



Код безопасности
ГК «Информзащита»

Решения «Кода Безопасности» для защиты персональных данных

В статье рассматриваются новые и традиционные продукты компании и их применение для защиты информационных систем обработки персональных данных.

www.securitycode.ru

info@securitycode.ru, +7 (495) 980–2345

Введение

Федеральным законом №152 «О персональных данных», главой 14 Трудового кодекса Российской Федерации и Постановлением Правительства РФ №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 «Об утверждении порядка проведения классификации информационных систем персональных данных», а также были утверждены методические 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 информацией 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 фактически сформулировали новые дополнительные технические требования к безопасности информации при ее автоматизированной обработке. 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.

Требования по защите систем персональных данных привели к необходимости создания новых типов продуктов. В 2010 году «Код Безопасности» выпускает и сертифицирует продукты, которые комплексно закрывают требования к защите персональных данных – как на рабочих местах, так и в сети. Особую важность при этом приобретает совместимость средств защиты между собой (если они куплены у разных производителей), а также объединенные средства централизованного управления и мониторинга, которые позволяют наблюдать за событиями из «одного окна», а не использовать отдельный пользовательский интерфейс администратора на каждый компонент защиты.



«Код Безопасности» является единственным российским разработчиком средств защиты информации, продуктами которого можно закрыть все требования нормативных документов для ИСПДн любого класса.

Использование аппаратных средств доверенной загрузки при защите ИСПДн

Важным является вопрос о необходимости применения аппаратных средств доверенной загрузки при защите персональных данных по требованиям ФСТЭК.

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.

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. 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.

Актуальность угрозы загрузки с внешних носителей для информационных систем класса К2 будет определяться в процессе проектирования системы безопасности с учетом среднего уровня показателя опасности угрозы. Фактически угроза может быть признана неактуальной только в системах с высокой степенью исходной защищенности

и в некоторых системах со средней степенью исходной защищенности, где реализация угрозы будет признана маловероятной, таким образом, есть основания полагать, в большинстве систем K2 угроза будет признана актуальной.

Для информационных систем класса K3 актуальность угрозы будет определяться в процессе проектирования системы безопасности с учетом низкого уровня показателя опасности угрозы, и в большинстве систем угроза будет признана неактуальной.

На основании вышеизложенного можно сделать вывод, что 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 компания «Код Безопасности» представляет на рынке набор аппаратных средств защиты, нейтрализующих угрозу загрузки с внешних носителей информации:

- **Электронный замок «Соболь»** - это аппаратно-программное средство защиты компьютера от несанкционированного доступа (аппаратно-программный модуль доверенной загрузки). «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.
- **Secret Net Touch Memory Card** представляет собой плату PCI/PCI Express и позволяет осуществлять аппаратную поддержку реализуемой Secret Net процедуры идентификации и аутентификации пользователей с помощью электронных идентификаторов iButton и запрет несанкционированной загрузки операционной системы с внешних съемных носителей.

Защита от программно-математических воздействий

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 информации от программно-математических воздействий (СЗИ от ПМВ) разделяются на два вида: сетевые и локальные. Локальные СЗИ от ПМВ устанавливаются на рабочих местах и являются оправданным решением в случае, когда установка сетевого СЗИ от ПМВ масштаба офиса не является рентабельной. 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 неустранимыми уязвимостями системы безопасности, что делает данную ловушку привлекательной для нарушителя.

Согласно требованиям документов ФСТЭК 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.

«Код Безопасности» представляет на рынке следующие средства данного класса:

1. **СЗИ от ПМБ Honeypot Manager** – первая система имитации персональных данных на базе специальных ловушек, специально созданная в соответствии с требованиями документов ФСТЭК; выпущена в конце августа 2009 г. и в настоящий момент находится на сертификации.
2. **Security Studio Suite** – защита персональных данных на рабочих местах. Это комплексное решение, включающее в себя следующие компоненты:
 - a. **Безопасный доступ в сеть** – межсетевой экран с контролем трафика пресекает попытки несанкционированного доступа к защищаемой информации из локальной сети или Интернета.
 - b. **Антивирусная защита** – быстрый и эффективный сканер, сочетающий антивирус и антишпион, автоматически обнаруживает и обезвреживает или удаляет вредоносное ПО. Монитор доступа защищает компьютер от попыток проникновения и активации вредоносных программ.
 - c. **Защита от программно-математического воздействия** – модуль «Локальная безопасность» контролирует взаимодействие программ, предотвращая неизвестные или подозрительные операции, позволяя защитить систему от нераспознаваемых угроз.
 - d. **Защита от отключения системы безопасности** – вирусы и хакеры не смогут отключить работу системы защиты, благодаря чему она всегда будет оставаться на страже безопасности.
 - e. Дополнительные модули «**Веб-контроль**» и «**Антиспам**» оградят от угроз Интернета, включая риски обращения к вредоносному контенту веб-серверов и кражи личных данных. Самообучающиеся инструменты защиты от спама позволяют эффективно распознавать и отсеивать ненужные письма.



При необходимости можно приобрести отдельные компоненты системы для закрытия определенных требований по защите персональных данных. Security Studio Suite обеспечивает защиту ИСПДн до класса К1.

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 веб-сервисы или серверы приложений), в веб-приложениях и т. п. В то же время 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. Таким образом, требуется использование механизма доверенной сетевой аутентификации и авторизации пользователя, вошедшего в систему на одном компьютере сети, к сетевому сервису, расположенному на другом компьютере сети. Также требуется обеспечивать идентификацию отправителя каждого IP-пакета для определения начала и конца различных виртуальных соединений.

Поэтому в «Коде Безопасности» было принято решение о разработке специального продукта для сетевого разграничения доступа, созданного для реализации требований ФСТЭК и получившего название **TrustAccess**.

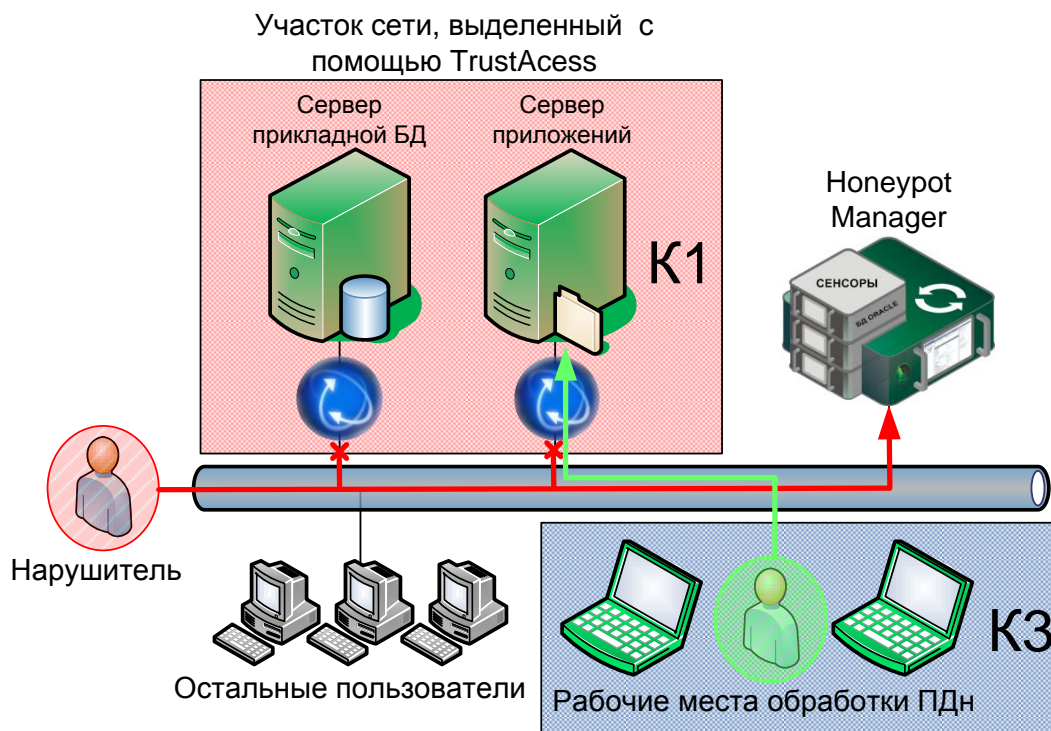
Продукт имеет собственные механизмы сетевой идентификации, аутентификации и разграничения доступа на базе протоколов сервера аутентификации Керберос и протоколов создания доверенных соединений на базе IPSec – Authentication Header и ISAKMP. По сути это дополнительная «защитная оболочка», в которую можно «обернуть» практически любую информационную систему (в текущей версии – только на основе ОС семейства 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.

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.



Продукт готовится к выпуску в 1 полугодии 2010 г. и будет проходить сертификацию в ФСТЭК.

На данной схеме демонстрируется реальный пример работы и взаимодействия продуктов компании «Код Безопасности»:



Рабочие места обработки ПДн защищаются с помощью **Security Studio Suite**. Пул серверов защищается с помощью **TrustAccess** и компонентов **Security Studio Suite**: СЗИ от НСД, антивирус, СЗИ от ПМВ.

Сегментирование заключается в разделении ИСПДн на взаимодействующие участки сети, которые можно применять для оптимизации набора СЗИ, применяемых в каждом сегменте. Это приводит, с одной стороны, к снижению стоимости защиты, а с другой стороны, снижает избыточность СЗИ в тех случаях, когда защищаемые данные расположены неравномерно по сети.

Применение системы серверных межсетевых экранов 2 класса с централизованным управлением **TrustAccess** позволяет реализовать в проекте безопасности такое сегментирование ИСПДн до К1 включительно, что образованные сегменты могут представлять собой отдельные ИСПДн индивидуального уровня защищенности или класса.

Аутентифицированный и авторизованный пользователь ИСПДн получает доступ к персональным данным, а при попытке соединения с ресурсами ИСПДн не прошедший процедуру аутентификации пользователь или пользователь, не обладающий на это правами, автоматически перенаправляется в ловушку **Security Studio Honeypot Manager**.

Защита ИСПДн в виртуальной среде

Все больше компаний отдают предпочтение технологиям виртуализации. Причиной являются те выгоды, которые они получают после переноса своих информационных систем в виртуальную среду. Это значительная экономия на обслуживании ИТ-инфраструктуры, повышение ее гибкости и надежности работы приложений при аппаратных сбоях.

Безопасность информации – один из ключевых вопросов при развертывании ИСПДн в виртуальной среде. Нужно учитывать, что, во-первых, виртуальным машинам присущи ровно те же уязвимости, что и физическим, а во-вторых, как и любая новая технология, виртуализация несет в себе новые угрозы безопасности. Проблема усугубляется тем, что, с одной стороны, традиционные средства защиты информации не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. С другой стороны, они не защищают от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры.

Специалисты «Кода Безопасности» выполнили анализ угроз, характерных для виртуализации. В результате было принято решение о разработке специализированного средства защиты информации в виртуальной среде, причем такого средства, которое обеспечит сертифицированную защиту в виртуальной среде и в результате поможет операторам ПДн пройти аттестацию «виртуальных» ИСПДн.

В настоящее время готовится к началу продаж первая версия продукта vGate, предназначенная для защиты виртуальных инфраструктур на платформе VMware Infrastructure 3 и vSphere 4. Продукт имеет сертификат ФСТЭК, позволяющий применять его для защиты ИСПДн до К2 включительно.

Во втором квартале 2010 года готовится выход vGate 2.0, после чего продукт будет передан на сертификацию. Уровень сертификации vGate 2.0 позволит защитить в виртуальной среде ИСПДн до К1 включительно.

Классификация продуктов «Кода Безопасности» по классам защиты ИСПДн

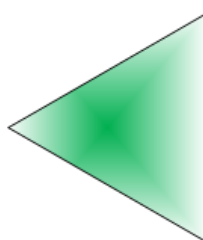
Класс СЗИ	Продукты	Класс ИСПДн		
		К3	К2	К1
Средство защиты информации от несанкционированного доступа	СЗИ Secret Net	○	○	●
	СЗИ Security Studio	●	●	
	vGate	●	●	●
Межсетевой экран	АПКШ «Континент»	●	●	●
	TrustAccess	●	●	●
Средство доверенной загрузки	Электронный замок «Соболь»	○	●	●
Средство криптографической защиты	СКЗИ М-506А-ХР ¹	●	●	●
Защита от ПМВ	HoneyPot Manager	●	●	●

● - ТРЕБУЕТСЯ, ○ - РЕКОМЕНДУЕТСЯ

Типовые схемы защиты ИСПДн на рабочих местах в соответствии с требованиями ФСТЭК

Для защиты рабочих мест обработки персональных данных без подключения к сетям общего пользования, в том числе и локальным сетям, в зависимости от класса необходимо использовать следующий набор продуктов компании «Код Безопасности»:

Класс К3:



Тип Продукта	Название Продукта
Модуль доверенной загрузки	ПАК «Соболь» 3.0
Антивирус	Security Studio Endpoint Protection AV

¹ М-506А-ХР следует применять при аттестации по линии ФСБ в ИСПДн всех классов либо при аттестации по линии ФСТЭК в ИСПДн 1 класса в многопользовательских системах с равными правами доступа.

Класс К2:

Тип Продукта	Название Продукта
Модуль доверенной загрузки	Secret Net Touch Memory Card PCI 2
СЗИ от НСД	Secret Net
Антивирус	Security Studio Endpoint Protection AV

Класс К1:

Тип Продукта	Название Продукта
Модуль доверенной загрузки	ПАК «Соболь» 3.0
СЗИ от НСД	Secret Net
Антивирус	Security Studio Endpoint Protection AV

При подключении рабочего места к сети общего пользования набор средств защиты необходимо дополнить межсетевым экраном. Это позволит обеспечить защиту персональных данных до класса К1 включительно.



Тип Продукта	Название Продукта
Защита информационного канала между АРМ и Интернетом	Security Studio Endpoint Protection FW + HIPS или СЗИ "Континент" АП 3.5

