

DeviceLock для соответствия Combined Code on Corporate Governance (UK)



Оглавление:

- [Введение](#)
- [Требования Combined Code](#)
 - [Отличие SOX и Combined Code](#)
 - [Ключевые компоненты Combined Code](#)
 - [Внутренний контроль в Combined Code](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock для создания системы внутреннего контроля](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Корпоративное управление публичных компаний, представленных на Лондонской фондовой бирже (LSE, London Stock Exchange), регулируется Объединенным Кодексом ([The Combined Code on Corporate Governance](#)). Принципы, правила и требования, заложенные в Объединенный Кодекс, призваны повысить эффективность раскрытия информации и тем самым увеличить прозрачность компаний-эмитентов, а также установить средства внутреннего контроля над финансовыми отчетами и активами корпораций, чтобы защитить интересы инвесторов.

В отличие от жесткого американского закона SOX (Sarbanes Oxley Act of 2002) британский Объединенный Кодекс, во многом, не является обязательным для исполнения. Однако, в том случае, если руководство публичной компании отказывается от реализации правил или принципов Кодекса, оно обязано четко аргументировать свою позицию перед инвесторами. Таким образом, чаще всего эмитенту намного удобнее использовать лучшие практики, заложенные в Кодекс, чем игнорировать их.

В то же самое время между Объединенным Кодексом и американским законом SOX есть много общего. В частности известный параграф 404 из SOX, требующий внедрения средств внутреннего контроля, во многом повторяет принципы Объединенного Кодекса, которые были закреплены в докладе Тёрнбулла ([Turnbull Report](#)) еще в 1999 году.

Таким образом, перед британскими публичными компаниями сегодня стоит задача создания системы внутреннего контроля, которая призвана бороться с мошенничеством, а также защищать корпоративные активы от кражи, присвоения и других злоупотреблений. На практике это означает, что корпорациям следует внедрить процедуры контроля над отчетностью и активами. Между тем, финансовая отчетность сегодня ведется в электронном формате, а в число важнейших активов компании входят интеллектуальная собственность, конфиденциальная информация и базы данных клиентов. Другими словами, средства внутреннего контроля также должны быть построены на информационных технологиях, чтобы отследить операции с активами и отчетностью.

В данном документе будут рассмотрены требования Combined Code, которые влияют на информационную инфраструктуру организаций и использующиеся в ней средства безопасности, а также возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого организация может гораздо эффективнее достичь соответствия данному кодексу корпоративного управления.

Требования Combined Code

Объединенный Кодекс состоит из нескольких разделов, каждый из которых называется «докладом» и носит имя человека, руководившего его подготовкой.

Первоначально Объединенный Кодекс был сформирован на основе докладов Кэдбюри (Cadbury), Гринбюри (Greenbury) и Хэмпеля (Hampel) и вступил в силу 1 января 1999 года. В дальнейшем Кодекс был дополнен докладами Тёрнбулла (Turnbull), Майнерса (Myners), Смита (Smith), Хиггса (Higgs) и Тайсона (Tyson).

В итоге Совет по финансовой отчетности (Financial Reporting Council) объединил все доклады и выпустил в июле 2003 года новую редакцию Объединенного Кодекса, которая действует с 1 ноября 2003 года.

В таб. 1 ниже приведены важнейшие доклады, составляющие каркас современной системы корпоративного управления в Великобритании.

Корпоративное управление Великобритании		
Название	Дата опубликования	Пояснение
Доклад Кэдбюри (Cadbury Report)	Декабрь 1992	Финансовые аспекты корпоративного управления
Доклад Рутмана (Rutteman Report)	Декабрь 1994	Внутренний контроль и финансовая отчетность
Доклад Гринбюри (Greenbury Report)	Июль 1995	Вознаграждение членов совета директоров
Доклад Хэмпеля (Hampel Report)	Январь 1998	Фундаментальные принципы корпоративного управления
Объединенный Кодекс (The Combined Code)	Июнь 1998	Принципы хорошего управления и кодекс передового опыта
Доклад Тёрнбулла (Turnbull Report)	Сентябрь 1999	Система внутреннего контроля
Доклад Майнерса (Myners Report)	Март 2001	Институциональные инвесторы
Доклад Смита (Smith Report)	Январь 2003	Комитеты советов директоров по аудиту
Доклад Хиггса (Higgs Report)	Январь 2003	Роль неисполнительных директоров
Доклад Тайсона (Tyson Report)	Июнь 2003	Наем и подготовка неисполнительных директоров
Объединенный Кодекс (The Combined Code)	Июль 2003	Объединенный кодекс корпоративного управления

Таб. 1. Стандарты корпоративного управления Великобритании

Отличие SOX и Combined Code

Основное отличие американского закона SOX и британского Объединенного Кодекса состоит в том, что британская система корпоративного управления не является жестко регулируемой. Она действует по правилу «подчинитесь или объясните» (comply or explain). Это означает, что все корпорации, чьи акции зарегистрированы на LSE, должны ежегодно публиковать итоговые отчеты, состоящие из двух частей. В первой части раскрывается, как фирма использует принципы Кодекса. Во второй части нужно либо подтвердить соответствие корпоративной практики положениям Combined Code, либо объяснить причины отступления от них.

Таким образом, участники рынка добровольно принимают или отвергают положения Кодекса. Британские специалисты считают, что такой подход зарекомендовал себя очень хорошо, а потому изменять его не следует ни сейчас, ни в ближайшем будущем. Кроме того, новая редакция Combined Code (от 2003 года) лишь подчеркнула добровольный характер Кодекса. Представленные в ней принципы корпоративного управления разделены на основные и вспомогательные. В результате, компании получили еще большую гибкость в принятии решений.

Заметим, что Кодекс никак не регламентирует форму итогового отчета. Другими словами, менеджмент корпорации должен решать самостоятельно, какие положения Combined Code адресовать в отчете, как доказать эффективность реализованных в компании принципов Кодекса и как объяснить отступления от него.

Ключевые компоненты Combined Code

Помимо основных положений, занимающих примерно одну треть Combined Code, в обновленный британский Кодекс (от 2003 года) входят три поясняющих документа: Руководство Тёрнбулла по созданию системы внутреннего контроля, Руководство Смита по организации деятельности комитетов по аудиту и Указания Хиггса по обеспечению эффективного корпоративного управления.

Следует отметить, что Руководство Тёрнбулла (по созданию системы внутреннего контроля) заменило собой Доклад Руттмана (Rutteman Report) по внутреннему контролю и финансовой отчетности в предыдущей версии Кодекса. Однако само Руководство Тёрнбулла в октябре 2005 года было заменено другим [документом](#), выпущенным Советом по финансовой отчетности. Новый документ называется: «Система внутреннего контроля – пересмотренное руководство по Объединенному Кодексу для директоров» (Internal Control – Revised Guidance for Directors on the Combined Code). Это руководство введено в действие 1 января 2006 года.

Внутренний контроль в Combined Code

Согласно принципу С.2 Объединенного Кодекса, совет директоров обязан *«поддерживать разумную систему внутреннего контроля для защиты инвестиций акционеров и корпоративных активов»*. Далее положение С.2.1 требует от совета директоров *«по крайней мере ежегодно проверять эффективность коллективной системы внутреннего контроля и докладывать о результатах акционерам»*. Такая проверка, согласно Combined Code, должна охватывать средства контроля над материальной, финансовой и организационной базой корпорации, а также систему управления рисками, включая нормативные риски.

Создание системы внутреннего контроля неразрывно связано с ее последующим аудитом. Так, положение С.3.2 требует от совета директоров создать комитет по аудиту, в обязанности которого среди всего прочего будет входить *«мониторинг целостности финансовой отчетности компании»*, *«проверка средств контроля над финансовой*

отчетностью», «проверка системы внутреннего контроля и системы управления рисками».

Пояснение того, что такое *«разумная система внутреннего контроля»*, дает пересмотренное Руководство Тёрнбулла (от 2005 года). Согласно параграфам №15 и №16, это, прежде всего, такая система, которая минимизирует все возможные неприемлемые для данной конкретной организации риски. То есть, те риски, которые можно избежать или минимизировать.

Рассмотрим параграф №19: *«система внутреннего контроля объединяет политики, процессы, задания, роли и другие аспекты компании»*, которые *«способствуют достижению целей организации»* путем *«адекватной реакции на деловые, финансовые, операционные, нормативные и другие риски»*. Среди таких рисков авторы руководства особо выделяют *«нецелевое использование или потерю корпоративных активов»*, *«мошенничество»* и т.д. В рамках разумной системы внутреннего контроля должна быть точно определена ответственность за те или иные корпоративные активы.

Однако помимо функциональности, которая преследует только интересы инвесторов, система внутреннего контроля позволяет повысить конкурентоспособность компании. Согласно тому же параграфу №19, система должна *«улучшить качество внутренней и внешней отчетности»* и помочь в обеспечении совместимости с другими нормативными актами и законами.

Среди остальных характеристик *«разумной системы внутреннего контроля»* следует отметить, что она должна включать в себя:

- процессы мониторинга (параграф №20);
- процедуры для немедленного информирования уполномоченных лиц в случае выявления нарушений (параграф №21);
- средства для надежной (гарантированной) защиты от *«растрат, мошенничества, нарушений законов или нормативных актов»* (параграф №23).

В то же самое время параграф №26, адресующий проблемы аудита механизмов внутреннего контроля, указывает, что основным компонентом *«разумной»* системы является постоянный мониторинг, а также возможность регулярно получать отчеты о состоянии средств внутреннего контроля.

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 организациях. 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 съемные носители, 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.

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.

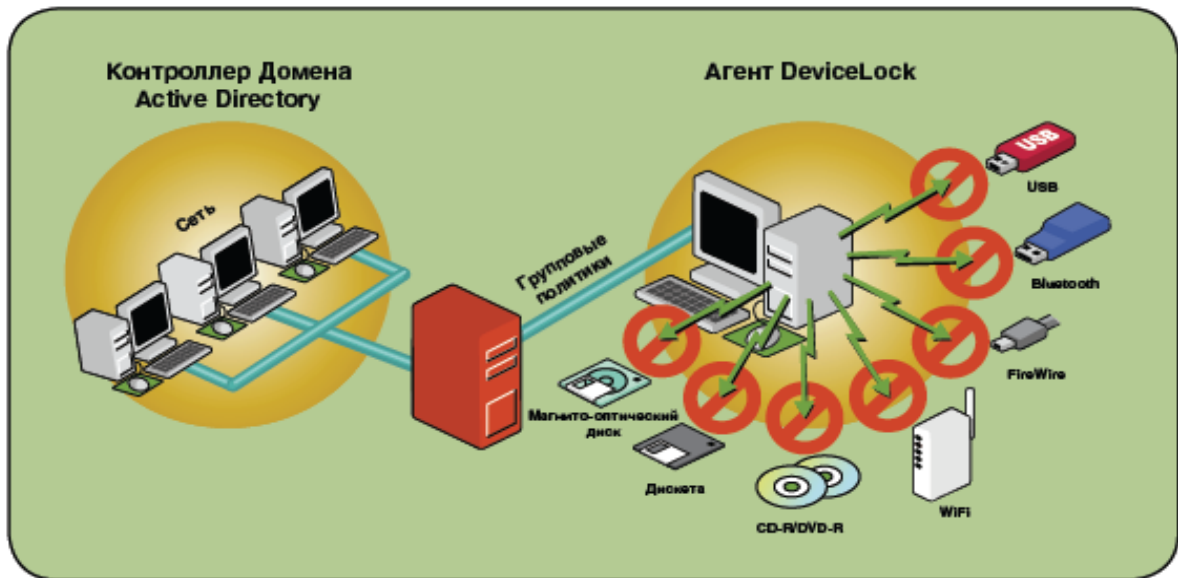


Рис. 1. Схема работы DeviceLock

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

Возможности DeviceLock для создания системы внутреннего контроля

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 основному требованию Объединенного Кодекса: в соответствии с принципом С.2, в организации должна быть создана система внутреннего контроля для защиты активов и финансовой отчетности. 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 интеллектуальной собственности и конфиденциальных документов фирмы, что может существенно сказаться на благосостоянии акционеров компании.

В таблице далее (см. таб. 2) просуммирована функциональность DeviceLock в соответствии с требованиями Объединенного Кодекса.

Таб. 2. Функциональность DeviceLock применительно к Combined Code	
Требования Combined Code	Возможности DeviceLock
Принцип С.2: совет директоров должен поддерживать разумную систему внутреннего контроля для защиты инвестиций акционеров и корпоративных активов	Продукт DeviceLock является элементом системы внутреннего контроля, обеспечивая контроль над передачей данных, когда они покидают 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 существенно снижает риск неконтролируемой утечки конфиденциальных сведений, кражу интеллектуальной собственности и информационных активов компании.
Положение С.2.1: совет директоров должен проверять эффективность системы внутреннего контроля	Благодаря использованию DeviceLock руководство компании может быть спокойно: в соответствии с заданной политикой продукт в автоматическом режиме сможет контролировать передачу данных, включая информационные активы фирмы, через локальные порты рабочих станций, беспроводные сети и съемные носители. 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. Очень важно, что наличие такого журнала является обязательным для прохождения успешного аудита корпоративных информационных систем компании.
Положение С.3.2: совет директоров должен обеспечить выполнение функций мониторинга целостности финансовой отчетности, проверки средств контроля над финансовой отчетностью, проверки системы внутреннего контроля и системы управления рисками	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 и кражи информационных активов

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