основы понимания феномена электронного обмена информацией. Мн., 2004. – 327 с.

4. Конявский В. А. Компьютер с "вирусным иммунитетом" // Информационные ресурсы России. – М., 2015. – №6. – С. 31–34.

5. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. №15