



Код безопасности
ГК «Информзащита»

127018, Москва, а/я 55; т./ф.: (495) 980 23 45
e-mail: market@infosec.ru, web: www.securitycode.ru

Почему необходимо использовать платы аппаратной защиты при защите персональных данных



Введение

С каждым днем все острее стоит вопрос – как защитить персональные данные и что для этого нужно? В данном материале хотелось бы рассмотреть необходимость использования аппаратных средств, обеспечивающих доверенную загрузку операционных систем компьютеров информационной системы персональных данных (ИСПДн). Такие средства помогают защититься от угрозы несанкционированного доступа (НСД) к персональным данным. Чтобы реализовать недоверенную загрузку, достаточно иметь любой внешний накопитель (CD, DVD, USB Flash, USB Token + Flash, внешний USB-винчестер и т. д.). Защититься от такой угрозы программными средствами невозможно, так как операционная система, в которую они установлены, не будет запущена нарушителем.

Данную угрозу можно описать в трех качествах:

- как доступ в ИСПДн пользователя, не идентифицированного средством защиты (в силу того что эти средства даже не были запущены, так как не запускалась операционная система, где они установлены);
- как способ обхода средства защиты информации (СЗИ) от НСД;
- непосредственно как реализация угрозы недоверенной загрузки либо как модификация схемы загрузки операционной системы.

Теперь хотелось бы рассказать о том, какие документы ФСТЭК требуют учитывать указанную угрозу во всех трех качествах.

При выборе СЗИ от НСД для применения в типовой ИСПДн недостаточно рассмотреть лишь типовой класс конкретной ИСПДн (К1–К3) и требования к ней в отрыве от типовой модели угроз ФСТЭК и типовой модели нарушителя ФСТЭК. Необходимо руководствоваться следующими аспектами, описанными на стр. 12 документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»:

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.



Необходимость защиты ИСПДн от НСД с использованием средств аппаратной поддержки

Далее пойдет подробное описание с цитатами из нормативных документов, которое поможет объяснить, почему нельзя реализовать требования ИСПДн к защите от НСД без аппаратной части.

Для начала обратимся к документу «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»:

пункт 5.1 – «Характеристика источников угроз несанкционированного доступа в информационной системе персональных данных»:

«Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.»;

пункт 5.3 – «Характеристика угроз непосредственного доступа в ИСПДн»:

«Эти угрозы могут быть реализованы в случае физического доступа в ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. Их можно объединить по условиям реализации в три группы:

Первая группа включает в себя угрозы, реализуемые в ходе загрузки операционной системы. Эти угрозы безопасности направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации».

Проанализировав все типовые модели угроз, описанные в пункте 6 данного документа, можно отметить, что во всех случаях есть указание такого источника угроз, как отчуждаемые носители информации. Даже если рассматривать наиболее простейшую модель угрозы, описанную в пункте 6.1, можно встретить следующую информацию: *«Угрозы НСД в автономном АРМ связаны с действием нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в АРМ могут быть аппаратные закладки и отчуждаемые носители вредоносных программ».*

Почему же так важно уделять достаточное внимание угрозе отчуждаемых носителей? Это вытекает из пункта 5.1. документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», именно там определены 8 категорий внутренних потенциальных нарушителей. Согласно их описанию,

Документ не может быть полностью или частично перепечатан, скопирован или передан без разрешения ООО «Код Безопасности»



нарушители 1–6 категорий потенциально могут реализовать угрозу НСД через загрузку с внешних носителей, так как уже в описании нарушителя первой категории сказано, что эти нарушители могут:

«Изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съём информации, используя непосредственное подключение к техническим средствам ИСПДн».

Остальные категории нарушителей включают возможности предыдущих.

Рассмотрев типовые модели угроз персональных данных, можно определить, что сменные носители и программное обеспечение на них являются источниками угроз и все категории нарушителей, введенные ФСТЭК для ИСПДн, могут реализовать угрозу НСД через недоверенную загрузку.

Теперь рассмотрим документ ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Для того чтобы определить актуальность, необходимо определить опасность угрозы:

«низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных».

Описания опасности угроз определяются так же, как и системы К1–К3 согласно пункту 3 документа «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

Актуальность угрозы недоверенной загрузки можно определить, используя таблицу 2 рассматриваемого документа:

Таблица 2 – Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Документ не может быть полностью или частично перепечатан, скопирован или передан без разрешения ООО «Код Безопасности»



Используя приведенную таблицу, можно с уверенностью утверждать, что:

- **В системе К1** уровень опасности угрозы недоверенной загрузки будет высоким, а угроза – актуальной, причем ВНЕ зависимости от вероятности ее реализации. Таким образом, использование средств аппаратной защиты будет всегда обязательным. Оргмерами запретить флешки на проходной компании фактически невозможно.
- **В системе К2** уровень опасности угрозы недоверенной загрузки будет средним («средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны»). А угроза не будет актуальной, только если в проекте безопасности ИСПДн будет показано, что возможность реализации угрозы – низкая. Возможность реализации угрозы зависит от двух факторов – исходной защищенности системы и вероятности реализации угрозы. Таким образом, на практике, на наш взгляд, таких К2 систем будет не меньше 50%.
- **В системе К3** также в большинстве случаев будет требоваться решения проблемы недоверенной загрузки. Особенностью этого класса ИСПДн является относительно меньший объем требований по их защите, что по нашему мнению открывает возможность использовать Соболь как единственное и достаточное средство защиты. Подробное обоснование этого утверждения приведено в последнем разделе этого документа.

Вывод: Мы считаем, что для реализации защиты от угрозы недоверенной загрузки необходимо использовать ПАК «Соболь» или Secret Net TM Card, поскольку защититься от такой угрозы программными средствами невозможно, ведь операционная система, в которую они установлены, не будет загружена и запущена нарушителем.



Применение требований и подходов к обеспечению защиты информации к автоматизированным системам в ИСПДн

Согласно документу ФСТЭК «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (стр.12) при организации и осуществлении защиты ПДн **необходимо** руководствоваться РД ФСТЭК по защите автоматизированных систем.

«В целом обеспечение безопасности ПДн при их обработке в ИСПДн достигается реализацией совокупности организационных и технических мер, причем в интересах обеспечения безопасности ПДн в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации. При организации и осуществлении защиты ПДн необходимо руководствоваться требованиями нормативных и методических документов по защите информации в автоматизированных системах, учитывая при этом, что ПДн, в соответствии с Федеральным законом от 27 июля 2006 г. №152 «О персональных данных», отнесены к информации ограниченного доступа.

В связи с тем, что ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, целесообразно при их защите максимально использовать традиционные подходы к технической защите информации».

Угроза загрузки с внешнего носителя влечет за собой следующие последствия:

- загрузка нарушителем своей программной среды;
- получение доступа в ИСПДн без аутентификации и идентификации;
- обход программных СЗИ от НСД;
- создание неидентифицированного терминала или ЭВМ – компонента защищаемой ИСПДн.

Таким образом, для управления доступом в ИСПДн необходима таблица, в которой приведено детальное описание этой угрозы:

Документ ФСТЭК	Цитата
П. 2.12 РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»	2.12. Требования к классу защищенности 1Г: Подсистема управления доступом: - должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов; - должна осуществляться идентификация



Документ ФСТЭК	Цитата
	терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам.
П. 5. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»	К основным способам НСД относятся: <ul style="list-style-type: none">создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты.
П. 4.2.8. «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» – требование присутствует не только в этом пункте, а относится ко всем типам ИСПДн	В подсистеме управления доступом: <ul style="list-style-type: none">- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
П. 2.2.2. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»	Комплекс средств защиты должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась

Исходя из приведенных выше данных, можно с уверенностью сказать, что для защиты от обхода СЗИ от НСД требуется использовать сертифицированное аппаратное средство блокировки загрузки с внешних носителей – ПАК «Соболь» или Secret Net Touch Memory Card. (Если возможно организовать оргмеры, деактуализирующие угрозу несанкционированной загрузки, – можно и без аппаратной части.)



ПАК «Соболь» как необходимое и достаточное СЗИ от НСД

На наш взгляд, в ряде подклассов ИСПДн 2 и 3 классов можно обойтись одним лишь ПАК «Соболь» (без использования каких-либо дополнительных программных СЗИ от НСД). Например, при условии, что компьютер, обрабатывающий ПДн, один и не подключен к сети компании и на нем работает один главный бухгалтер. Ниже приведена таблица требований к ИСПДн 2 и 3 классов, где достаточно «Соболя» плюс учета носителей информации (организационными мерами).

Обозначения в таблице:

- 2, 3 – обозначает класс ИСПДн
- “О” – однопользовательская ИСПДн
- “МО” – многопользовательская с одинаковыми правами
- “МР” – многопользовательская с разными правами

Формулировка	3О	2О	3МО	2МО	3МР
Вход/выход пользователей в/из систему					
Идентификация и проверка подлинности субъектов доступа при входе в систему (ОС) ИСПДн по паролю условно-постоянного действия длиной не менее 6 буквенно-цифровых символов	Да	Да	Да	Да	Да
Регистрация входа (выхода) субъекта доступа в систему (из системы) либо регистрация загрузки и инициализации ОС и ее программного останова. Регистрация выхода из системы или останова не производится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная)	Да	Да	Да	Да	Да
В дополнение к предыдущему пункту: в параметрах регистрации должен указываться идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа					Да



Формулировка	3О	2О	3МО	2МО	3МР
Регистрация событий (аудит, персональных данных при их обработке в информационных системах персональных данных общие требования)					
Данные регистрации должны быть защищены от их уничтожения или модификации нарушителем	Да	Да	Да	Да	
Должны быть реализованы механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов	Да	Да	Да	Да	
Должны быть реализованы механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров	Да	Да	Да	Да	
Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительно защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров в составе ИСПДн, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта – логическое имя (номер)					
Контроль целостности					
Должна быть обеспечена целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ	Да	Да	Да	Да	



Формулировка	3О	2О	3МО	2МО	3МР
Должна быть обеспечена целостность программных средств защиты информации в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по контрольным суммам компонентов СЗИ, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации					Да
Надежное восстановление					
Должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности	Да	Да	Да	Да	Да
Тестирование					
Должно производиться периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД	Да	Да	Да	Да	Да