DeviceLock для соответствия ФЗ «О коммерческой тайне»

Оглавление:

Введение

Поддержка и обеспечение режима коммерческой тайны – одна из важнейших задач любой современной компании. В период экономического кризиса и массовых сокращений персонала, угрозы утечки конфиденциальной информации многократно возрастают, а их последствия становятся критическими. Внутренние нарушители и халатные сотрудники значительно увеличивают коммерческие и репутационные риски компаний, которые в условиях кризиса и без того достаточно велики.

Согласно российскому законодательству, обеспечение режима коммерческой тайны должно осуществляться в соответствии с одноименным Федеральным законом. ФЗ «О коммерческой тайне», вступивший в действие 16 июля 2004 года, устанавливает основные отношения, связанные с обеспечением режима коммерческой тайны в организациях любого типа и размера. Это означает, что если компания хочет защитить свою конфиденциальную информацию – она обязана соответствовать данному Федеральному закону. В противном случае – само понятие коммерческой тайны теряет юридический смысл, и все сотрудники компании имеют полное право распространять любую корпоративную информацию произвольным образом.

Федеральный закон ФЗ N 98 «О коммерческой тайне» состоит из 16 статей, в которых определяются отношения между обладателем информации (организацией или индивидуальным предпринимателем), его сотрудниками и внешними контрагентами. Помимо Федерального закона в России также действует ряд других нормативов, непосредственно связанных с коммерческой тайной:

- В статье 139 Гражданского кодекса РФ устанавливается ответственность за разглашение коммерческой тайны;

- В статье 2 ФЗ №24 «Об информации, информатизации и защите информации» содержится понятие информации;

- В статье 57 Трудового кодекса РФ предусматривается возможность включения условия «о неразглашении» в трудовой договор работников.

Однако, основную нагрузку по регулированию отношений, связанных с коммерческой тайной, несет именно Федеральный закон N 98.

В данном документе будут рассмотрены требования ФЗ «О коммерческой тайне», влияющие на информационную инфраструктуру организаций и использующиеся в ней средства безопасности. После этого будет приведен обзор возможностей продукта DeviceLock производства компании Смарт Лайн Инк, а также описание функций данного

продукта, при помощи которого организация может гораздо эффективнее достичь соответствия Федеральному закону.

Требования ФЗ «О коммерческой тайне»

В первой статье Федерального закона определяются его цели и область применения. Согласно первому пункту статьи, «закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, […] а также определяет сведения, которые не могут составлять коммерческую тайну». Таким образом, основная цель закона – контроль всех взаимоотношений, связанных с коммерческой тайной в российских компаниях. Второй пункт статьи указывает, что положения закона распространяется на любую информацию «независимо от вида носителя», а третий пункт – ограничивает сферу действия закона информацией, которая не составляет государственную тайну.

Полный текст Федерального закона приведен на официальном сайте «Российской Газеты»[1].

Терминология Федерального закона

Прежде чем говорить о конкретных требованиях Федерального закона, необходимо определиться с терминологией. Список терминов, использующихся в законе, приводится в его третьей статье. В таб. 1 приведены ключевые определения данного нормативного акта.

Таб. 1. Терминология Федерального закона «О коммерческой тайне»

Термин	Определение
1) Коммерческая тайна	Конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
2) Информация, составляющая коммерческую тайну	Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация [...], которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны
3) Режим коммерческой тайны	Правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности
4) Обладатель информации, составляющей коммерческую тайну	Лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны
5) Доступ к информации, составляющей коммерческую тайну	Ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации

[1] http://www.rg.ru/2004/08/05/taina-doc.html

6) Передача информации, составляющей коммерческую тайну	Передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности
7) Контрагент	Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию
8) Предоставление информации, составляющей коммерческую тайну	Передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций
9) Разглашение информации, составляющей коммерческую тайну	Действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору

Согласно первому определению (см. таб. 1), коммерческая тайна представляет собой некоторое свойство информации, имеющей определенную ценность. Каждый конкретный информационный массив может либо обладать этим свойством, либо им не обладать. Но как определить, какая информация может являться коммерческой тайной?

Ответ на этот вопрос дает следующее определение, согласно которому к коммерческой тайне может быть отнесена «научно-техническая, технологическая, производственная, финансово-экономическая или иная информация […], которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны». Другими словами, существует четыре обязательных признака информации, которая составляет коммерческую тайну:

- Информация должна иметь действительную или потенциальную коммерческую ценность;
- Ценность этой информации должна быть обусловлена ее неизвестностью третьим лицам;
- К информации не должно быть свободного доступа на законном основании;
- В отношении данной информации должен быть введен режим коммерческой тайны.

Таким образом, если какая-то информация не обладает хотя бы одним из перечисленных квалификационных признаков, то она не составляет коммерческой тайны и ее разглашение не может привести к какой-либо ответственности.

Отметим, что особенно важную роль играет последний признак, который обязывает обладателя информации ввести режим коммерческой тайны. Данный режим устанавливается в письменной форме и представляет собой «правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности». Обладатель информации вправе установить режим коммерческой тайны для любых сведений, которые удовлетворяют перечисленным выше критериям, а также не входят в список сведений, которые не могут составлять коммерческую тайну (данный список установлен в ст. 5 Федерального Закона).

Права обладателя информации, составляющей коммерческую тайну

Определив сведения, которые составляют коммерческую тайну, а также установив режим, обладатель информации получает определенные права. Полный список этих прав приводится в статье 7 Федерального закона. Согласно п. 2, ст. 7, обладатель информации имеет право устанавливать и отменять режим коммерческой тайны (в письменной форме), а также управлять информацией в рамках введенного режима. В частности, обладатель коммерческой тайны имеет право:

- Использовать эту информацию для собственных нужд;
- Разрешать или запрещать доступ к этой информации, а также определять порядок и условия доступа;
- Вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров;
- Требовать охраны конфиденциальности информации от лиц, которым она была передана (юридических и физических лиц, государственных и муниципальных органов);
- Требовать охраны конфиденциальности информации от лиц, которые получили доступ к ней случайно или по ошибке;
- Защищать свои права в случае разглашения или незаконного использования информации, а также требовать возмещения убытков.

С точки зрения информационной безопасности, фундаментальным для всего ФЗ является право, позволяющее обладателю коммерческой тайны ограничивать доступ к ней. В большинстве случаев именно это право побуждает организации вводить режим коммерческой тайны и следить за его соблюдением.

Требования к режиму коммерческой тайны

Режим коммерческой тайны означает не только дополнительные права, но и ряд обязанностей для обладателя информации. Чтобы ввести режим коммерческой тайны, организация должна выполнить условия, установленные в ст. 10-13 Федерального закона. Общие требования к обладателю информацию приводятся в статье 10 (таб. 2).

Таб. 2. Общие требования к режиму коммерческой тайны (ст. 10)

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

а) определение перечня информации, составляющей коммерческую тайну;

б) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

в) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

г) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

д) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

а) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

б) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Прежде всего (п. 1, пп.1), обладатель информации обязан вести перечень сведений, которые составляют коммерческую тайну. Кроме того, должен быть установлен порядок обращения с этой информацией (пп.2) и проводиться учет лиц, которые получили к этой информации доступ (пп. 3). Следующий подпункт указывает, что отношения по коммерческой тайне прописываются в трудовых договорах сотрудников, а также гражданско-правовых договорах контрагентов. Перечень обязанностей обладателя

завершается требованием обязательной маркировки материальных носителей с информацией, которая составляет коммерческую тайну.

Отметим, что согласно п. 4. ст. 10, обладатель информации вправе «применять при необходимости средства и методы технической защиты конфиденциальности этой информации». Согласно п. 5 эти меры признаются разумно-достаточными, если сотрудники и контрагенты могут использовать данную информацию, а третьи лица – нет. Наконец, согласно п. 6. «режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства».

Статья 11 Федерального закона регулирует отношения обладателя информации и его сотрудников в рамках установленных трудовых отношений. Принципиально важно, что «работодатель обязан создать работнику необходимые условия для соблюдения установленного режима коммерческой тайны» (п. 1). Кроме того, следует выделить п. 3 и п. 4., согласно которым ущерб в результате утечки коммерческой тайны может быть взыскан с провинившегося сотрудника, а также п. 6., который устанавливает ответственность руководителя организации за разглашение коммерческой тайны в рамках договорных отношений.

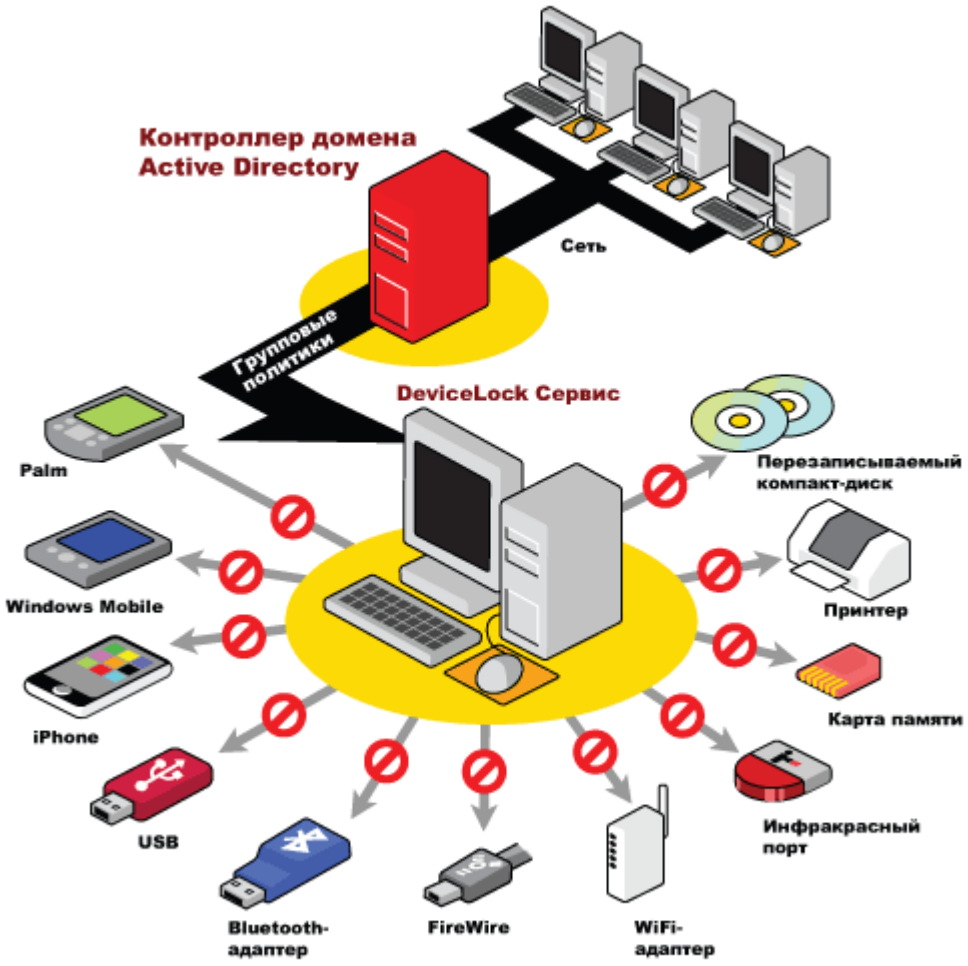
Однако взыскать ущерб от разглашения коммерческой тайны на самом деле достаточно трудно. Согласно п. 2. ст. 14, работник, который допустил утечку информации при отсутствии состава преступления, несет исключительно дисциплинарную ответственность. Таким образом, для защиты коммерческой тайны обладатель информации должен доказать факт разглашения, а значит – использовать какой-либо инструментарий для сбора подобных доказательств.

В завершение обзора требований отметим еще одно положение закона, сформулированное в п. 1 ст. 13., согласно которому все органы государственной власти «обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями» в соответствии с Федеральным законом. Таким образом, положения закона критически важны для всех российских государственных учреждений, которым вменено безусловное выполнение этих требований.

Обзор продукта DeviceLock от компании Смарт Лайн Инк

Программный комплекс DeviceLock производства российской компании Смарт Лайн Инк – это система централизованного контроля доступа пользователей корпоративных информационных систем (ИС) к периферийным устройствам и портам ввода-вывода персональных компьютеров и серверов под управлением операционных систем Microsoft Windows. С помощью DeviceLock предприятия любого масштаба могут обеспечить всесторонний контроль над данными, покидающими корпоративную сеть через порты рабочих станций, сменные накопители и беспроводные сети, а также эффективно противодействовать инсайдерским утечкам информации ограниченного доступа с персональных компьютеров сотрудников и серверов организации.

Рис. 1. Схема работы DeviceLock



С функциональной точки зрения, комплекс DeviceLock состоит из трех частей:

- 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.

- 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.

- Консоль управления – это интерфейс контроля, который администратор использует для управления системой, на которой установлен агент. DeviceLock поставляется с тремя консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

К основным функциям контроля DeviceLock относятся управление доступом к операциям передачи данных и форматирования носителей, событийное протоколирование действий пользователей и администраторов, теневое копирование передаваемых с компьютера

данных, а также обнаружение и блокировка работы аппаратных USB и PS/2 кейлоггеров. В дополнение к основным функциям при наличии на защищаемом компьютере совместимых средств криптографической защиты (СКЗИ) DeviceLock предотвращает несанкционированное копирование нешифрованных данных на съемные устройства памяти.

Относящийся к классу контекстных (context-aware) систем предотвращения утечек данных с оконечных вычислительных устройств (Endpoint Data Leak Prevention), DeviceLock позволяет управлять доступом пользователей ко всем типам интерфейсов и периферийных устройств компьютеров корпоративной информационной системы (ИС), включая USB, FireWire, COM, LPT, IrDA порты, а также жесткие диски, флоппи-дисководы, CD/DVD-приводы, съемные накопители, КПК и смартфоны, локальные и сетевые принтеры, устройства Wi-Fi, Bluetooth и т.п.

DeviceLock обеспечивает контроль всех видов локальных каналов потенциальной утечки данных с компьютеров, включая операции файловой системы со съемными накопителями и другими типами PnP устройств, обмен данными по протоколам синхронизации с КПК и смартфонами, а также канал печати документов.

В DeviceLock поддержаны времязависимые политики, что позволяет контролировать доступ пользователей и их групп к устройствам и портам ввода-вывода с точностью до часа и дня в рамках недельного графика. Кроме того, для каждого пользователя или их группы можно задать индивидуальный «белый список» USB устройств (USB white listing), доступ к которым будет всегда разрешен вне зависимости от установленных политик доступа для других устройств аналогичных типов. Устройства в «белом списке» идентифицируются с точностью до модели и уникального экземпляра – с использованием его серийного номера. Также в DeviceLock поддержан «белый список» носителей: для каждого пользователя или группы можно идентифицировать индивидуальный CD/DVD-диск на основе записанных на него данных и разрешить его использование, даже если CD/DVD-привод заблокирован. Даже если с агентом DeviceLock невозможно установить сетевое соединение, пользователю можно обеспечить временный доступ к определенным периферийным устройствам, сообщив ему короткий буквенно-цифровой код разблокировки по телефону или иным средствам связи.

DeviceLock поддерживает разграничение операций обмена данными на уровне их типов: версия 6.4 продукта принципиально повышает уровень контроля за привилегиями и действиями пользователей за счет поддержки функции детектирования и фильтрации типов файлов для операций файловой системы. Используемый бинарно-сигнатурный метод позволяет определить тип файла по его реальному содержимому, а не по меткам или служебным метаданным - то есть, детектируется подлинная форма представления данных внутри файла. Технология обеспечивает распознавание более 3000 форматов и легко расширяема. DeviceLock 6.4 поддерживает перехват, экстракцию, детектирование типа и блокирование файловых объектов во всех локальных каналах потенциальной утечки данных на компьютерах: через любые устройства хранения информации, а также при локальной синхронизации с мобильными устройствами и смартфонами на базе Windows Mobile. Для любого из этих каналов DeviceLock позволяет не только устанавливать ограничения на типы передаваемых файлов, но и задавать гибкие избирательные политики событийного протоколирования, а также теневого копирования с точностью до типа файла.

Отличительной особенностью DeviceLock является способность фильтровать протоколы локальной синхронизации данных с любыми типами КПК и смартфонов под управлением ОС Windows Mobile® и Palm® OS вне зависимости от интерфейсов их подключения (USB, COM, IrDA, Bluetooth, WiFi). При этом обмен данными можно блокировать или разрешать на уровне типов объектов – таких, как файлы, контакты, почта, записи в календаре и т.д. С такой же гранулированностью поддерживается событийное протоколирование и теневое копирование операций локальной синхронизации.

Другая уникальная характеристика DeviceLock – поддержка централизованного контроля доступа пользователей к локальным, сетевым и виртуальным принтерам вне зависимости от интерфейса их подключения к компьютеру, включая любые не-USB интерфейсы. Для каждого отдельного компьютера в сети или их групп DeviceLock позволяет задать гибкие правила, определяющие кому, когда и на каких принтерах разрешено печатать. Разные прав доступа могут быть установлены к реальным (локальным и сетевым) и виртуальным принтерам – например, программам конвертации в PDF. Дополнительная степень гибкости достигается за счет возможности задать разные политики для принтеров, подключенных к разным интерфейсам: USB, LPT, Bluetooth, Wi-Fi. При подключении по USB разные правила доступа могут быть определены для каждой модели и каждого отдельного принтера.

В комплексе с несколькими популярными СКЗИ, включая продукты компаний Инфотекс, PGP, TrueCrypt и Lexar, DeviceLock позволяет предотвратить несанкционированный экспорт данных с корпоративных компьютеров на съемные устройства памяти в нешифрованном виде. Шифрование данных и все административные криптографические функции в таких интегрированных решениях реализуются совместимыми СКЗИ, а DeviceLock контролирует доступ пользователей к шифрованным и нешифрованным данным на внешних носителях. При этом DeviceLock распознает зашифрованные устройства хранения данных и позволяет централизованно устанавливать специальные права доступа к ним пользователей компьютера. С помощью таких политик можно, например, разрешить определенным пользователям запись только зашифрованных данных на съемные устройства и запретить запись незашифрованных данных. Одновременно и независимо от политик «шифрованного» доступа администратор безопасности может установить для тех же пользователей иные права доступа к нешифрованным съемным устройствам памяти, таким образом не ограничивая их штатное, в соответствии с установленной политикой ИБ организации, использование в служебных целях.

Гибкое и оперативное управление политиками доступа, протоколирования и теневого копирования агентов DeviceLock, установленных на защищаемых компьютерах, а также полным комплексом администрирования их жизненного цикла обеспечивается централизованно либо с выделенной платформы управления на базе одного или нескольких компонентов DeviceLock Enterprise Server, либо, если в организации используется платформа системного управления Microsoft Active Directory, через ее групповые политики (Group Policy Objects), для чего предоставляется специальная GPO-оснастка DeviceLock Group Policy Manager (GPM), полностью интегрированная в инфраструктуру Microsoft AD. Одно из принципиальных преимуществ DeviceLock GPM состоит в том, что его пользователи не должны выделять дополнительные финансовые и трудовые ресурсы на установку и эксплуатацию отдельной серверной платформы для управления агентами DeviceLock, и, что не менее важно, масштабируемость DeviceLock GPM полностью определяется масштабом развернутой в организации Microsoft AD, таким образом автоматически обеспечивая потребности владельца.

Кроме того, в DeviceLock поддержано полнофункциональное задание исполняемых на агентах политик контроля доступа в режиме offline, когда компьютер находится вне корпоративной сети или серверы управления недоступны. При этом переключение между режимами онлайн и офлайн осуществляется агентом DeviceLock автоматически.

Событийное протоколирование и теневое копирование являются столь же важными функциональными характеристиками комплекса DeviceLock, как и управление доступом к интерфейсам и устройствам, поскольку позволяют администрации ИБ отслеживать поведение пользователей и административного персонала, проводить централизованный аудит а также обеспечивать доказательную базу для расследования инцидентов ИБ и участия в судебных разбирательствах.

DeviceLock поддерживает детальное протоколирование действий пользователей и административного персонала а также теневое копирование с автоматическим централизованным сбором и хранением всех данных, копируемых с защищаемых компьютеров, в базе данных DeviceLock Enterprise Server. При этом политики сбора данных аудита и теневого копирования задаются централизованно с консоли DeviceLock Group Policy Manager или DeviceLock Enterprise Server – в зависимости от того, применяется ли у пользователя платформа Microsoft Active Directory. К уникальным преимуществам DeviceLock относится поддержка исполнительным агентом алгоритма автоматического выбора оптимального для передачи собранных протокольных данных на лог- сервер при наличии в системе нескольких таких серверов, а также возможность задать для агентов пределы пропускной способности (traffic shaping) канала передачи данных теневого копирования и лог-файлов в центральную базу данных.

Устанавливаемый на защищаемых компьютерах агент DeviceLock полностью защищен от удаления или выведения из строя в результате нештатных или деструктивных действий пользователей и локальных системных администраторов, а надежность, масштабируемость и высокое качество технической поддержки продукта подтверждены многолетней промышленной эксплуатацией в производственных условиях крупных российских и зарубежных организаций из самых разных отраслей экономики.

Возможности DeviceLock и требования ФЗ «О коммерческой тайне»

Продукт DeviceLock осуществляет контроль над перемещением 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 основным требованиям ФЗ «О коммерческой тайне»:

- Согласно пп. 2, п. 1, ст. 10, доступ к информации, составляющей коммерческую тайну, должен быть ограничен «путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка». Решение DeviceLock обеспечивает технический контроль распространения информации через локальные порты рабочей станции, беспроводные сети и принтеры, что позволяет минимизировать риск утечки информации, которая составляет коммерческую тайну;

- Согласно пп. 3, п. 1, ст. 10, обладатель информации должен проводить «учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана». DeviceLock предлагает уникальную функциональность – теневое копирование данных, покидающих корпоративную сеть через локальные порты рабочих станций, сменные носители, беспроводные сети и мобильные устройства. Таким образом, организация всегда знает, какая информация покинула ее корпоративную сеть, и какой сотрудник мог допустить утечку;

- Согласно п. 4, ст. 10 обладатель информации, составляющей коммерческую тайну, вправе применять технические средства защиты конфиденциальности такой информации. Являясь одним из таких средств, продукт DeviceLock обеспечивает контроль над передачей информации на съемные накопители, мобильные устройства, беспроводные сети и принтеры. Продукт DeviceLock разработан в России имеет необходимые сертификаты для использования в качестве средства защиты информации на территории РФ. DeviceLock может применяться для создания автоматизированных систем до класса защищенности 1Г включительно;

- Согласно п. 5, ст. 10 меры по обеспечению конфиденциальности информации, составляющей коммерческую тайну, должны быть разумно-достаточными. Это означает, что доступ третьих лиц к этой информации без согласия ее обладателя должен быть исключен, а работники и контрагенты должны иметь возможность доступа к ней без нарушения режима коммерческой тайны. Система DeviceLock минимизирует риски утечки информации через съемные носители, мобильные устройства, беспроводные сети и принтеры, что позволяет исключить доступ любых лиц к этой информации без согласия ее обладателя.

В таблице далее (таб. 3) представлены сводные сведения по функциональности DeviceLock в рамках обеспечения требований Федерального закона «О коммерческой тайне»:

Таб. 3. Функциональность DeviceLock применительно к требованиям Федерального закона «О коммерческой тайне»:

Требования ФЗ «О коммерческой тайне»	**DeviceLock**
Ст. 10, п.1, пп.2. Обладатель информации, составляющей коммерческую тайну, должен ограничить доступ к ней, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.	С помощью агента DeviceLock Service администратор системы может ограничить доступ к локальным портам компьютеров, беспроводным сетям и принтерам. Программное ограничение в данном случае эквивалентно аппаратному, поскольку доступ к агенту могут получить только специально авторизованные администраторы. Таким образом, решение DeviceLock обеспечивает порядок обращения с информацией на рабочих станциях и контролирует соблюдение такого порядка.
Ст. 10, п.1, пп.3. Обладатель информации, составляющей коммерческую тайну, должен проводить учет лиц, получивших доступ к информации […] и (или) лиц, которым такая информация была предоставлена или передана.	Продукт DeviceLock имеет развитую функцию теневого копирования, которая не только протоколирует все попытки передачи данных на внешние устройства, но и копирует переданную информацию в специальную базу данных. Вместе с каждым событием в базе сохраняется подробная информация о нем (время события, тип канала передачи, идентификатор пользователя и другие параметры). Таким образом, с помощью DeviceLock администратор системы всегда будет иметь исчерпывающую событийную информацию о перемещении данных компании через локальные порты и интерфейсы рабочих станций, удобную для аудита, а также анализа и сбора доказательной базы при проведении расследований инцидентов информационной безопасности.
Ст. 14, п.2. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, […], в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации	
Ст. 10, п.4. Обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации/	DeviceLock является одним из средств технической защиты и имеет необходимые сертификаты для использования на территории РФ (может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно). Таким образом, DeviceLock может применяться для защиты информации, составляющей коммерческую тайну.

Ст. 10, п.5. Меры по охране конфиденциальности информации признаются разумно достаточными, если: а) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя; б) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.	Осуществляя контроль над портами рабочих станций, беспроводными сетями и принтерами, продукт DeviceLock минимизирует риски утечки информации, составляющей коммерческую тайну. Тем самым вероятность доступа третьих лиц к этой информации существенно уменьшается. При этом система DeviceLock никак не ограничивает работу пользователей с информацией, составляющей коммерческую тайну, в пределах локальной рабочей станции.
Ст. 11, п.1, пп.3. В целях охраны конфиденциальности информации работодатель обязан создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.	Продукт DeviceLock технически контролирует порты рабочих станций, беспроводные сети и принтеры. Тем самым, сокращаются риски непреднамеренной утечки информации по этим каналам. Таким образом, DeviceLock обеспечивает соблюдение установленного на предприятии режима коммерческой тайны.
Ст. 13, п.1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим […] обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателям.	Поскольку продукт DeviceLock помогает достичь соответствия ряду требований ФЗ и имеет необходимые сертификаты (см. выше), он может применяться для обеспечения режима коммерческой тайны в государственных органах и органах местного самоуправления. В настоящее время система DeviceLock успешно используется в ряде государственных учреждений, обеспечивая защиту конфиденциальной информации юридических лиц и индивидуальных предпринимателей.

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 58 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 4 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силовые 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) 967-99-60, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@devicelock.com

Тех. поддержка: support@devicelock.com