

РЕШЕНИЯ «КОДА БЕЗОПАСНОСТИ» ДЛЯ ВЫПОЛНЕНИЯ НОВЫХ ТРЕБОВАНИЙ ФСТЭК К БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Ширманов А.Е.

ООО «Код Безопасности» (ГК «Информзащита»)

сайт: www.securitycode.ru e-mail: a.shirmanov@securitycode.ru

Введение

Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных", главой 14 Трудового Кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ и постановлением Правительства РФ от 17 ноября 2007 г. № 781 установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных данных собственных работников и сторонних физических лиц, персональные данные которых обрабатываются в организации. В 2008 г. был издан приказ от 13 февраля 2008 года №55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных", а также были утверждены нормативные документы ФСТЭК и ФСБ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

В результате указанных государственных инициатив персональные данные стали, в юридических терминах, видом информации ограниченного доступа, вследствие чего физические лица в России получили всеобъемлющую юридическую защиту своих персональных данных со стороны государства.

Нормативные документы ФСТЭК по защите персональных данных [4-7] фактически сформулировали новые дополнительные технические требования к безопасности информации при ее автоматизированной обработке, расширяющие и дополняющие существующие руководящие документы по безопасности автоматизированных систем. Были добавлены требования по антивирусной защите, контролю сетевого доступа к конфиденциальной информации внутри одного сегмента сети, защите от программно-математических воздействий, уточнены требования по применению средств межсетевого экранирования и средств криптографической защиты информации.

В указанных методических рекомендациях ФСТЭК были подробно сформулированы типовые модели угроз с методикой определения актуальности угроз и виды нарушителей в информационных системах персональных данных. Это, в свою очередь, позволило сформулировать типовые классы информационных систем персональных данных и оптимальные требования к их технической защищенности.

Использование аппаратных средств доверенной загрузки при защите информационных систем персональных данных по требованиям ФСТЭК

Важным является вопрос о необходимости применения аппаратных средств доверенной загрузки при защите персональных данных по требованиям ФСТЭК. Для ответа на вопрос необходимо рассмотреть методические рекомендации ФСТЭК.

В документе [6] установлено требование защиты от несанкционированного доступа к персональным данным. Оно реализуется программными средствами защиты информации от несанкционированного доступа при условии, что само средство защиты запущено и функционирует.

Однако нарушитель может обойти средство программное защиты, перезагрузив компьютер с внешнего носителя информации. Нужно ли рассматривать эту угрозу и что-то предпринимать для защиты от нее?

Согласно базовой модели угроз безопасности персональных данных [4] внутренние нарушители всех категорий имеют физический доступ к информационной системе. При этом оператор информационной системы персональных данных обязан рассматривать группу угроз, реализуемых нарушителями в процессе загрузки операционной системы и направленных на перехват управления загрузкой с модификацией специальных технических параметров с целью совершения несанкционированного доступа к информационной системе. Чаще всего следует ожидать использование внешних сменных накопителей: CD/DVD-диски, устройства USB флэш-памяти, носимые жесткие диски, фотоаппараты, мобильные телефоны, электронные токены с флэш-памятью и т.п. Рассматривая далее типовые модели угроз персональных данных можно определить, что во всех типовых моделях угроз персональных данных есть указание такого источника угроз как сменные носители информации и программное обеспечение на них.

Следовательно, при проектировании безопасности персональных данных требуется рассматривать угрозу загрузки с внешних носителей в процессе загрузки операционной системы. Однако, это не означает, что во всех случаях эта угроза является актуальной. Для оценки актуальности угрозы следует применить методику, изложенную в соответствующем нормативном документе [5]. Например, в системах К1 все оцениваемые угрозы являются актуальными по причине высокого уровня показателя опасности угрозы в силу определения самого класса системы персональных данных класса К1 (“нарушение безопасности этих систем может привести к значительным негативным последствиям для субъектов персональных данных” [3]). Это делает показатель возможности реализации угрозы в К1 нерелевантным при определении актуальности угрозы. Все угрозы системы К1 всегда будут актуальными вне зависимости от возможности их реализации.

Можно сделать следующий общий вывод, что угроза загрузки с внешних накопителей:

- Для всех информационных систем класса К1 будет признана актуальной и будет подлежать анализу в проектах безопасности, в результате чего угроза должна быть нейтрализована либо организационными мерами, либо применением аппаратных средств защиты информации;
- Для информационных систем класса К2 и К3 актуальность угрозы будет определяться в процессе проектирования системы безопасности с учетом среднего и низкого уровней показателей опасности угрозы, что, по моему мнению, будет приводить к неактуальности угрозы во многих системах этого класса.

Как следствие из вышеизложенного, можно сделать вывод, что в аппаратные средства защиты от загрузки с внешних носителей информации должны применяться в информационных системах персональных данных при условии, что эта угроза оценена как актуальная и не может быть устранена организационными мерами. Следует отметить, что, обычно, применение технических средств является более эффективным и надежным средством обеспечения безопасности информации, чем применение организационных мер, если рассматривать не только момент внедрения, но и весь период последующей эксплуатации системы безопасности.

В настоящий момент на рынке представлен набор аппаратных средств защиты, нейтрализующих угрозу загрузки с внешних носителей информации: АПМДЗ “Соболь” и PCI-плата “SecretNet Touch Memory Card” (производства ГК “ИНФОРМЗАЩИТА”), “Аккорд-АМДЗ” (производства ОКБ САПР), АПМДЗ “КРИПТОН-ЗАМОК” (производства фирмы “АНКАД”) и другие.

Защита от программно-математических воздействий по требованиям ФСТЭК

Программно-математическое воздействие – это несанкционированное воздействие нарушителя на ресурсы информационных систем персональных данных, осуществляемое с помощью специальных вредоносных программ, ставящее целью получение несанкционированного доступа к информации. Обычно такие вредоносные программы эксплуатируют известные нарушителю уязвимости программного обеспечения, используемого в информационной системе.

Средства защиты от программно-математических воздействий (СЗИ от ПМВ) разделяется на два вида: сетевые и локальные. Локальные устанавливаются на рабочих местах и являются оправданным решением в случае, когда установка сетевого СЗИ от ПМВ масштаба офиса не является рентабельным. Сетевые СЗИ от ПМВ предназначены для установки внутри информационной системы и разделяются на два подвида:

- Сигнатурные СЗИ от ПМВ – проверяют каждый сетевой пакет на предмет совпадения с сигнатурой известной сетевой атаки, имеющейся в базе сигнатур такой системы;
- Поведенческие СЗИ от ПМВ – определяют аномальное поведение внутри сети: проводят статистический анализ сетевых пакетов или имитируют наличие защищаемых данных на специальных ловушках, отслеживая все обращения к ним, и сообщают администратору безопасности о факте доступа к ловушкам. Ловушка обычно имитирует прикладную систему с известными не устраненными уязвимостями системы безопасности, что делает данную ловушку привлекательной для нарушителя.

Согласно требованиям документов [6-7] для защиты информационных систем персональных данных 1 и 2 классов должны применяться комбинированные методы обнаружения атак (сигнатурные и поведенческие), в частности на базе имитаторов персональных данных на основе специальных модулей-ловушек.

В настоящий момент на рынке доступны такие средства защиты данного класса как:

- IBM ISS (сигнатурная система обнаружения атак);
- PacketMotion (сетевая система выявления аномалий);
- СЗИ от ПМВ Honeypot Manager (производства компании “Код Безопасности”) – первая система имитации персональных данных на базе специальных ловушек, специально созданная в соответствии с требованиями документа [6], которая выпущена в конце августа 2009 г и в настоящий момент находится на сертификации.
- Продукт Endpoint Protection (производства компании “Код Безопасности”), входящий в пакет Security Studio, который содержит продукты для защиты персональных данных на автоматизированных рабочих местах. Продукт выпущен в начале сентября 2009 г и в настоящий момент находится на сертификации сразу по трем компонентам защиты: персональный межсетевой экран, персональная комбинированная система обнаружения атак на рабочее место, антивирус (созданный с учетом требований документа [6]).

Защита сетевых приложений и сервисов, обрабатывающих информацию ограниченного доступа

Персональные данные зачастую обрабатываются не на локальных компьютерах, а на серверах баз данных, в клиентских приложениях, использующих сетевые сервисы (такие как внутрикорпоративные web сервисы или сервера приложений), в web приложениях, и т.п. В то время как традиционные средства защиты информации от несанкционированного доступа, созданные

на базе требований к автоматизированным системам сконцентрированы на защите локальных конфиденциальных файловых ресурсов. Последние версии таких СЗИ от НСД поддерживают работу в терминальном режиме Microsoft и Citrix, что позволяет осуществлять защиту в рамках сетевого доступа в терминальном режиме к локальным ресурсам пользователя на сервере терминалов, что является безусловным шагом вперед. Однако в ряде вариантов систем персональных данных, применение таких СЗИ от НСД не позволяет закрыть новые требования ФСТЭК к подсистеме защиты от НСД информационной системы.

Технической проблемой является также то, что, используя традиционное СЗИ от НСД, пользователь аутентифицируется на локальном автоматизированном рабочем месте и его аутентичность достоверна только в пределах этого рабочего места. При попытке обратиться к сетевому ресурсу (т.е. установить TCP/IP соединение через некий порт с целью получить данные ограниченного доступа) нет предусмотренной возможности передать некий доверенный токен безопасности пользователя – реально передается стандартный токен безопасности операционной системы (на встроенные функции безопасности которой нет сертификата об отсутствии в них недеklarированных возможностей). Т.о. для доверенного контроля доступа требуется использование механизма доверенной сетевой идентификации, аутентификации и авторизации – т.е. пользователя, вошедшего в систему на одном компьютере сети к сетевому сервису, расположенного на другом компьютере сети. Также требуется обеспечивать идентификацию отправителя каждого сетевого пакета для определения начала и конца различных виртуальных соединений.

Одним из возможных решений может быть применение такого продукта как КриптоПро TLS совместно с удостоверяющим центром КриптоПро УЦ. Данное решение решает проблемы доверенной аутентификации и доверенной сетевой сессии, однако функция доверенной авторизации к информационному ресурсу данным решением не реализуются. “Протокол TLS предоставляет возможности аутентификации и безопасной передачи данных с использованием криптографических средств” [8], однако третья функция (авторизация) в принципе выпадает за рамки его назначения. В то время как для защиты персональных данных в информационных системах требуется реализация доверенного контроля доступа, реализованного во всех его трех компонентах. Дополнительной особенностью применения КриптоПро TLS является необходимость реконфигурации всех сетевых приложений и сервисов на использование протокола TLS, что, во-первых, может не всеми ими поддерживаться, во-вторых, будет требовать постоянного контроля над тем, что порты и протоколы, не защищенные TLS, вновь не открыты.

Поэтому нами было принято решение о разработке специального продукта для сетевого разграничения доступа, созданного для реализации требований документа [6], и получившего название TrustAccess.

Продукт имеет собственные механизмы сетевой идентификации, аутентификации и разграничения доступа на базе протоколов сервера аутентификации Керберос, и протоколов создания доверенных соединений на базе IPSec – Authentication Header и ISAKMP. По сути это дополнительная «защитная оболочка», в которую можно «обернуть» практически любую информационную систему (в текущей версии — только на основе ОС Windows). При развертывании продукта можно использовать существующую топологию локальной сети без какой-либо реконфигурации. Защита является прозрачной для приложений. В результате нет необходимости вносить изменения в логику работы информационных систем, не нужно дорабатывать приложения и менять протоколы сетевого взаимодействия (например, переключать на SSL) компонентов информационной системы.

Независимые механизмы защиты могут быть востребованы также для дополнительного ограничения полномочий администраторов Windows, если они не должны быть одновременно администраторами безопасности. Пользователь, обладающий административными правами доступа, является очень важным субъектом безопасности информационной системы. Зачастую он может манипулировать защищаемыми данными в обход существующей политики информацион-

ной безопасности, отключать механизмы защиты, предоставлять несанкционированный доступ прочим субъектам.

Вопросы доверия к действиям высокопривилегированных пользователей нельзя рассматривать лишь с точки зрения злого умысла последних. Администраторы, как и все люди, могут совершать ошибки при выполнении штатных операций, кроме того, их учетные записи могут стать предметом целенаправленной атаки (например, подбор пароля, повышение привилегий и т. п.) со стороны нарушителей.

Обычно не существует технических возможностей защититься от высокопривилегированных пользователей информационной системы с помощью встроенных средств защиты самой информационной системы, а организационные меры порой сложны в реализации. TrustAccess решает эту проблему техническими средствами.

Важным следствием внедрения продукта является возможность задавать права субъектам доступа (пользователям) на объекты доступа (сетевые сервисы) как это и требует документ [6], т.е. устанавливать правила вида “Пользователь А имеет (не имеет) право доступа на ресурс В с любого компьютера в сети”.

Продукт готовится к выпуску в 4 квартале 2009 г и будет проходить сертификацию в ФСТЭК.

Защита виртуальной инфраструктуры

Решения на базе виртуализации получают сегодня все большее распространение, однако в такой среде возникают специфические особенности обеспечения информационной безопасности, без учета которых нельзя гарантировать сохранность данных ограниченного доступа. При обработке информации в виртуальной среде имеет свои специфические особенности, отсутствующие в физической среде:

- **информация обрабатывается в гостевых машинах, которые находятся под полным контролем гипервизора**, способным абсолютно незаметно для традиционных средств защиты информации, расположенные в гостевых машинах, перехватывать все данные, идущие через устройства;
- **администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору становится очень важным субъектом безопасности информационной системы** – фактически, он может получить доступ к информационным ресурсам в обход существующей политики информационной безопасности компании;
- **средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки**, проникновение в которые дает возможность нарушителю получить доступ к гипервизорам серверов виртуализации, а затем к конфиденциальным данным, обрабатываемым на гостевых машинах;
- **диски гостевых машин обычно размещаются в сетевых хранилищах**, которые должны физически защищаться как самостоятельные устройства;
- **традиционные межсетевые экраны не контролируют трафик внутри сервера виртуализации**, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети, однако это сетевой трафик не покидает сервера виртуализации и не проходит через физические межсетевые экраны и другое физическое сетевое оборудование;
- **каналы передачи служебных данных серверов виртуализации** обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной

памяти гостевых машин, которые разумеется могут содержать конфиденциальные данные.

Первые 4 угрозы могут быть успешно нейтрализованы новым продуктом “Кода Безопасности“ vGate, первая версия которого разработана для сертифицированной защиты данных ограниченного доступа, обрабатываемых в среде виртуализации компании VMware и созданного с учетом требований документа [6]. Аналогов на российском рынке данный продукт пока не имеет.

Проблему экранирования внутри сервера виртуализации предлагается выполнять с помощью межсетевых экранов в виртуальном исполнении, либо с помощью персональных межсетевых экранов, расположенных внутри гостевых машин.

Последнюю угрозу можно нейтрализовать путем применения СКЗИ – VPN, либо межсетевым экранированием служебного сегмента.

Заключение

Как можно видеть нормативные документы по защите персональных систем персональных данных [4-7] привели к необходимости создания новых типов продуктов. В этом году “Код Безопасности” выпускает и сертифицирует продукты, которые комплексно закрывают требования к защите персональных данных: как на рабочих местах, так и в сети. Особенную важность, при этом приобретает совместимость средств защиты между собой (если они куплены у разных производителей) и объединенные средства централизованного управления и мониторинга, которые позволяют не иметь отдельный пользовательский интерфейс администратора на каждый компонент защиты, а наблюдать за событиями из “одного окна”.

Список литературы

[1] Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных"

[2] Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"

[3] Приказ от 13 февраля 2008 года N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"

[4] Нормативный документ ФСТЭК: "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года

[5] Нормативный документ ФСТЭК: "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года

[6] Нормативный документ ФСТЭК: "Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" от 15 февраля 2008 года

[7] Нормативный документ ФСТЭК: "Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года

[8] Сайт “Википедия”, статья о протоколе TLS: <http://ru.wikipedia.org/wiki/TLS>