

DeviceLock для соответствия законам GLBA и FACTA



Оглавление:

- [Введение](#)
- [Требования законов GLBA и FACTA](#)
- [Программа информационной безопасности](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock для GLBA и FACTA](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Защита любых персональных данных клиентов, находящихся в информационной системе финансовой компании, регулируется в США двумя основными законами GLBA (Gramm-Leach-Bliley Act of 1999) и FACTA (Fair and Accurate Credit Transactions Act of 2003). Оба нормативных акта ставят своей целью защитить финансовые сведения граждан от утечки, а также злоупотреблений и, тем самым, затруднить кражу личных идентификационных данных и другие виды мошенничества.

В рамках GLBA и FACTA надзорные органы США разработали ряд специальных стандартов – «[Interagency Guidelines Establishing Information Security Standards](#)» (далее просто Security Guidelines). Эти стандарты конкретизируют и уточняют требования GLBA и FACTA в сфере защиты чувствительных данных клиентов. В соответствии с Security Guidelines, финансовые компании обязаны принять административные, технические и физические меры безопасности, чтобы гарантировать безопасность, конфиденциальность, целостность и правильное уничтожение информации клиентов. Требования Security Guidelines вступили в силу 1 июля 2005 года.

В данном документе будут рассмотрены требования GLBA и FACTA (Security Guidelines), которые влияют на информационную инфраструктуру финансовых компаний и используемые в ней средства безопасности, а также возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия GLBA и FACTA.

Требования законов GLBA и FACTA

Под действие GLBA и FACTA попадают все компании, которые так или иначе связаны с финансовой деятельностью и, следовательно, имеют доступ к финансовой информации граждан. Это в первую очередь банки, страховые, брокерские компании, центры обработки транзакций.

Требования Security Guidelines регулируют в частности не только хранение и использование чувствительных финансовых сведений в компаниях, но еще и перемещение этих данных между различными юридическими лицами, что особенно актуально в свете того, что частная финансовая информация клиентов служит объектом купли-продажи между банками, кредитными и страховыми компаниями.

Чтобы минимизировать все риски, связанные с утечкой частных финансовых сведений и злоупотребления ими, стандарты Security Guidelines требуют обеспечить безопасность персональной финансовой информации во время ее хранения или пересылки. В целом, в Security Guidelines закреплены все требования к безопасности подлежащих защите персональных сведений, которые должны выполнять финансовые компании в соответствии с секцией 501(b) закона GLBA и секцией 216 закона FACTA.

Отметим, что в соответствии с Security Guidelines финансовые институты обязаны обеспечить безопасность информации граждан (consumer information) вне зависимости от того, являются ли они клиентами данной компании.

Остановимся на самом термине – информация клиентов (consumer information). Под ним понимается, например, кредитный отчет, в котором указаны следующие сведения. Во-первых, гражданин, который подавал заявку, но не получил кредит. Во-вторых, гражданин, который гарантирует возврат кредита. В-третьих, служащий или, в-четвертых, потенциальный служащий. Финансовый институт должен требовать от своих поставщиков услуг при заключении контракта, чтобы они разработали и внедрили соответствующие меры для надлежащего хранения и использования информации.

По определению Security Guidelines, информация клиентов – это любые записи, содержащие непубличную персональную информацию индивида, который приобрел у данной компании финансовый продукт или финансовую услугу, использующиеся преимущественно для личных, семейных или семейно-хозяйственных целей, и который установил продолжающиеся отношения с финансовым институтом.

Чтобы защитить информацию клиентов, финансовая компания обязана разработать и внедрить программу безопасности (information security program). Это письменный план, созданный для того, чтобы выявить и взять под контроль риски по отношению к информации клиентов, а также, чтобы обеспечить надлежащее уничтожение этих данных. План включает политики и процедуры, касающиеся оценки риска, средств внутреннего контроля, тестирования, контроля над поставщиками услуг, периодической проверки и обновления принимаемых мер, а также отчетности совету директоров.

Программа информационной безопасности

Параграфы II.A-B стандарта Security Guidelines требуют от финансового института разработать и внедрить программу информационной безопасности, включающую административные, технические и физические меры безопасности, предназначенные для достижения следующих целей:

- Гарантировать безопасность и конфиденциальность информации клиентов;
- Защитить информацию клиентов от любых прогнозируемых угроз или рисков по отношению к безопасности или целостности;
- Защитить информацию клиентов от неавторизованного доступа и использования, если реализация этих угроз может причинить существенный вред или существенное неудобство любому клиенту; и
- Гарантировать надлежащее уничтожение информации клиентов.

Реализация программы информационной безопасности начинается с проведения оценки наиболее вероятных рисков. Точно так же, как и другие элементы программы безопасности, процедуры оценки рисков, анализ угроз и все полученные результаты должны быть оформлены в письменном виде.

Согласно стандарту Security Guidelines оценка рисков должна включать следующие шаги:

- Идентификация наиболее вероятных внутренних и внешних угроз, которые могут привести к неавторизованному разглашению (утечке), неправильному использованию, искажению или уничтожению информации клиентов или системы информации клиентов;

- Оценка вероятности и потенциального ущерба выявленных рисков с учетом уровня чувствительности (конфиденциальности) информации клиентов;
- Оценка достаточности политик, процедур, систем защиты информации клиентов и других мероприятий, используемых для контроля над выявленными рисками; и
- Реализация всех предшествующих шагов с учетом надлежащих мест и условий хранения информации клиентов.

Требования стандарта включают список мер безопасности, которые должны быть рассмотрены финансовым институтом и, в случае необходимости, внедрены. Следующие средства безопасности перечислены в параграфе III.C.1.a-h стандарта Security Guidelines:

- Контроль доступа к системам информации клиентов, включая средства аутентификации и разрешения доступа только для авторизованных пользователей, а также средства контроля над действиями служащих, чтобы исключить попадание информации клиентов к неавторизованным лицам (что может привести к мошенничеству);
- Ограничения на доступ к физическому месторасположению информации клиентов, например, на вход в здание, центры данных, хранилища записей и т.д. Только авторизованные лица должны иметь доступ в такие помещения.
- Шифрование информации клиентов, представленной в электронной форме, включая шифрование во время передачи и хранения данных в сетях и системах, к которым могут иметь доступ неавторизованные лица;
- Процедуры, гарантирующие, что изменения системы информации клиентов проходят в соответствии с программой IT-безопасности;
- Процедуры двойного контроля, разделение обязанностей, проверка прошлого тех служащих, которые имеют доступ к информации клиентов в силу должностных полномочий;
- Системы мониторинга и процедуры, позволяющие выявить реальную атаку и попытку атаковать, а также вторжение в системы информации клиентов;
- Программы ответных действий, которые определяют действия в случае, если финансовый институт выявит или заподозрит, что неавторизованные лица получили доступ к системам информации клиентов, включая обращение в надзорные и правоохранительные органы; и
- Средства защиты от уничтожения, потери или повреждения информации клиентов вследствие стихийных бедствий и аналогичных опасностей, например пожара, затопления, технологических проблем.

В заключение отметим, что совет директоров или соответствующий комитет должны убедиться в том, что программа информационной безопасности организации разработана, внедрена и поддерживается под управлением ответственных лиц. При этом совет или комитет должны утвердить письменную программу безопасности. Кроме того, согласно параграфу III.A совет или комитет должны получать отчеты о внедрении программы и периодически проверять достигнутые результаты.

В то же время менеджмент должен отчитываться перед советом или соответствующим комитетом, как минимум, ежегодно, чтобы описать результаты, достигнутые по программе безопасности, и подтвердить соответствие стандарту Security Guidelines.

Согласно параграфу III.F в отчете, который менеджмент предоставляет совету директоров, должны быть отражены такие моменты, как: проводит ли институт оценку рисков самостоятельно или нанимает внешнего консультанта, достигнутые с поставщиком услуг соглашения, результаты тестирования, выявленные бреши безопасности и нарушения политик, рекомендации по изменению программы информационной безопасности.

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 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 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 теньевые 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.

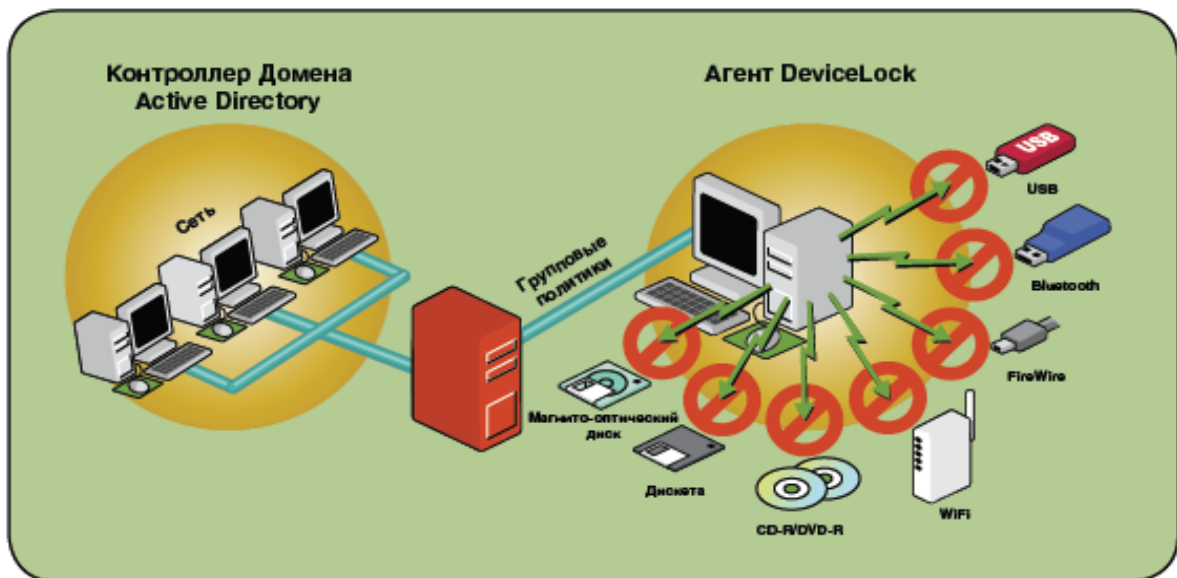


Рис. 1. Схема работы DeviceLock

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

Возможности DeviceLock для GLBA и FACTA

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 Security Guidelines:

- Стандарт требует обеспечить контроль над тем, что служащие компании делают с персональными финансовыми данными клиентов (III.C.1.a-h). Другими словами, необходимо обеспечить защиту от утечки этой информации и злоупотребления ею. В данном контексте DeviceLock выполняет функции необходимого элемента системы внутреннего контроля, при помощи которого обеспечивается управление доступом к локальным портам и интерфейсам и к типам синхронизируемых данных. Эффективное применение DeviceLock существенно снижает риск неконтролируемой утечки и позволяет письменно зафиксировать это в программе безопасности.
- Стандарт требует оповещать пострадавших в случае утечки информации клиентов. Другими словами, финансовая компания обязана иметь механизмы выявления утечки. В противном случае предприятие может столкнуться с большими штрафами и отзывом лицензии. На помощь приходит продукт DeviceLock, обеспечивающий теневое копирование данных на сменные носители и мобильные устройства. Анализируя собранную информацию, можно легко определить, где, когда, каким способом и как произошла утечка. Более того, компания сможет узнать, какие конкретно сведения скомпрометированы, и оповестить только идентифицированных клиентов, а не всю клиентскую базу.

В таблице далее (см. таб. 1) просуммирована функциональность DeviceLock в соответствии с требованиями Security Guidelines.

| Таб. 1. Функциональность DeviceLock применительно к требованиям GLBA и FACTA | |
|---|---|
| Требования | Возможности DeviceLock |
| Разработка комплексной программы информационной безопасности | Комплексная программа предполагает, что компания должна взять под контроль риски внутренней информационной безопасности. Т.е. минимизировать угрозу утечки персональных данных клиентов или злоупотребления этими сведениями со стороны внутренних нарушителей. Использование продукта DeviceLock позволяет управлять рисками утечки, что дает финансовой компании достаточные основания, чтобы письменно отразить в разработанной программе этот факт. |

| | |
|--|---|
| Идентификация рисков, оценка угроз и потенциального ущерба | Многие компании пытаются не замечать угрозы со стороны внутренних нарушителей. Однако игнорирование риска утечки персональных финансовых сведений клиентов или злоупотребление ими вряд ли можно считать рациональным шагом. Например, утечка частной информации клиентов обходится компании в сотни тысяч долларов прямого убытка, многомиллионные штрафы со стороны регулятора и приводит к навсегда испорченной репутации. DeviceLock помогает решить эту проблему: внутренние нарушители не смогут получить несанкционированный доступ к рабочим станциям через их локальные интерфейсы, чтобы выкрасть данные клиентов через сменные носители и портативные устройства, а система теневого копирования сможет доказать и документировать факт неудачных и успешных попыток доступа, а также копирования конкретных данных. |
| Оценка достаточности политик и процедур безопасности | С помощью DeviceLock компания может одним служащим разрешить локальный доступ к информационным ресурсам, а другим запретить. Все полномочия распределяются в соответствии с политикой информационной безопасности, принципом минимальных привилегий и здравым смыслом. Это уже не игнорирование риска внутренней безопасности, а управление им. При этом у компании создается необходимая документальная база для подтверждения достаточности внедренных процедур. |
| Контроль над доступом к чувствительной информации | Ключевой особенностью DeviceLock является возможность не только существенно снизить риск утечки чувствительной информации со стороны авторизованных пользователей, но и сохранить точную копию данных, которые покидают сеть через локальные соединения рабочей станции. Таким образом, при помощи DeviceLock компания обеспечивает контроль за фактами копирования данных с рабочих станций сотрудников. |
| Мониторинг и выявление атак | Чтобы узнать, что атака произошла, необходимо иметь систему выявления атак. При помощи системы теневого копирования DeviceLock компания всегда сможет вычислить и узнать, была ли утечка, а если да, то какие конкретно данные были скомпрометированы. Без такой системы финансовому институту не удастся выявить утечку через сменные носители и мобильные устройства и, следовательно, не удастся оповестить пострадавших. А это, в свою очередь, влечет за собой штрафы и судебное разбирательство. |
| Ответственность и отчетность совета директоров | Специфика нормативных актов, подобных GLBA и FACTA, такова, что совет директоров во многих случаях несет ответственность за эффективность программы безопасности. Применение DeviceLock позволяет существенно улучшить информационное обеспечение ответственности и качество отчетности топ-менеджмента и ответственных лиц компании. |

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

Отдел продаж: sales@devicelock.com

Тех. поддержка: support@devicelock.com