

DeviceLock для соответствия кодексам корпоративного управления



Оглавление:

- [Введение](#)
- [Современное корпоративное управление](#)
 - [Принципы корпоративного управления ОЭСР](#)
 - [Принципы корпоративного управления Euroshareholders](#)
 - [Объединенный Кодекс корпоративного управления](#)
 - [Закон SOX](#)
 - [Немецкий Кодекс корпоративного управления](#)
 - [Кодекс корпоративного управления ФСФР](#)
 - [Выводы](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock для создания системы внутреннего контроля](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

Введение

Сегодня практически каждая публичная компания подчиняется требованиям того или иного кодекса корпоративного управления, специфичного для той страны, где торгуются акции данной корпорации. Например, в США действует закон SOX (Sarbanes-Oxley Act of 2002), в Британии – Объединенный Кодекс корпоративного управления (Combined Code), в Германии – немецкий Кодекс, а в России – Кодекс корпоративного поведения Федеральной службы по финансовым рынкам (ФСФР). Кроме того, существуют кодексы, охватывающие целые группы стран. Так, Принципы корпоративного управления Организации экономического сотрудничества и развития (ОЭСР) предназначены для всех 30 стран-участниц ОЭСР, а Принципы корпоративного управления Euroshareholders охватывают все страны Евросоюза.

Кодексы корпоративного управления призваны установить четкие правила по раскрытию информации в публичных компаниях, повысить прозрачность фирм, а также обеспечить дополнительный контроль над финансовой отчетностью и использованием активов корпорации, чтобы тем самым защитить интересы инвесторов.

Это означает, что на практике внедрение любого из упомянутых выше кодексов требует от публичной компании создать системы управления рисками и внутреннего контроля, которые призваны минимизировать случаи финансового мошенничества, защитить активы фирмы от злоупотреблений, кражи и присвоения.

Отметим, что сегодня документооборот почти каждой организации является электронным, а многие корпоративные активы носят информационный характер. Например, интеллектуальная собственность, база данных клиентов и партнеров – все эти данные являются информационными активами компании и нуждаются в защите в соответствии с требованиями внутреннего контроля в кодексах корпоративного управления.

В данном документе будут рассмотрены требования основных кодексов (указанные выше), 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 кодексам корпоративного управления.

Современное корпоративное управление

Основная задача корпоративного управления состоит в том, чтобы в максимально полном объеме учесть требования всех заинтересованных лиц, участвующих в жизнедеятельности публичной компании. В общем виде это менеджмент, акционеры, работники, регуляторы, общество и т.д. Однако на практике корпоративное управление фокусируется в основном на проблеме взаимоотношений менеджмента фирмы и инвесторов. Более того, все современные кодексы корпоративного управления направлены на то, чтобы защитить интересы акционеров, так как с самого начала считается, что менеджмент компании намного ближе к ее имуществу, активам и финансовой отчетности, а, следовательно, может злоупотреблять своим положением в ущерб инвесторам. Таким образом, сегодня корпоративное управление и его основные принципы, зафиксированные в целом ряде кодексов, направлены на защиту инвесторов посредством глубокого и широкого контроля над отчетностью и активами публичной компании.

Важно заметить, что далеко не все кодексы корпоративного управления сегодня являются обязательными для исполнения. Безусловно, самым жестким в этом отношении является американский закон SOX, который необходимо выполнять всем публичным компаниям, чьи акции торгуются на фондовом рынке США. Немного менее жестким, но тоже обязательным является немецкий Кодекс. Однако кодексы других европейских стран (Британия, Россия) не возведены в ранг нормативных актов, так что корпорации могут игнорировать их некоторые положения. В то же самое время, существует целый ряд стимулов, которые поощряют публичные компании к добровольному внедрению положений кодексов.

Прежде всего, публичные компании стремятся повысить свою репутацию в глазах общественности, инвесторов и финансовых аналитиков, а лучший способ сделать – повысить качество и эффективность корпоративного управления. Так что внедрение положений кодекса зачастую сразу же положительно влияет на котировки акций компаний, что выгодно как инвесторам, так и менеджменту.

Далее, несмотря на добровольный характер некоторых кодексов, постоянно существует вероятность их трансформации в обязательные для исполнения. Такие процессы в частности происходят в России, где Кодекс ФСФР может стать обязательным уже в ближайшие годы. Кроме того, даже в тех странах, которые специально подчеркивают добровольный характер кодекса, например, в Британии, менеджмент обязан аргументировать свою позицию, чтобы объяснить инвесторам, какие положения кодекса и почему не внедрены в корпорации.

Последним аргументом, но отнюдь не по значению, является тот факт, что положения кодексов позволяют повысить конкурентоспособность корпорации благодаря контролю над финансовыми отчетами и повышению качества той информации, на основании которой принимаются важные управленческие решения.

Таким образом, сегодня многие публичные и непубличные компании самостоятельно внедряют требования кодексов корпоративного управления, так как это положительно сказывается на внутренних бизнес процессах и конкурентоспособности фирмы.

Принципы корпоративного управления ОЭСР

В 1999 году Консультативная группа бизнес-сектора по корпоративному управлению ОЭСР сформулировала «Принципы корпоративного управления» («[Principles of Corporate Governance](#)»), Кодекс ОЭСР), которые были одобрены правительствами стран-членов ОЭСР. Разработкой своих рекомендаций занялись и крупнейшие международные институциональные инвесторы – пенсионные и инвестиционные фонды.

Кодекс ОЭСР включает пять основных принципов: права акционеров, равное отношение к акционерам, роль заинтересованных лиц в управлении компанией, раскрытие информации

и прозрачность бизнеса, обязанности правления. Последний принцип – обязанности правления – как раз и предусматривает создание эффективной системы внутреннего контроля. Отметим, что данный Кодекс не является обязательным для исполнения, а служит лишь каркасом для разработки национальных версий кодекса.

В таблице ниже (см. таб. 1) просуммированы требования Кодекса ОЭСР в рамках внутреннего контроля над финансовой отчетностью и активами публичной компании.

Таб. 1. Требования к системе внутреннего контроля в рамках Принципов корпоративного управления ОЭСР	
Принцип VI. Обязанности Совета Директоров. «Система корпоративного управления должна служить стратегическим целям компании, эффективному мониторингу менеджмента со стороны совета директоров и отчетности совета перед компанией и акционерами».	D.1. Совет директоров должен выполнять определенные ключевые функции, включая ... руководство корпоративной политикой рисков и ее проверку...
	D.6. Совет директоров должен выполнять определенные ключевые функции, включая ... мониторинг и управление потенциальными конфликтами между менеджментом, членами совета и акционерами, включая неправильное использование корпоративных активов и злоупотребление транзакциями.
	D.7. Совет директоров должен выполнять определенные ключевые функции, включая ... гарантию целостности корпоративных систем бухгалтерской и финансовой отчетности, включая независимый аудит, наличие и использование систем контроля, в частности, систем управления рисками, финансового и операционного контроля, а также соответствие законам и стандартам.

Принципы корпоративного управления Euroshareholders

В 2000 году Группа европейских акционеров (Shareholders) приняла свои собственные «Принципы корпоративного управления Euroshareholders» ([«Euroshareholders Corporate Governance Guidelines»](#)), Кодекс Euroshareholders). Данный кодекс основывается на руководящих принципах ОЭСР, но содержит более специфические и детализированные рекомендации. Кодекс Euroshareholders (в случае его принятия различными компаниями и странами) должен улучшить права и влияние акционеров. Насколько это позволяют национальные правовые системы, составители Кодекса Euroshareholders попытались максимально детально описать свою точку зрения на различные проблемы корпоративного управления. В частности, Кодекс указывает, что исполнительные директора компании несут ответственность за создание и эффективное функционирование системы внутреннего контроля. Отметим, что данный кодекс носит необязательный характер, но рекомендуется к применению в странах и корпорациях Евросоюза.

В таблице ниже (см. таб. 2) просуммированы требования Кодекса Euroshareholders в рамках внутреннего контроля над финансовой отчетностью и активами публичной компании.

Таб. 2. Требования к системе внутреннего контроля в рамках Принципов корпоративного управления Euroshareholders	
Часть V. Роль совета директоров. Глава – Члены совета исполнительных директоров.	«Основная обязанность исполнительных лиц состоит в том, чтобы обеспечить функционирование эффективных систем внутреннего контроля. Эта обязанность вытекает из ответственности исполнительных лиц за корпоративную стратегию и достижение бизнес целей».

Объединенный Кодекс корпоративного управления

С 1 января 1999 года в Великобритании вступил в силу «Объединенный кодекс корпоративного управления» («[The Combined Code on Corporate Governance](#)», Объединенный Кодекс). В нем с самого начала были зафиксированы требования к системе внутреннего контроля, представленные в специальной главе – Руководстве Тёрнбулла (Turnbull Guidance), которая в октябре 2005 года была заменена отдельным документом, выпущенным Советом по финансовой отчетности. Новое руководство, вступившее в силу 1 января 2006 года, называется: «Система внутреннего контроля – пересмотренное руководство по Объединенному Кодексу для директоров» («[Internal Control – Revised Guidance for Directors on the Combined Code](#)»).

Отметим, что британская система корпоративного управления, построенная на Объединенном Кодексе, не является жестко регулируемой. Она действует по правилу «подчинитесь или объясните» (comply or explain). Это означает, что все корпорации, чьи акции зарегистрированы на LSE (London Stock Exchange – Лондонская Фондовая Биржа), должны ежегодно публиковать итоговые отчеты, состоящие из двух частей. В первой части раскрывается, как фирма использует принципы Объединенного Кодекса. Во второй части нужно либо подтвердить соответствие корпоративной практики положениям Кодекса, либо объяснить причины отступления от них. Таким образом, участники рынка добровольно принимают или отвергают положения Объединенного Кодекса, но при этом они обязаны мотивировать свое решение перед инвесторами.

В таблице ниже (см. таб. 3) просуммированы требования Объединенного Кодекса в рамках внутреннего контроля над финансовой отчетностью и активами публичной компании.

Таб. 3. Требования к системе внутреннего контроля в рамках Объединенного Кодекса	
Принцип С.2. Внутренний контроль. «Совет директоров должен поддерживать разумную систему внутреннего контроля для защиты инвестиций акционеров и корпоративных активов».	Положение С.2.1. «Совет обязан минимум раз в год проверять эффективность системы внутреннего контроля и отчитываться перед акционерами в результатах. Проверка должна покрывать все материальные сферы контроля, включая финансовый, операционный и нормативный контроль, а также системы управления рисками».
Принцип С.3. Комитет по аудиту и аудиторы. «Совет должен создать формальные и прозрачные процедуры финансовой отчетности и внутреннего контроля, а также поддерживать соответствующие отношения с аудитором».	Положение С.3.2. «Главная роль и обязанности комитета по аудиту должны быть закреплены письменно и включать в себя следующее: <ul style="list-style-type: none">• Мониторинг целостности финансовых данных компании и любых формальных заявлений о ее финансовых результатах, а также проверка важных решений, содержащихся в финансовой отчетности;• Проверка корпоративной системы внутреннего контроля и (если этим не занимается отдельный комитет совета по рискам, состоящий из независимых директоров, или сам совет) проверка систем внутреннего контроля и управления рисками

Закон SOX

В 2002 году Конгресс США принял закон SOX («[Sarbanes-Oxley Act](#)»), который получил всемирную известность благодаря параграфу 404. Этот параграф описывает ответственность руководства компании за установление внутреннего контроля над финансовой отчетностью и корпоративными актами. Отметим, что закон SOX является обязательным для исполнения всеми компаниями, чьи акции котируются на биржах США. Причем в рамках своей ответственности исполнительные и финансовые директора фирмы обязаны обеспечить разумные гарантии предотвращения или своевременного обнаружения случаев несанкционированного приобретения, использования или перемещения корпоративных активов, если это может существенно повлиять на финансовую отчетность компании. Причем под термином «активы» понимаются, в том числе, информационные активы (интеллектуальная собственность, исходные коды, коммерческие и торговые секреты, сведения о слияниях и поглощениях, медицинские сведения, а также иная важная информация, несанкционированное разглашение которой может оказать негативное влияние на стоимость акций или финансовую деятельность компании). Сегодня закон SOX имеет репутацию самого жесткого нормативного акта в сфере корпоративного менеджмента. Руководители, которые нарушают положения SOX и намеренно предоставляют фальшивые отчеты, могут оказаться в тюрьме на срок до 20 лет и заплатить штраф в размере до 25 млн. долларов.

В таблице ниже (см. таб. 4) просуммированы требования закона SOX в рамках внутреннего контроля над финансовой отчетностью и активами публичной компании.

Таб. 4. Требования к системе внутреннего контроля в рамках закона SOX	
Секция 103. Аудит, контроль качества, стандарты и правила независимости. 103(а). Аудит, контроль качества, стандарты этики.	103(а).(2).(А)(i): «Совет [обязан] готовить и хранить не менее 7 лет все документы, касающиеся аудита, и любую другую информацию, имеющую отношение к отчету об аудите, в таком объеме, чтобы обосновать выводы, представленные в отчете об аудите»
Секция 302. Корпоративная ответственность за финансовую отчетность. 302(а). Обязательные требования.	302(а).4(А): «...главный исполнительный директор(а) или лица с такими же функциями ... обязаны создать и поддерживать систему внутреннего контроля»
	302(а).4(В): «...главный исполнительный директор или лица с такими же функциями ... обязаны спроектировать систему внутреннего контроля ...»
	302(а).4(С): «...главный исполнительный директор или лица с такими же функциями ... обязаны оценить эффективность системы внутреннего контроля не позднее, чем за 90 дней до составления отчета»
	302(а).4(Д): «...главный исполнительный директор или лица с такими же функциями ... обязаны включить в отчет результаты проверки эффективности системы внутреннего контроля, основанные на последней проверке»
Секция 404. Оценка менеджментом системы внутреннего контроля.	404(а): «...каждый годовой отчет [должен включать в себя] отчет о системе внутреннего контроля, который должен — (1) утверждать ответственность менеджмента за создание и поддержание адекватной системы внутреннего контроля и процедур финансовой отчетности; и (2) содержать оценку эффективности системы внутреннего контроля и процедур финансовой отчетности, выставленную на конец текущего финансового года для данной корпорации».

	404(b): «В соответствии с оценкой системы внутреннего контроля, требуемой подсекцией (а), каждая зарегистрированная публичная бухгалтерская фирма, которая готовит или выпускает отчет об аудите данной корпорации, должна аттестовать и включить в отчет оценку системы внутреннего контроля, выставленную менеджментом корпорации. Аттестация должна быть проведена в соответствии со стандартами аттестации, выпущенными или одобренными Советом».
Секция 802. Уголовная ответственность за фальсификацию документов. 802(a). Общие.	§1520(a).(1): «Каждый бухгалтер, осуществляющий аудит, ... должен хранить все документы, касающиеся аудита, не менее 5 лет с момента окончания финансового года, в котором был произведен аудит».
	§1520(a).(2): Организации обязаны хранить все записи, рабочие документы и другие данные, которые имеют отношение к аудиту, а также корреспонденцию и электронные документы, которые были созданы, получены или отправлены компанией, могут пригодиться для аудита, содержат выводы, мнения, анализы, финансовые сведения о компании.
Секция 1102. Искажение записей или другое препятствование расследованию. 1102(2):	1102(2): «Любой, кто изменяет, уничтожает, искажает или скрывает запись, документ или другой объект, или пытается это сделать с тем, чтобы нарушить целостность объекта или его доступность при проведении официального расследования ... должен быть оштрафован согласно этой статье или лишен свободы на срок до 20 лет, или и то и другое одновременно».

Немецкий Кодекс корпоративного управления

В сентябре 2001 года в Германии была создана Правительственная комиссия по разработке Немецкого Кодекса корпоративного управления («[German Corporate Governance Code](#)»). 26 февраля 2002 года этот Кодекс был разработан, а 26 июля 2006 в результате принятия соответствующего закона Кодекс стал обязательным для исполнения корпорациями, акции которых котируются на немецких биржах. Среди всего прочего Немецкий Кодекс требует от высших исполнительных лиц создать систему оценки и управления рисками, а от аудиторов – убедиться в наличии системы внутреннего контроля.

Немецкий Кодекс корпоративного управления пересматривается ежегодно. Комиссия вносит поправки, а также включает в Кодекс предложения, не обязательные для исполнения. Последняя версия Немецкого Кодекса была принята 12 июня 2006 года, причем все новые поправки уже вступили в силу. Более подробная информация о Немецком Кодексе доступна на [сайте](#) Правительственной Комиссии.

В таблице ниже (см. таб. 5) просуммированы требования закона немецкого Кодекса в рамках внутреннего контроля над финансовой отчетностью и активами публичной компании.

Таб. 5. Требования к системе внутреннего контроля в рамках немецкого Кодекса	
Глава 4. Совет управляющих. 4.1. Задачи и обязанности.	4.1.4. «Совет Управляющих должен убедиться в наличии эффективной системы управления рисками и контроле рисков в корпорации».

Кодекс корпоративного управления ФСФР

Наконец, соответствующий свод правил есть и в России – «[Кодекс корпоративного управления ФСФР](#)» (Кодекс ФСФР). По сравнению с американским законом SOX, британским и немецким Кодексами российский нормативный акт является полностью добровольным и намного более подробным. Сама ФСФР объясняет такой высокий уровень детализации тем, что ее Кодекс пытается восполнить недостаточный объем действующей в России нормативно-правовой базы, регулирующей процесс корпоративного управления. При этом добровольный характер Кодекса ФСФР продиктован тем, что на момент принятия в 2002 году, в стране еще не сформировалась необходимая корпоративная культура, чтобы сделать такой документ обязательным. Тем не менее, есть все основания полагать, что в ближайшие годы будет принята новая версия Кодекса ФСФР, которая станет обязательной для исполнения корпорациями, чьи акции котируются на российских биржах.

В таблице ниже (см. таб. 6) просуммированы требования российского Кодекса ФСФР в рамках внутреннего контроля над финансовой отчетностью и активами публичной компании.

Таб. 6. Требования к системе внутреннего контроля в рамках российского Кодекса ФСФР	
Принцип №7: «Практика корпоративного поведения должна обеспечивать эффективный контроль над финансово-хозяйственной деятельностью общества с целью защиты прав и законных интересов акционеров».	Гл.8 п.(2): установление и обеспечение соблюдения эффективных процедур внутреннего контроля;
	Гл.8 п.(3): ...предупреждение и пресечение злоупотреблений со стороны исполнительных органов и должностных лиц общества;
	Гл. 8 п.(4): предупреждение, выявление и ограничение финансовых и операционных рисков;
	Гл.8 п.(5): обеспечение достоверности финансовой информации, используемой либо раскрываемой обществом.

Выводы

Анализ положений рассмотренных выше кодексов позволяет утверждать, что каждый из них выдвигает те или иные требования к системе внутреннего контроля и/или управления рисками в публичной компании. Если принять во внимание все стимулы, побуждающие к внедрению кодексов, то у современной компании практически не остается выбора, кроме как следовать по пути лучших практик и внедрять даже необязательные принципы корпоративного управления. Конкурентоспособность и успех приходят к тем компаниям, которые берут на вооружение передовой опыт и создают процедуры внутреннего контроля над финансовой отчетностью и корпоративными активами. В следующей главе будет рассмотрена функциональность продукта DeviceLock в контексте требований различных кодексов.

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 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 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.

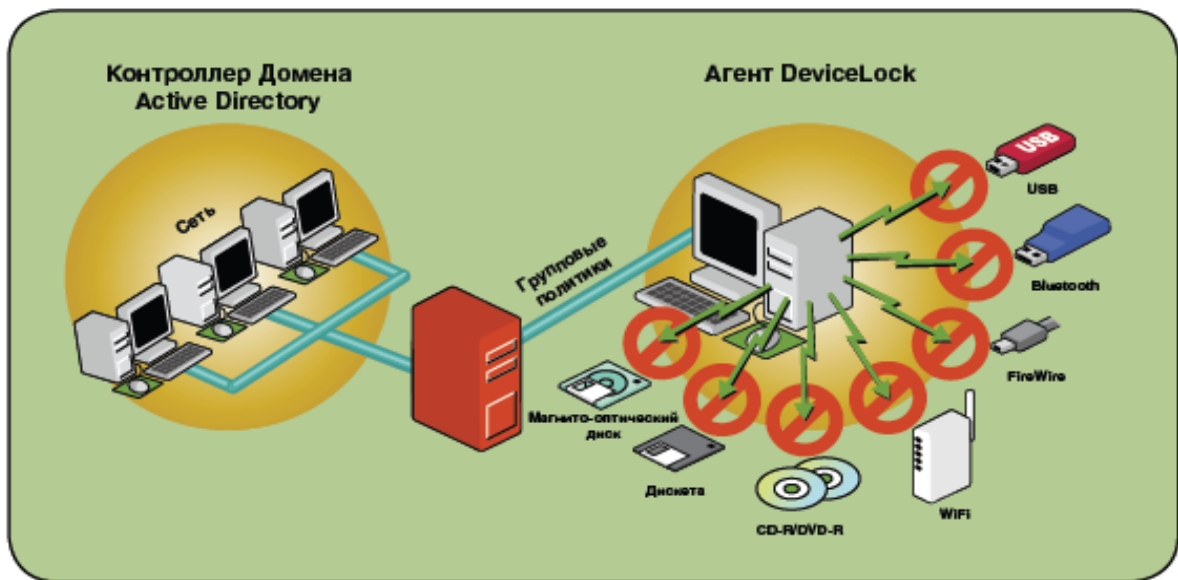


Рис. 1. Схема работы DeviceLock

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

Возможности DeviceLock для создания системы внутреннего контроля

Продукт DeviceLock осуществляет контроль над передачей 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 каждого кодекса корпоративного управления: 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. 7) просуммирована функциональность DeviceLock в соответствии с требованиями различных кодексов.

Таб. 7. Соответствие DeviceLock требованиям кодексов	
Кодекс	Возможности DeviceLock
Принципы корпоративного управления ОЭСР (страны-члены ОЭСР)	При помощи продукта DeviceLock публичная компания может построить систему внутреннего контроля, которая минимизирует риск несанкционированной утечки данных (следовательно, и информационных активов) через локальные коммуникации рабочих станций (этого требует пункт D.7). Тем самым корпорация, взявшая на вооружение DeviceLock, минимизирует часть операционных рисков, связанных с утечкой данных, что является требованием пункта D.7.
Принципы корпоративного управления Euroshareholders (Евросоюз)	Часть V данного Кодекса требует от публичных компаний внедрить систему внутреннего контроля и управления рисками. DeviceLock как раз и является необходимой частью такой системы, так как он, во-первых, позволяет значительно снизить риск несанкционированной утечки через локальные коммуникации рабочей станции, а во-вторых, обеспечивает теневое копирование данных, покидающих корпоративную сеть через порты, беспроводные сети и съемные носители на рабочих станциях.
Объединенный Кодекс корпоративного управления (Британия)	При помощи DeviceLock публичная компания может обеспечить соответствие пункту C.2.1 Объединенного Кодекса, в соответствии с которым в компании должна быть создана система внутреннего контроля. Как уже указывалось выше, продукт минимизирует риск утечки на уровне рабочей станции, ведет журналы событий, необходимые для успешного аудита, а также организует теневое копирование данных, покидающих сеть через локальные коммуникации рабочей станции. Подробнее о соответствии функциональности DeviceLock требованиям Объединенного Кодекса смотрите специальную White Paper на эту тему.
Немецкий Кодекс корпоративного управления (Германия)	Немецкий Кодекс, в отличие от других кодексов, не концентрируется на системе внутреннего контроля, зато требует внедрения системы управления рисками, в том числе, операционными рисками. В данном контексте DeviceLock позволяет достичь соответствия с требованиями пункта 4.1.4: т.е. построить систему управления операционным риском, минимизировав риски несанкционированной утечки через съемные носители, порты или беспроводные сети.
Sarbanes-Oxley Act of 2002, SOX (США)	<p>Продукт DeviceLock является элементом системы внутреннего контроля, обеспечивая контроль над перемещением данных через локальные порты и интерфейсы рабочих станций. Вдобавок, продукт позволяет реализовать гибкую политику безопасности при работе с КПК, смартфоном и коммуникатором, разрешив одни операции, но запретив другие. Тем самым DeviceLock минимизирует риск утечки данных, включая информационные активы, что является важным требованием секции 404 закона SOX.</p> <p>Более того, теневое копирование данных, покидающих корпоративную сеть через порты рабочей станции, внешние устройства и носители, а также беспроводные сети – это важная 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, что соответствует требованиям секции 802. Подробнее о соответствии функциональности DeviceLock требованиям закона SOX смотрите специальную White Paper на эту тему.</p>

<p align="center">Кодекс корпоративного управления ФСФР (Россия)</p>	<p>Кодекс ФСФР требует от публичных компаний создать и внедрить систему внутреннего контроля (пункт 8.2), которая позволит минимизировать риски злоупотребления информационными активами. Именно эту функцию выполняет DeviceLock в контексте несанкционированных утечек через рабочие станции. Кроме того, Кодекс ФСФР требует минимизировать операционные риски и создать всестороннюю систему управления рисками (пункт 8.4), что отвечает функциональности DeviceLock: защита от утечек данных является необходимой частью любой системы управления операционными рисками.</p>
---	--

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) 967-9960, +7 (495) 366-21-93 (контактное лицо – Анастасия Дементьева)

Отдел продаж: sales@smartline.ru

Тех. поддержка: support@smartline.ru