

DeviceLock для соответствия закону Sarbanes-Oxley Act



Оглавление:

- [Введение](#)
- [Требования SOX](#)
- [Система внутреннего контроля](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock в рамках SOX](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Закон SOX (Sarbanes-Oxley Act) был принят в США в 2002 году. Этот нормативный акт определяет требования к документообороту и финансовой отчетности компаний, закрепляет персональную ответственность финансовых и генеральных директоров предприятия, а также вводит процедуру регулярного независимого аудита.

Сегодня абсолютно все публичные компании, чьи ценные бумаги котируются на фондовом рынке США, обязаны соответствовать требованиям SOX. Более того, высшие исполнительные лица организации – генеральный и финансовый директора – несут личную ответственность за реализацию ключевых положений SOX. Нарушение требований закона чревато персональными штрафами в размере до 25 млн. долларов и лишением свободы на срок до 20 лет.

Несмотря на всю свою жесткость, за годы использования SOX фактически превратился в негласный стандарт корпоративного управления. Даже не котирующиеся в США организации предпочитают внедрять положения закона, чтобы повысить свою конкурентоспособность, стать более привлекательными в глазах инвесторов и партнеров, а также эффективнее защитить корпоративные активы.

Нормативный акт не предъявляет требований к информационной безопасности компаний напрямую, однако содержит целый ряд положений относительно средств внутреннего контроля, целостности чувствительной финансовой документации, а также возможности аудита. Модернизация корпоративной системы информационной безопасности позволяет существенно облегчить внедрение вышеперечисленных ключевых положений закона.

В данном документе будут рассмотрены требования SOX, которые влияют на информационную инфраструктуру компании и использующиеся в ней средства безопасности, а также возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия положениям закона.

Требования SOX

Закон SOX состоит из секций, каждая из которых предъявляет те или иные требования к корпоративному управлению. Ключевыми положениями SOX являются секции 302, 404 и 802. Они закрепляют персональную ответственность высших исполнительных лиц, необходимость внедрения системы внутреннего контроля и хранения всей корпоративной корреспонденции.

Секция 302. В соответствии с данным параграфом генеральные и финансовые директора обязаны включать свои собственные отчеты в протоколы проведенного аудита для того, чтобы удостоверить правильность информации, содержащейся в данных протоколах.

Руководители, которые намеренно предоставляют фальшивые отчеты, несут серьезную уголовную ответственность. Им угрожают штрафы в размере до 25 млн. долларов и лишение свободы на срок до 20 лет.

Секция 404. Данный параграф закрепляет необходимость внедрения системы внутреннего контроля. Это необходимо для того, чтобы вовремя обнаружить неавторизованное или нецелевое использование активов компании, в том числе информационных. Другими словами, все операции, осуществляемые как с цифровыми активами компании, так и с финансовой отчетностью должны тщательно протоколироваться, а инфраструктура организации обязана включать в себя механизм выявления мошенничества.

Секция 802. В продолжение требований предыдущего раздела, данная секция обязывает компанию обеспечить хранение всех деловых документов и любой другой информации, имеющей отношение к финансовой отчетности. Срок хранения определен 5 годами. Вдобавок, секция 103 расширяет до 7 лет срок хранения любых документов, имеющих отношение к аудиту. Отметим, что хотя SOX не определяет, какие конкретно данные необходимо хранить, независимые компании-аудиторы требуют обеспечить сбор и архивирование самого широкого спектра электронных документов.

Таким образом, высшие исполнительные лица компании лично заинтересованы в обеспечении соответствия требованиям SOX. Во-первых, невыполнение предписанных правил чревато судебным преследованием и уголовной ответственностью. Во-вторых, внедрение SOX в компании повышает ее конкурентоспособность и инвестиционную привлекательность.

Система внутреннего контроля

Ключевым требованием SOX, безусловно, является секция 404, в соответствии с которой руководство обязано создать систему внутреннего контроля у себя в компании. Между тем, закон не раскрывает подробно, что следует считать такой системой и какие функции она должна выполнять.

Однако это делает Стандарт Аудита №5¹, принятый в 2007 году организацией PCAOB (Public Company Accounting Oversight Board – Комитет по надзору за отчетностью открытых акционерных компаний). Этот орган выполняет функции надзора за правильностью учета в публичных компаниях и разрабатывает стандарты, конкретизирующие требования SOX.

Стандарт Аудита №5 по построению системы внутреннего контроля во многом основан на стандарте «Internal Control – Integrated Framework», выпущенном организацией COSO (Committee of Sponsoring Organizations of the Treadway Commission – Комитет спонсорских организаций в Комиссии Трэдуэйя).

Согласно пункту А5 Стандарта Аудита №5, система внутреннего контроля над финансовой отчетностью это:

Процесс, разработанный под руководством или с участием генерального и финансового директоров компании (или соответствующих уполномоченных лиц)... [этот процесс] включает политики и процедуры, которые:

1. *Обеспечивают сохранение записей, которые с достаточной степенью подробности, точности и беспристрастности отражают транзакции и перемещения корпоративных активов;*

¹Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements.

http://pcaob.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

2. *Предоставляют разумную гарантию того, что все транзакции записаны должным образом и могут быть отражены в финансовых отчетах в соответствии с общепринятыми принципами бухгалтерского учета, а также что все корпоративные приходы и расходы произведены с разрешения менеджмента и директоров компании; и*
3. *Предоставляет разумную гарантию предотвращения или своевременного выявления неавторизованного приобретения, использования или перемещения корпоративных активов, которое может материально повлиять на финансовую отчетность.*

Очень важно, что в понятие «корпоративные активы» также входят цифровые активы компании: интеллектуальная собственность, коммерческие или технологические секреты, а также целый ряд конфиденциальных документов. Очевидно, что кража или утечка этой информации отрицательно скажется на бизнесе фирмы, ее финансовых показателях и, следовательно, акционерах компании. Таким образом, система внутреннего контроля должна обеспечить защиту не только самих финансовых отчетов, но еще и информационных активов фирмы.

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 информацией, покидающей 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, 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 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 приближающейся консьюмеризации корпоративных IT-систем. Авторитетные исследовательские агентства Yankee Group и CSC Research утверждают, что директора и менеджеры IT-департаментов не могут игнорировать то обилие портативных устройств, которыми постоянно пользуются служащие. Они просто обязаны обеспечить поддержку мобильных компьютеров сотрудников. В противном случае компания рискует потерять инновационный потенциал, а следом и конкурентоспособность. Между тем, массовая консьюмеризация чревата новыми серьезными рисками, так как мобильные устройства могут быть использованы для осуществления мошенничества, утечки и других внутренних нарушений. Решить эту проблему позволяет DeviceLock.

Таким образом, продукт защищает компанию от утечки цифровых активов, попадания во внутреннюю сеть нежелательного контента, 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.

Мнение Gartner

Для предотвращения кражи интеллектуальной собственности и конфиденциальных данных компаниям следует предпринять 5 обязательных шагов:

1. Внедрить средства мониторинга и фильтрации контента.
2. Шифровать резервные копии.
3. **Внедрить средства контроля над портами рабочей станции, беспроводными сетями и внешними устройствами.**
4. Шифровать ноутбуки.
5. Осуществлять мониторинг обращений к базе данных.

Источник: [Gartner](#)

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 различными консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager.

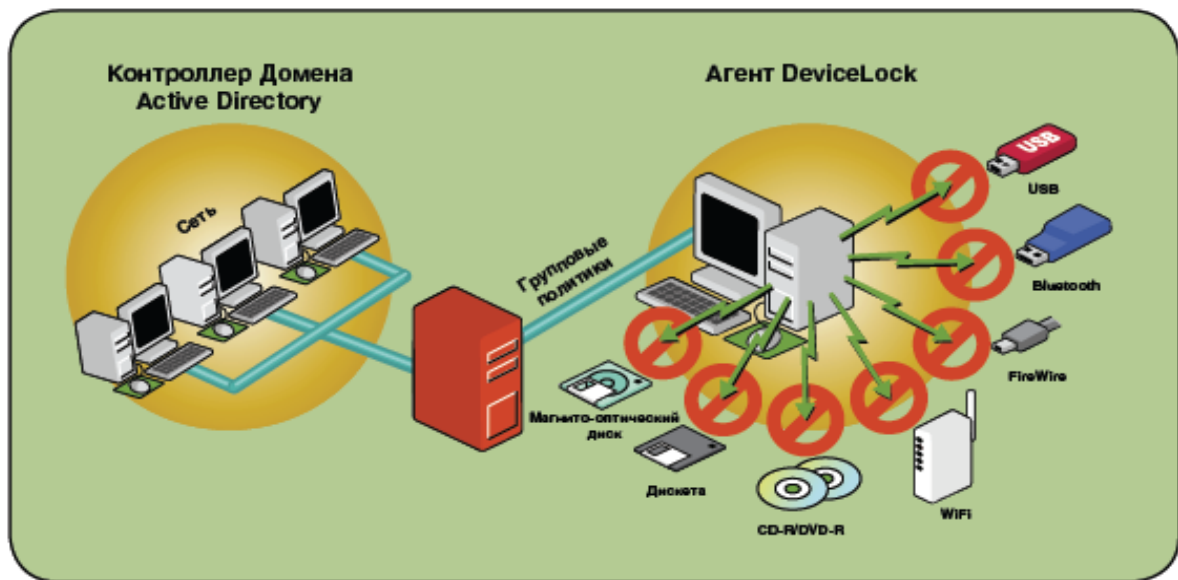


Рис. 1. Схема работы DeviceLock

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

Возможности DeviceLock в рамках SOX

Продукт DeviceLock осуществляет контроль над передвижением информации через 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, что является одним из основных требований SOX.

Использование DeviceLock в корпоративной среде позволяет обеспечить соответствие двум основным требованиям закона:

- **Секция 404** требует наличия системы внутреннего контроля, которая бы охватывала финансовую отчетность и позволяла контролировать перемещение корпоративных активов. В данном контексте DeviceLock выполняет функции ключевого элемента системы внутреннего контроля, при помощи которого обеспечивается управление доступом к информационным активам организации на уровне рабочей станции и при работе с мобильными устройствами. Эффективное применение DeviceLock предотвратит утечку интеллектуальной собственности и конфиденциальных

документов фирмы, что может существенно сказаться на благосостоянии акционеров компании.

- **Секция 802** предполагает архивирование всей корпоративной корреспонденции, которая может иметь отношение к финансовой отчетности, аудиту и благосостоянию организации. В этой связи DeviceLock предлагает уникальную функциональность – теневое копирование всех или необходимого подмножества данных, покидающих корпоративную сеть через порты рабочих станций, сменные носители, беспроводные сети и мобильные устройства. Все сведения складываются в базу данных и доступны для последующего аудита и ретроспективного анализа.

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

Таб. 1. Функциональность DeviceLock применительно к закону SOX	
Требования закона SOX	Возможности DeviceLock
§802: архивирование корпоративной информации (прежде всего, любой исходящей электронной документации) и хранение ее в течение минимум 7 лет	Теневое копирование данных, покидающих корпоративную сеть через порты рабочей станции, внешние устройства и носители, а также беспроводные сети – это уникальная функциональность DeviceLock. Решение сохраняет все исходящие сведения во внешней базе данных Microsoft SQL Server, что позволяет проводить последующий аудит, ретроспективный анализ и расследования фактов утечки, кражи информационных активов и мошенничества.
§404: механизмы внутреннего контроля, препятствующие нецелевому использованию и краже корпоративных активов	Продукт DeviceLock является элементом системы внутреннего контроля, обеспечивая контроль над передвижением чувствительной документации, когда она покидает рабочую станцию через порты или беспроводные сети. Вдобавок, продукт позволяет реализовать гибкую политику безопасности при работе с КПК, смартфоном и коммуникатором, разрешив одни операции, но запретив другие. Тем самым, DeviceLock предотвращает утечку конфиденциальных сведений, кражу интеллектуальной собственности и информационных активов компании.
§302: личная ответственность руководства за правдивость финансовых отчетов, эффективность процедур внутреннего контроля и совместимость с требованиями закона SOX	Благодаря использованию DeviceLock руководство компании может быть спокойно: в соответствии с заданной политикой продукт в автоматическом режиме не позволит украсть информационные активы компании. В то же время настройки и политики самого продукта легко и полностью аудируемы. Помимо теневого копирования продукт ведет журнал событий, отражая все произведенные пользователем операции по перемещению информации с рабочей станции во внешнюю среду через порты и беспроводные сети. Между тем, наличие такого журнала является обязательным для прохождения успешного аудита корпоративных информационных систем 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 Smart 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. Smart Лайн Инк – международная компания с офисами в Лондоне, Милане, Москве, Ратингене (Германия) и Сан Рамоне (штат Калифорния, США). Основной офис разработки программных продуктов Smart 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