

DeviceLock для соответствия законам о персональных данных



Оглавление:

- [Введение](#)
- [Анализ требований законов о персональных данных](#)
 - [Закон SB 1386 \(Калифорния, США\)](#)
 - [Data Protection Directive \(ЕС\)](#)
 - [Directive on privacy and electronic communications \(ЕС\)](#)
 - [Data Protection Act \(Великобритания\)](#)
 - [ФЗ «О персональных данных» \(Россия\)](#)
 - [Act on the Protection of Personal Information \(Япония\)](#)
 - [Privacy Act 1988 \(Австралия\)](#)
 - [PIPEDA \(Канада\)](#)
 - [Выводы](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock для защиты персональных данных](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Каждое государство сегодня имеет свои собственные нормативные акты для защиты персональных данных граждан от утечки, разглашения и неавторизованного использования. Область действия таких законов включает в себя абсолютно все организации, действующие на территории данной страны. Таким образом, международные и глобальные компании вынуждены иметь политики и процедуры для защиты персональных данных и соответствия нормативным актам для каждой страны.

Кроме того, с проблемой обеспечения безопасности персональных данных в контексте различных законов сталкиваются и локальные компании. Сегодня нормативные акты по защите персональных сведений существуют в США, Канаде, Евросоюзе, а также в Японии, Австралии и т.д. Более того, различные законы действуют в различных штатах внутри США и в различных государствах внутри ЕС. Другими словами, даже те организации, которые не выходят в своей деятельности за рамки государства или экономического союза, вынуждены учитывать различные нормативные требования в сфере обеспечения безопасности персональных данных.

В данном документе будут проанализированы требования законов в сфере защиты персональных данных таких стран как США, ЕС, Канада, Япония, Австралия, Россия. Отдельное внимание будет уделено нормативным актам Великобритании и штату Калифорния, США. Кроме того, будут рассмотрены возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия всем вышеупомянутым законам.

Анализ требований законов о персональных данных

Наибольшие трудности при защите персональных данных в соответствии с нормативными требованиями испытывают крупные организации, ведущие операции на рынках нескольких стран. В этом случае бизнесу приходится иметь дело с требованиями сразу целого ряда законов. В таблице ниже (см. таб. 1) перечислены основные нормативные акты о защите персональных данных.

Таб. 1. Национальные законы о персональных данных	
Страна	Нормативный акт
США	Федеральный закон еще не принят. Многие штаты имеют свои собственные законы. В качестве эталона следует рассмотреть закон SB 1386 (Калифорния).
Евросоюз	Data Protection Directive , Privacy and Electronic Communication Regulation
Британия	Data Protection Act
Россия	Федеральный закон « О персональных данных »
Япония	Personal Information Protection Act 2003
Австралия	The Federal Privacy Act (Privacy Act 1988)
Канада	Personal Information Protection and Electronic Document Act (PIPEDA)

Отметим, что помимо этих законов практически в каждой стране существуют специализированные нормативные акты, область действия которых включает компании, работающие в определенных секторах экономики. Например, в США закон HIPAA требует от организаций защищать персональные медицинские сведения граждан, а закон GLBA предписывает обеспечить безопасность персональных финансовых записей. Однако использование DeviceLock позволяет обеспечить совместимость, в том числе, и с этими законами и нормативными актами. Подробнее об этом смотрите в соответствующих white papers.

Закон SB 1386 (Калифорния, США)

Данный закон штата Калифорния вступил в силу 1 июля 2003 года. Согласно секции 2 закона SB 1386, секция 1798.29 Гражданского Кодекса дополняется следующими пунктами:

(a) Любая организация, которая владеет персональными компьютерными данными или лицензирует их, обязана оповестить всех резидентов штата Калифорния об утечке или потенциальной утечке их персональных данных в незашифрованном виде. Сделать это следует немедленно – сразу же после того, как утечка будет выявлена.

(b) Любая организация, имеющая персональные компьютерные данные граждан, но не владеющая ими, должна незамедлительно уведомить об утечке или потенциальной утечке этих данных владельца или лицо, которое эту информацию лицензировало.

(c) Организация может отложить уведомление, требуемое предыдущими секциями, только по распоряжению правоохранительных органов, проводящих расследование.

(d) Под «утечкой» понимается неавторизованное использование компьютерных данных, вследствие которого нарушается безопасность, конфиденциальность или целостность персональной информации, находящейся на попечении организации. Добросовестное использование персональных данных служащими или представителями организации в целях организации не является утечкой.

(e) Под персональными или приватными данными следует понимать имя гражданина в комбинации с одной или несколькими следующими записями: номер социального страхования, водительского удостоверения или Калифорнийской идентификационной карты, номер счета, кредитной или дебитной карты в комбинации с кодом

безопасности, доступа или паролем, которые позволяют получить доступ к банковскому счету гражданину. Кроме того, эти данные должны быть не зашифрованы.

Таким образом, закон SB 1386 напрямую не предписывает защищать персональные данные граждан. Однако он требует оглашать все случаи утечки этой информации. Следовательно, организация, допустившая утечку, не сможет замолчать инцидент и обязательно столкнется с его отрицательными последствиями. А именно: понижением репутации, ухудшением общественного мнения о компании, оттоком клиентов и т.д. Кроме того, закон SB 1386 позволяет любому резиденту штата Калифорния, который пострадал вследствие утечки, подать гражданский иск против организации, допустившей утечку, и потребовать возмещения убытков. Другими словами, потери вследствие утечки могут возрасти многократно. Именно поэтому бизнес нуждается в решениях для выявления и предотвращения утечек персональных данных.

Data Protection Directive (EC)

Директива о защите данных была принята Евросоюзом в 1995 году. Она защищает персональные сведения граждан – так называемую персонально идентифицирующую информацию (Personal Identifiable Information – PII). Директива обязывает каждое государство, входящее в состав ЕС, принять свой собственный закон о защите персональных сведений, совместимый с рекомендациями ОЭСР¹ от 1980 года. Среди этих рекомендаций стоит отметить Принцип гарантированной безопасности №11 (Security Safeguards Principle 11), который требует, чтобы «персональные данные были защищены разумными средствами безопасности от таких угроз, как утрата или неавторизованный доступ, разрушение, использование, модификация или утечка». Кроме того, эти требования закреплены в статье 17 секции VIII главы 2 Директивы о защите данных.

Отметим, что Директива Евросоюза также вводит классификацию личных данных (медицинские, финансовые и т.п.). Каждая категория таких данных требует дополнительных мер безопасности ввиду ее конфиденциальной природы. Более того, требования Директивы ЕС являются довольно жесткими. В частности организации обязаны защищать персонально идентифицирующую информацию (PII) как клиентов компании, так и сотрудников. Вдобавок, Директива запрещает передавать персональные данные в страны, где законы, защищающие конфиденциальность, не адекватны аналогичным актам в Евросоюзе.

Директива не определяет, какие конкретно технические решения следует использовать для защиты персональных данных странам. Так что членам ЕС дана достаточная свобода, чтобы урегулировать этот вопрос самостоятельно. Например, законодательство Италии требует от представителей бизнеса защищать данные с помощью межсетевых экранов и антивируса, а в Испании некоторые виды персональных данных должны храниться в зашифрованном виде.

Однако, в любом случае нарушение Директивы Евросоюза может повлечь наступление гражданской и уголовной ответственности, включая большие штрафы, а в некоторых странах даже лишение свободы.

¹ В состав ОЭСР (Организации экономического сотрудничества и развития) входят 30 стран (Россия не входит): Австралия, Австрия, Бельгия, Канада, Чехия, Дания, Финляндия, Франция, Германия, Греция, Венгрия, Исландия, Ирландия, Италия, Япония, Корея, Люксембург, Мексика, Нидерланды, Новая Зеландия, Норвегия, Польша, Португалия, Словакия, Испания, Швеция, Швейцария, Турция, Великобритания, США.

Directive on privacy and electronic communications (EC)

[Директива Евросоюза о приватности и электронных коммуникациях](#) была принята 12 июля 2002 года. Она закрепляет положения предыдущей директивы относительно безопасности и конфиденциальности персональных сведений граждан в электронной форме при передаче по сетям связи.

20 пункт Директивы ЕС требует, чтобы поставщики коммуникационных услуг принимали разумные меры для обеспечения безопасности своих сервисов. Кроме того, провайдеры обязаны за свои собственные средства внедрять технологические и другие решения, призванные минимизировать риски IT-безопасности. Согласно 21 пункту, поставщики услуг должны предотвратить неавторизованный доступ к коммуникационным каналам, чтобы обеспечить конфиденциальность пересылаемых по сети данных. Более того, особое внимание следует обратить на «внутренний неавторизованный доступ» к каналам связи. Наконец, 26 пункт Директивы ЕС предписывает провайдерам защищать всю информацию, которая относится к частной и приватной жизни клиентов. Это не только пересылаемая по сети корреспонденция, но и любые другие личные сведения. Помимо этого, персональные данные граждан нельзя использовать в маркетинговых целях, если не получить на то согласие самих клиентов.

Data Protection Act (Великобритания)

Британский закон о защите данных был принят в 1998 году. Он защищает персональные сведения и критичные личные данные граждан. К первой категории, согласно пункту 1 части I, относится любая информация живого человека, по которой его можно идентифицировать. Ко второй категории (чувствительные персональные данные) относятся сведения о политических взглядах, вероисповедании, расе, членстве в профсоюзе, физическом и умственном состоянии, сексуальной жизни и судимостях гражданина. В соответствии с этими категориями в законе предусмотрены два отдельных приложения (schedules), определяющих, когда возможна обработка данных. Schedule 2 покрывает обработку всех персональных сведений, а Schedule 3 только чувствительных персональных данных. Однако наибольший интерес представляет первое приложение «The Data Protection Principles».

Часть 1 этого приложения содержит основные принципы по защите данных. Согласно 7 принципу, организации должны «принимать разумные технические и организационные меры против неавторизованной или незаконной обработки и случайной потери персональных данных или их уничтожения или повреждения».

Часть 2 этого приложения содержит разъяснения к принципам, изложенным в предыдущей части. В комментариях к 7 принципу говорится (приложение 1, часть 2, пункт 9), что организации должны реализовать разумные технические меры, чтобы предотвратить ущерб своим клиентам в результате неавторизованной или незаконной обработки персональных данных, а также их потери, уничтожения или повреждения.

Более того, 10 пункт этого приложения требует: «Организация должна сделать разумные шаги, чтобы обеспечить надежность любого служащего, имеющего доступ к персональным данным».

Наконец, рассмотрим ответственность за нарушение закона. Согласно пункту 55 части IV, лицо, которое распространяет чужую персональную информацию без разрешения граждан, нарушает закон и должно быть привлечено к ответственности. Кроме того, предусмотрена ответственность для организаций, нарушающих требования закона к защите персональных данных.

ФЗ «О персональных данных» (Россия)

27 июля 2006 года в России был принят закон N152-ФЗ «[О персональных данных](#)». В сферу действия этого нормативного акта попадают все юридические и физические лица, на попечении которых находятся персональные сведения других граждан. Новый закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов, партнеров и т.д., обеспечила конфиденциальность всей этой информации. В случае нарушения положений закона компания может лишиться лицензии и подвергнуться судебному преследованию со стороны граждан, чьи персональные записи были скомпрометированы. Кроме того, виновные лица, нарушившие требования закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

ФЗ «О персональных данных» предъявляет требования к мерам IT-безопасности, которые должны быть предприняты для защиты личных сведений. Согласно ст.19 ч.1, оператор данных «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». Другими словами, бизнесу необходимо обеспечить мониторинг всех операций, которые инсайдеры осуществляют с персональными данными клиентов и служащих. Более того, это должен быть активный мониторинг, то есть такой, который позволяет заблокировать действия, нарушающие политику безопасности.

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 за 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».

Act on the Protection of Personal Information (Япония)

Японский закон о защите персональной информации был принят 30 мая 2003 года и полностью вступил в силу с 1 апреля 2005 года. Нормативный акт ставит своей целью защитить персональные сведения граждан в быстро развивающемся мире электронных коммуникаций и информационных систем. Проблеме безопасности персональной информации в законе посвящена вся третья глава «Measures for the Protection of Personal Information, etc». Согласно 7 статье 3 главы, Правительство Японии должно разработать Базовую политику безопасности персональной информации. Эта политика должна предусматривать меры, которые должно принимать государство, органы местного самоуправления и организации для защиты персональных данных граждан. Таким образом, японские организации находятся в довольно жестких рамках и обязаны соответствовать требованиям Базовой политики.

Кроме того, 20 статья («Security Control Measures») предъявляет требования именно к IT-безопасности: «Любая организация, на попечении которой находится персональная информация, должна принять необходимые и адекватные меры, чтобы предотвратить утечку, потерю или повреждение персональных данных, а также для осуществления другого контроля над безопасностью этой информации».

Следующая статья (21) посвящена конкретно проблеме инсайдеров: «Когда организация, на попечении которой находится персональная информация, использует служащих для обработки этих данных, она должна внедрить необходимые и адекватные меры наблюдения и контроля, чтобы обеспечить безопасность персональной информации». Другими словами, японский закон однозначно требует от бизнеса и госструктур внедрить систему защиты от инсайдеров и утечек данных.

Privacy Act 1988 (Австралия)

Австралийский федеральный закон о персональных данных был принят в 1988 году. Последние изменения с учетом развития вычислительных сетей и перевода информации в электронный вид были внесены в октябре 2006 года. При этом в Уголовный Кодекс Австралии сразу же были добавлены положения, предусматривающие ответственность за нарушение Privacy Act 1988.

Австралийский закон предусматривает целый ряд принципов приватности. Согласно 4 принципу, организация, на попечении которой находятся личные сведения граждан, должна убедиться, что эта информация защищена от утечки, потери, неавторизованного доступа, использования, модификации и другого злоупотребления. Кроме того, организация обязана предусмотреть средства контроля над тем, чтобы доступ к информации и полномочия по ее использованию имели только те работники, которым это необходимо в силу служебных обязанностей.

Согласно другим принципам приватности, организация обязана предоставить гражданину доступ к его персональным данным, использовать эту информацию только в законных целях и т.д. Другими словами, все возможные сферы и способы использования личных сведений регламентируются австралийским законом.

Таким образом, Privacy Act 1988 напрямую указывает на необходимость защиты персональных данных, предотвращения утечек и злоупотреблений со стороны персонала организаций.

PIPEDA (Канада)

Канадский закон о защите персональной информации и электронных документах (Personal Information Protection and Electronic Document Act) призван защитить персональные сведения граждан, используемые, в основном, в электронной коммерции. Закон выдвигает требования к безопасности персональных данных и предусматривает процедуры, согласно которым граждане могут пожаловаться на организацию, нарушающую положения закона. Уполномоченные государством лица могут провести аудит практик управления персональной информацией в организации, а в случае выявления нарушений привлечь ее к ответственности.

Требования к безопасности персональных сведений сгруппированы в первом приложении (Schedule 1) закона PIPEDA. Согласно принципу 4.1, каждой организации, на попечении которой находятся персональные данные граждан, рекомендуется назначить ответственное лицо, которое будет следить за безопасностью этой информации и соблюдением положений приватности. Кроме того, принцип 4.1 не снимает с организации ответственность за сохранность личных сведений граждан в том случае, если эта информация передается третьим лицам в рамках аутсорсинга. Наконец, согласно пункту 4.1.4(а), каждой организации рекомендуется разработать и внедрить политики и процедуры по защите персональных данных граждан.

Еще один принцип (пункт 4.7) предписывает организациям принимать меры безопасности для защиты персональной информации в соответствии с уровнем ограничения доступа к ней. Согласно пункту 4.7.1, эти меры безопасности должны защитить персональные

данные от утечки, потери или кражи, неавторизованного доступа, копирования, использования или модификации. При этом организации должны защитить персональную информацию независимо от того формата, в котором она хранится. Следующий пункт (4.7.3) требует, чтобы методы безопасности включали в себя физические, организационные и технические меры. Наконец, пункт 4.7.4 посвящен проблеме инсайдеров – организации должны донести важность сохранения конфиденциальности личных сведений до своих служащих.

Выводы

Таким образом, каждый проанализированный национальный закон требует от организаций обеспечить конфиденциальность персональных данных, предотвратить утечку и злоупотребления со стороны инсайдеров. В таблице ниже (см. таб. 2) просуммированы основные требования к IT-безопасности в разобранных нормативных актах.

Таб. 2. Основные требования законов к IT-безопасности	
Нормативный акт	Требования
Закон SB 1386 (Калифорния, США)	Секция 2(а): «Любая организация, которая владеет персональными компьютерными данными или лицензирует их, обязана оповестить всех резидентов штата Калифорния об утечке или потенциальной утечке их персональных данных в незашифрованном виде. Сделать это следует немедленно – сразу же после того, как утечка будет выявлена».
Data Protection Directive (Евросоюз)	Статья 17 секция VIII глава 2: «Персональные данные [должны быть] защищены разумными средствами безопасности от таких угроз, как утрата или неавторизованный доступ, разрушение, использование, модификация или утечка».
Privacy and Electronic Communication Regulation (Евросоюз)	<p>Пункт 20: Поставщики коммуникационных услуг должны принимать разумные меры для обеспечения безопасности своих сервисов. Кроме того, провайдеры обязаны за свои собственные средства внедрять технологические и другие решения, призванные минимизировать риски IT-безопасности.</p> <p>Пункт 21: Поставщики услуг должны предотвратить неавторизованный доступ к коммуникационным каналам, чтобы обеспечить конфиденциальность пересылаемых по сети данных. Более того, особое внимание следует обратить на «внутренний неавторизованный доступ» к каналам связи.</p>
Data Protection Act (Великобритания)	<p>Приложение 1, часть 1, принцип 7: Каждая организация должна «принимать разумные технические и организационные меры против неавторизованной или незаконной обработки и случайной потери персональных данных или их уничтожения или повреждения».</p> <p>Приложение 1, часть 2, пункт 9: Каждая организация должна реализовать разумные технические меры, чтобы предотвратить ущерб своих клиентов в результате неавторизованной или незаконной обработки персональных данных, а также их потери, уничтожения или повреждения. Вдобавок, каждая организация должна сделать разумные шаги, чтобы обеспечить надежность любого служащего, имеющего доступ к персональным данным».</p>

<p>Федеральный закон «О персональных данных» (Россия)</p>	<p>Ст.19 ч.1: «Оператор [персональных данных] 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».</p> <p>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».</p> <p>Ст.19 ч.4: «использовать и хранить биометрические персональные данные [разрешено] 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».</p>
<p>Personal Information Protection Act 2003 или PIPA (Япония)</p>	<p>Ст. 20: «Любая организация, на попечении которой находится персональная информация, должна принять необходимые и адекватные меры, чтобы предотвратить утечку, потерю или повреждение персональных данных, а также для осуществления другого контроля над безопасностью этой информации».</p> <p>Ст. 21: «Когда организация, на попечении которой находится персональная информация, использует служащих для обработки этих данных, она должна внедрить необходимые и адекватные меры наблюдения и контроля, чтобы обеспечить безопасность персональной информации».</p>
<p>The Federal Privacy Act или Privacy Act 1988 (Австралия)</p>	<p>Принцип 4: Каждая организация, на попечении которой находятся личные сведения граждан, должна убедиться, что эта информация защищена от утечки, потери, неавторизованного доступа, использования, модификации и другого злоупотребления. Кроме того, организация обязана предусмотреть средства контроля над тем, чтобы доступ к информации и полномочия по ее использованию имели только те работники, которым это необходимо в силу служебных обязанностей.</p>
<p>Personal Information Protection and Electronic Document Act или PIPEDA (Канада)</p>	<p>Приложение 1, принцип 4: Каждой организации, на попечении которой находятся персональные данные граждан, рекомендуется назначить ответственное лицо, которое будет следить за безопасностью этой информации и соблюдением положений приватности.</p> <p>Пункт 4.1.4(а): Каждой организации рекомендуется разработать и внедрить политики и процедуры по защите персональных данных граждан.</p> <p>Пункт 4.7: Каждой организации рекомендуется принимать меры безопасности для защиты персональной информации в соответствии с характером ее чувствительности.</p> <p>Пункт 4.7.1: Эти меры безопасности должны защитить персональные данные от утечки, потери или кражи, неавторизованного доступа, копирования, использования или модификации.</p>

DeviceLock может помочь достичь соответствия с этими нормативными требованиями гораздо более эффективно, о чем и пойдет речь в следующей главе.

DeviceLock от Смарт Лайн Инк

Продукт DeviceLock разработан российской компанией ЗАО «Смарт Лайн Инк» и предназначен для корпоративных пользователей. С помощью DeviceLock организации

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 бизнесе. Кроме того, нельзя сбрасывать со счетов приближающуюся консьюмеризацию корпоративных IT-систем. Авторитетные исследовательские агентства Yankee Group и CSC Research утверждают, что директора и менеджеры IT-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 консьюмеризация 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 организации от утечки персональных и финансовых сведений, 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 обеспечивает необходимую гибкость политики ИТ-безопасности 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 тремя консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

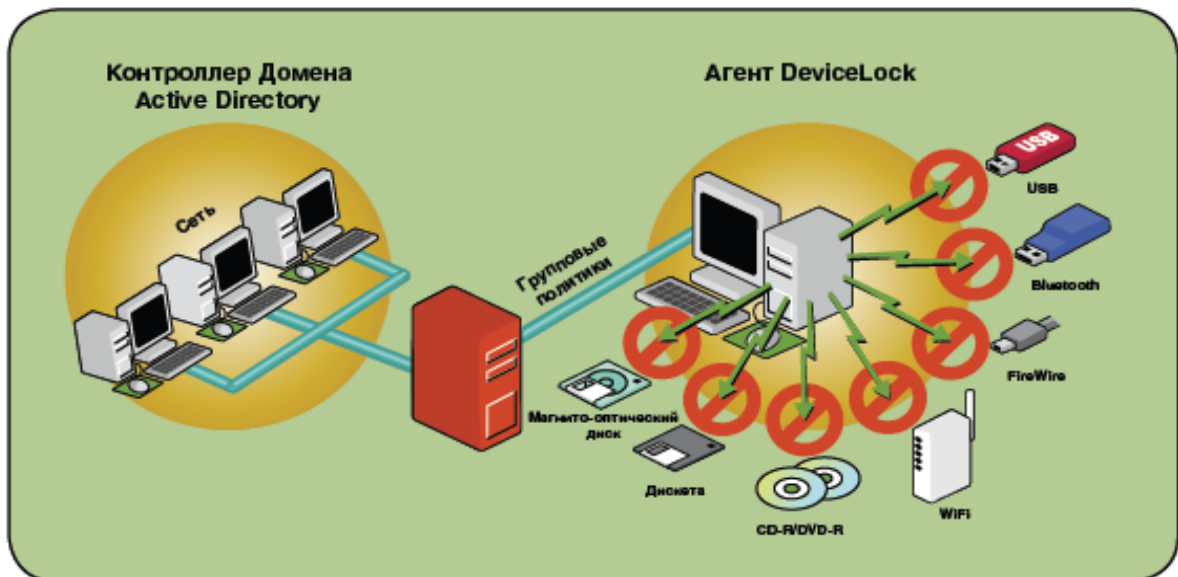


Рис. 1. Схема работы DeviceLock

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 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 ИТ-безопасности.

Использование DeviceLock в корпоративной среде позволяет обеспечить соответствие двум основным требованиям, которые чаще всего встречаются в законах о защите персональных данных:

- Персональные данные должны быть защищены от утечек, разглашения, несанкционированного доступа и использования. Именно для решения этой задачи

полезен DeviceLock, который позволяет минимизировать риски утечки через сменные носители, мобильные устройства и беспроводные сети, что является неотъемлемым требованием при обеспечении безопасности персональных данных.

- Организации обязаны своевременно обнаруживать факты «несанкционированного доступа к персональным данным» и, согласно некоторым нормативным актам, оповещать пострадавших. Отсюда следует, что 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 продукт DeviceLock, обеспечивающий теневое копирование данных, экспортируемых с ПК на сменные носители и мобильные устройства, а также отправляемых на принтер. Анализируя собранную информацию, можно легко определить, где, когда, каким способом и как произошла утечка.

В таблице далее (см. таб. 3) просуммирована функциональность DeviceLock в соответствии с нормативными требованиями.

Таб. 3. Функциональность DeviceLock применительно к национальным законам о персональных данных		
Страна	Требования законов	Возможности DeviceLock
Евросоюз, Великобритания, Япония, Россия, Канада	Каждая организация, на попечении которой находятся персональные данные граждан, должна принимать разумные меры (организационные, технические и т.д.) для защиты этой информации.	Одной из таких необходимых технических мер является использование продукта DeviceLock, при помощи которого организация, у которой имеются персональные данные, может минимизировать риски несанкционированного копирования или распространения этой информации, неправомерного или случайного доступа к ней со стороны неуполномоченных лиц.
Великобритания, Япония, Россия, Австралия, Канада	Каждая организация, владеющая персональными данными граждан, должна предотвратить утечку этой информации и злоупотребления именно со стороны своих собственных служащих.	Утечка информации является одной из самых опасных угроз, выделяемой отдельно, практически, каждым нормативным актом. Значительно снизить 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.

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 50 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 2 000 000 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) 967-99-60, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@smartline.ru

Тех. поддержка: support@smartline.ru