

DeviceLock для соответствия ФЗ «О персональных данных»



Оглавление:

- [Введение](#)
- [Требования ФЗ «О персональных данных»](#)
 - [Анализ положений закона](#)
 - [Требования Постановления Правительства РФ](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock для защиты персональных данных](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Федеральный Закон (ФЗ) «О персональных данных» был принят в конце июля 2006 года и вступил в силу в конце февраля 2007 года. В соответствии с этим нормативным актом все юридические и физические лица, хранящие или обрабатывающие персональные данные других граждан, обязаны обеспечить конфиденциальность этой информации. В противном случае организации или граждане, нарушающие закон, могут быть привлечены к суду, оштрафованы и/или лишены лицензии на обработку персональных данных, что неминуемо ведет к остановке бизнеса. При этом под самими персональными данными понимается очень широкая категория сведений: фамилия, имя, отчество, место и дата рождения, адрес регистрации, образование, профессия, доходы, истории болезни и т.д. По сути, любые сведения о жизни гражданина определены законом в качестве персональных данных.

С полным текстом федерального закона N 152-ФЗ «О персональных данных» можно ознакомиться в «Российской газете» N4131 от 29 июля 2006 года¹. Отметим, что, с одной стороны, этот нормативный акт определяет только самые общие требования к безопасности персональных данных. С другой стороны, даже ознакомление с этими абстрактными положениями делает очевидным, что соответствие закону потребует принятия административных мер и внедрения определенных решений в сфере ИТ-безопасности.

В данном документе будут рассмотрены требования ФЗ «О персональных данных», которые влияют на информационную инфраструктуру организаций и использующиеся в ней средства безопасности, а также возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия федеральному закону.

Требования ФЗ «О персональных данных»

Прежде чем перейти к анализу требований закона, следует дать несколько ключевых определений. Примеры персональных данных уже были даны ранее в этом документе, поэтому определим еще два основных понятия: оператор персональных данных и обработка персональных данных.

Согласно ст.2, оператор персональных данных это государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. Отсюда следуют два вывода. Во-первых, госструктуры также

¹ См. также текста закона на сайте «Российской газеты»: <http://www.rg.ru/2006/07/29/personaljnve-dannye-dok.html>

попадают под действие ФЗ «О персональных данных» и, следовательно, обязаны заботиться о конфиденциальности этих сведений. Во-вторых, в сферу действия закона попадают также физические лица, а не только организации.

Далее, согласно ст. 2, обработка персональных данных – это практически любые действия с этой информацией. Например, сбор, систематизация, накопление, хранение, уточнение (обновление, изменение). Помимо этого, в понятие обработки входят использование, распространение, передача, обезличивание, блокирование, уничтожение.

Принципиально важно, что в самом начале закона вместе с основными определениями дается толкование конфиденциальности персональных данных. Согласно нормативному акту, это обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания. Таким образом, требования к защите от утечек и несанкционированного доступа вплетены в саму структуру закона уже на уровне определений.

Анализ положений закона

Задача обеспечения конфиденциальности персональных данных ставится в тексте закона в нескольких местах. Выше уже было показано, что обязательность обеспечения защиты от утечек и несанкционированного доступа закреплена в законе на уровне определений. Еще раз это же требование встречается в 7 ст., согласно которой «операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных».

Более подробно проблема конфиденциальности персональных данных при их обработке рассмотрена в ст.19. Согласно ст.19 ч.1, оператор «обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных» от целого ряда угроз. Среди них закон выделяет «неправомерный или случайный доступ, уничтожение, изменение, блокирование, копирование, распространение, а также иные неправомерные действия». Таким образом, нормативный акт предписывает обеспечить защиту персональных данных от целого ряда угроз ИТ-безопасности. При этом требования ст. 19 выходят за рамки конфиденциальности и затрагивают еще и целостность персональных данных.

Согласно ст.19 ч.2, Правительство РФ должно установить требования к «обеспечению безопасности [персональных данных] при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Контроль над выполнением этих требований, согласно ст.19 ч.3, будет возложен на «федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защите информации». Наконец, ст.19 ч.4 разрешает «использовать и хранить биометрические персональные данные вне информационных систем персональных данных ... только на таких материальных носителях информации и с применением такой технологии хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения».

Требования Постановления Правительства РФ

Как уже было показано выше, в ст.19 ч.2 и ч.3 говорится, что Правительство РФ должно установить требования к безопасности персональных данных и возложить контроль над их исполнением на федеральный орган исполнительной власти.

В Постановлении Правительства от 17 ноября 2007 г. N 781 уже закреплено «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Методическую базу для более подробного раскрытия этого положения разрабатывают ФСБ и ФСТЭК России. Однако уже имеющихся требований к безопасности персональных данных, закрепленных в Постановлении Правительства, достаточно, чтобы сделать вывод о необходимых мерах и средствах ИТ-безопасности.

С полным текстом Постановления Правительства можно ознакомиться в «Российской газете» N4523 от 21 ноября 2007 года². Далее рассмотрим лишь ключевые требования.

Согласно п.2, безопасность персональных данных должна включать «организационные меры и средства защиты информации (в том числе шифровальные средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам...)». Другими словами, Правительство России однозначно указывает на опасность утечки персональных данных и злоупотребления ими.

Кроме того, п.4 подчеркивает обязательность требований по созданию системы безопасности персональных данных: «Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем».

Пункты 11 и 12 конкретизируют те меры и средства безопасности, которые должны быть приняты и внедрены в организации. Они просуммированы в таблице ниже (см. таб. 1.).

Таб. 1. Требования к безопасности персональных данных (Постановление Правительства от 17.11.07 N 781, пп.11-12)
--

11. При обработке персональных данных в информационной системе должно быть обеспечено:
--

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
--

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль над обеспечением уровня защищенности персональных данных.
--

² См. также сайт «Российской газеты»: <http://www.rg.ru/2007/11/21/personalnye-dannye-dok.html>

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
- з) контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- к) описание системы защиты персональных данных.

Таким образом, ФЗ «О персональных данных» и соответствующее Постановление Правительства РФ призваны урегулировать в полной мере проблему защиты персональных данных от утечки, несанкционированного доступа и других угроз.

DeviceLock от Смарт Лайн Инк

Продукт DeviceLock разработан российской компанией ЗАО «Смарт Лайн Инк» и предназначен для корпоративных пользователей. С помощью DeviceLock предприятия любого масштаба могут обеспечить всесторонний контроль над данными, покидающими корпоративную сеть через порты рабочих станций, беспроводные сети и внешние накопители. Помимо этого DeviceLock включает в себя защиту от аппаратных клавиатурных шпионов, использующихся для кражи ценной информации с рабочих станций сотрудника. Злоумышленник может подключить такое устройство между компьютером и клавиатурой служащего и тем самым обмануть антивирус и другое защитное программное обеспечение. Однако DeviceLock выявит подмену, блокирует работу «шпиона», предупредит пользователя и сделает запись в журнал событий.

Ключевой особенностью продукта является не только контроль над фактом передачи данных в соответствии с заданными политиками, но еще и полное теневое копирование всей исходящей информации. Хотя сегодня существует огромное количество решений для хранения почтовой корреспонденции, только DeviceLock позволяет собирать и анализировать информацию, покинувшую корпоративную сеть через локальные порты рабочей станции.

Когда речь заходит о контроле над карманными компьютерами, смартфонами и различными коммуникаторами, то DeviceLock не просто поддерживает теневое копирование всех данных, передаваемых на мобильное устройство, но позволяет также реализовать гибкие политики безопасности и проследить за их исполнением. Например, продукт может разрешить синхронизировать контакты и календарь, но запретить копирование файлов или синхронизацию электронной почты с вложениями.

Это крайне полезная функциональность, особенно, в свете постоянного роста популярности мобильных устройств в медицинских центрах. Кроме того, нельзя сбрасывать со счетов приближающуюся консолидацию корпоративных ИТ-систем. Авторитетные исследовательские агентства Yankee Group и CSC Research утверждают, что директора и менеджеры ИТ-департаментов не могут игнорировать либо запретить то обилие портативных устройств, которыми постоянно пользуются служащие. Они просто обязаны обеспечить поддержку мобильных компьютеров сотрудников. В противном случае компания рискует потерять инновационный потенциал, снизить производительность труда своих служащих, а следом и ослабить свою конкурентоспособность. Между тем, массовая консолидация чревата новыми серьезными рисками в области информационной безопасности, так как мобильные устройства могут быть использованы для осуществления мошенничества, утечки и других внутренних нарушений. Решить эту проблему, в существенной степени, позволяет DeviceLock.

Таким образом, продукт защищает компанию от утечки цифровых активов, попадания во внутреннюю сеть нежелательных типов данных, предоставляет инструментарий для ретроспективного анализа всей информации, которую сотрудники компании скопировали на внешние носители и забрали с собой, а также придает необходимую компании гибкость при работе с мобильными устройствами.

Следует отметить, что DeviceLock позволяет контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, Wi-Fi и Bluetooth-адаптеры, ленточные накопители, КПК, любые внутренние и внешние сменные накопители и жесткие диски. DeviceLock осуществляет детальный аудит действий пользователей с устройствами и данными.

Отдельно стоит выделить возможности DeviceLock по гранулированному контролю доступа пользователей к принтерам, в том числе виртуальным. Продукт не только может обеспечить выполнение политики информационной безопасности и тем самым минимизировать риск несанкционированной утечки через принтеры, но также ведет событийное протоколирование и оставляет теневые копии распечатываемых документов, которые впоследствии можно проанализировать и просмотреть в графическом формате.

Продукт может управляться через групповые политики Windows в домене Active Directory, благодаря чему легко интегрируется в существующую инфраструктуру организации любого масштаба.

С функциональной точки зрения DeviceLock состоит из трех частей (см. рис. 1):

1. DeviceLock Service – это агент, устанавливаемый на каждый компьютер, который автоматически запускается и обеспечивает защиту устройств на машине-клиенте, в то же время оставаясь невидимым для локального пользователя.
2. DeviceLock Enterprise Server – это дополнительный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита. DeviceLock Enterprise Server использует MS SQL Server для хранения данных.
3. Консоль управления – это интерфейс контроля, который администратор использует для управления системой, на которой установлен агент. DeviceLock поставляется с

три консолью управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

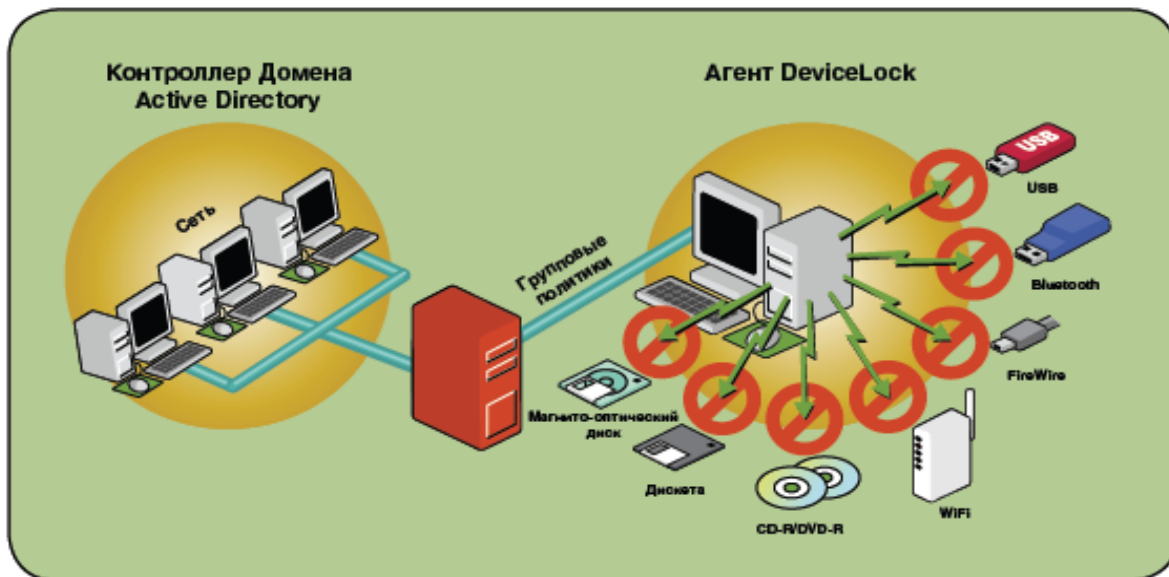


Рис. 1. Схема работы DeviceLock

Предприятия могут легко защищать десятки и сотни тысяч удаленных компьютеров при помощи DeviceLock, используя управление через групповые политики Active Directory.

Возможности DeviceLock для защиты персональных данных

Продукт DeviceLock осуществляет контроль над передвижением данных через локальные порты рабочей станции, беспроводные сети и съемные носители на основе гибких политик. Каждый раз решение о том, чтобы разрешить или запретить доступ к внешнему устройству принимается автоматически. Таким образом, настройки и политики DeviceLock легко подвержены аудиту, а сам продукт не создает дополнительных рисков информационной безопасности.

Использование DeviceLock в корпоративной среде позволяет обеспечить соответствие двум основным требованиям ФЗ «О персональных данных» и Постановления Правительства РФ:

- Согласно п.2 Постановления Правительства РФ, безопасность персональных данных должна включать «организационные меры и средства защиты информации (в том числе шифровальные средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам...)». Очевидно, здесь подразумевается и защита от утечки персональных данных по каналам связи и через локальные коммуникации рабочих станций. DeviceLock позволяет минимизировать риски утечки через сменные носители, мобильные устройства и беспроводные сети, что является неотъемлемым требованием при обеспечении безопасности персональных данных.
- Согласно п.11а Постановления Правительства РФ, организация обязана своевременно обнаруживать факты «несанкционированного доступа к персональным данным». Другими словами, каждая организация обязана иметь механизмы и средства выявления утечки, так как утечка является неавторизованным разглашением персональных данных, следствием чего неминуемо является несанкционированный доступ к этим сведениям со стороны неуполномоченных лиц. На помощь приходит DeviceLock, обеспечивающий теневое копирование данных, экспортируемых с ПК на

сменные носители и мобильные устройства. Анализируя собранную информацию, можно легко определить, где, когда, каким способом и как произошла утечка.

В таблице далее (см. таб. 2) просуммирована функциональность DeviceLock в соответствии с требованиями ФЗ «О персональных данных» и Постановления Правительства РФ.

Таб. 2. Функциональность DeviceLock применительно к ФЗ «О персональных данных» и Постановлению Правительства РФ	
Требования	Возможности DeviceLock
Ст.7 ч.1 ФЗ «О персональных данных»: «Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных...».	Предотвращение несанкционированного копирования и утечки персональных данных является одной из ключевых задач DeviceLock. Продукт с высокой степенью гранулярности контролирует локальные коммуникации рабочих станций, позволяя гибко реализовать положения политики информационной безопасности в отношении доступа к персональным данным.
Ст.19 ч.1 ФЗ «О персональных данных»: «Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».	Одной из таких необходимых технических мер является использование продукта DeviceLock, при помощи которого организация, обрабатывающая персональные данные, может минимизировать риски несанкционированного копирования или распространения персональных данных, неправомерного или случайного доступа к ним со стороны неуполномоченных лиц.
П.2 Постановления Правительства РФ. Безопасность персональных данных должна включать «организационные меры и средства защиты информации (в том числе шифровальные средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам...»).	Утечка информации является одной из самых опасных угроз, выделяемой отдельно, как в ФЗ «О персональных данных», так и в Постановлении Правительства РФ. Минимизировать риски утечки как раз и помогает продукт DeviceLock, позволяющий взять под контроль доступ к сменным носителям, мобильным устройствам и беспроводным сетям. Таким образом, DeviceLock контролирует наиболее популярные каналы утечки.
П.116 Постановления Правительства РФ. Организация должна своевременно обнаруживать факты несанкционированного доступа к персональным данным.	Отсюда следует, что каждая организация обязана иметь механизмы для выявления утечки, так как утечка является неавторизованным разглашением персональных данных, что неминуемо ведет к несанкционированному доступу к этим сведениям со стороны неуполномоченных лиц. На помощь приходит продукт DeviceLock, обеспечивающий теневое копирование данных, экспортируемых с персональных компьютеров на сменные носители и мобильные устройства. Анализируя собранную информацию, можно легко определить, где, когда, каким способом и как произошла утечка.

О компании Смарт Лайн Инк

Разработчик DeviceLock – ЗАО “Смарт Лайн Инк”. Основанная в 1996 году, российская компания Смарт Лайн Инк (SmartLine Inc) занимается разработкой программного обеспечения для администрирования компьютерных сетей. Качество и надежность продуктов Смарт Лайн Инк подтверждают более 55 тысяч клиентов в 80-ти странах мира – государственные, военные, медицинские, образовательные, крупнейшие финансовые и коммерческие учреждения, а также компании малого и среднего бизнеса. Программное обеспечение Смарт Лайн Инк установлено на более чем 3 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силловые машины", ВТБ 24, Российская государственная библиотека, BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank. Смарт Лайн Инк – международная компания с офисами в Лондоне, Милане, Москве, Ратингене (Германия) и Сан Рамоне (штат Калифорния, США). Основной офис разработки программных продуктов Смарт Лайн Инк находится в Москве.

Контактная информация

ЗАО “Смарт Лайн Инк”

Москва, Б. Семеновская ул., д. 40, офис 301

Телефон: +7 (495) 967-9960, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@devicelock.com

Тех. поддержка: support@devicelock.com