

# DeviceLock для соответствия соглашению Basel II



## Оглавление:

- [Введение](#)
- [Требования Basel II](#)
- [Оценка операционных рисков](#)
- [DeviceLock от Смарт Лайн Инк](#)
- [Возможности DeviceLock в рамках Basel II](#)
- [О компании Смарт Лайн Инк](#)
- [Контактная информация](#)

## Введение

Соглашение Basel II («Международная конвергенция измерения капитала и стандартов капитала: новые подходы»<sup>1</sup>) предъявляет требования к минимальному размеру банковского капитала. В соответствии с его требованиями финансовые компании обязаны оценивать операционные, рыночные и кредитные риски, а также резервировать капитал на их покрытие.

Часть этих требований особенно в сфере кредитных и рыночных рисков уже была отражена в первой итерации соглашения. Поэтому одним из ключевых нововведений Basel II является то, что банки обязаны управлять еще и операционным риском, в состав которого входят угрозы информационной безопасности и вредоносных действий сотрудников.

Чем эффективнее банк управляет операционным риском, тем меньшее количество капитала он обязан резервировать под реализацию этого риска. Тем самым, в распоряжении банка остается больше свободных средств, что положительно сказывается на его конкурентоспособности.

В данном документе будут проанализированы требования Basel II в сфере операционных рисков, структура этих рисков и их влияние на информационную инфраструктуру компании. Кроме того, будут рассмотрены возможности продукта DeviceLock компании Смарт Лайн Инк, при помощи которого банк может существенно снизить ту часть операционных рисков, которая приходится на угрозы информационной безопасности.

## Требования Basel II

Согласно пункту 644 соглашения Basel II, операционный риск определяется как «риск убытка в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий». Это определение включает юридический риск, но исключает стратегический и репутационный риски.

Легко видеть, что в определение операционных рисков попадают, прежде всего, угрозы информационной безопасности, реализующиеся в результате взаимодействия сотрудников и информационных систем банка. Например, вредоносные действия инсайдеров (кража конфиденциальной информации, мошенничество, халатность и безалаберность) входят в состав операционного риска и могут причинить банку существенный ущерб. Внутренние нарушители могут выкрасть конфиденциальные отчеты компании или приватные данные ее клиентов.

---

<sup>1</sup> Официальный перевод соглашения Basel II от Банка России доступен по адресу: <http://www.cbr.ru/today/PK/print.asp?file=Basel.htm>

В соответствии с пунктом 644 соглашения Basel II репутационные риски не входят в состав операционных. Следовательно, эти риски не влияют на требования к достаточности капитала. Тем не менее, согласно первому принципу надзорного процесса<sup>2</sup> и его третьему положению<sup>3</sup>, «в процессе оценки достаточности капитала должны учитываться все существенные риски, с которыми сталкивается банк». Далее, в пункте 732, Базельский Комитет указывает, что «в процессе оценки достаточности капитала должны учитываться все существенные риски, с которыми сталкивается банк». Согласно пункту 742, в состав этих «существенных рисков» обязательно должны входить репутационные риски. Хотя Базельский Комитет признает, что этот вид рисков «нелегко поддается измерению», он все же рекомендует разработать способы управления репутационным риском. Таким образом, от банков требуется приложить все усилия, чтобы обеспечить максимально эффективное управление, в том числе, репутационными рисками.

Следует отметить связь операционных и репутационных рисков. Например, успешная реализация многих инсайдерских угроз, которые напрямую относятся к операционным (согласно пункту 644), может привести к дополнительным отрицательным последствиям в виде ущерба имиджу и потери репутации, что подтверждает последнее исследование Deloitte<sup>4</sup>. Если произойдет утечка конфиденциальной информации, инсайдеры ограбят клиентов банка и т.д., то об этом может стать известно широкой общественности. В результате имидж компании может сильно испортиться, что приведет к сокращению клиентской базы и снижению прибылей. Другими словами, репутационные риски могут быть прямым следствием реализации операционных угроз.

Таким образом, соглашение Basel II требует от банка управлять операционными рисками, в состав которых, по определению, входят угрозы информационной безопасности в целом и инсайдерские риски в частности. Кроме того, нормативный документ рекомендует банку обеспечить управление репутационным риском, наступление которого зачастую является следствием реализации внутренних угроз информационной безопасности.

### **Оценка операционных рисков**

Согласно пункту 645, соглашение Basel II представляет три метода расчета требований к капиталу под операционный риск с учетом возрастания сложности и чувствительности риска: базовый индикативный подход, стандартизованный подход и усовершенствованные подходы (AMA - Advanced Measurement Approaches). Предполагается, что банки будут перемещаться вдоль цепочки возможных подходов по мере разработки более продвинутых систем и практики измерения операционного риска.

Самой простой методикой является **базовый индикативный подход**. Согласно пункту 649, в рамках этой методологии банки должны поддерживать капитал под операционный риск, равный среднему показателю за предыдущие три года, выраженному в фиксированных процентах положительного ежегодного валового дохода. Показатели за любой год, в котором ежегодный валовой доход был отрицательным или нулевым, должны исключаться как из знаменателя, так и из числителя при расчете среднего значения.

Чтобы перейти к **стандартизованному подходу**, банк, согласно пункту 660, должен доказать органам надзора, что он удовлетворяет трем основным условиям. Во-первых, совет директоров и старший менеджмент банка активно участвуют в надзоре за

---

<sup>2</sup> Первый принцип звучит следующим образом: «Банки должны иметь процедуры оценки общей достаточности капитала относительно характера своего риска и стратегию поддержания уровня этого капитала».

<sup>3</sup> Третье положение называется «Всесторонняя оценка рисков».

<sup>4</sup> Подробнее смотрите отчет Deloitte и Ponemon Institute "Enterprise@Risk: 2007 Privacy & Data Protection Survey".

[http://www.deloitte.com/dtt/cda/doc/content/us\\_risk\\_s%26P\\_2007%20Privacy10Dec2007final.pdf](http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf)

механизмом управления операционными рисками. Во-вторых, банк имеет концептуально надежную и адекватно реализованную систему управления операционными рисками. В-третьих, банк имеет достаточные ресурсы для использования подхода в основных бизнес-линиях<sup>5</sup>, а также в области контроля и аудита.

Формальные требования для **усовершенствованной методики (АМА)** отличаются от перечисленных выше условий тем, что система управления операционными рисками должна быть не просто «адекватно реализованной», а «полностью внедренной» (пункт 664). При этом банк должен иметь независимое подразделение (функцию), отвечающее за разработку и внедрение механизма управления операционными рисками. Помимо этого внутрибанковская система оценки операционных рисков должна быть тесно интегрирована с текущими процессами управления рисками в банке, а ее результаты – составлять неотъемлемую часть процесса мониторинга и контроля структуры операционных рисков банка. Например, эта информация должна играть существенную роль при составлении отчетов о рисках, управленческих отчетов, внутреннем распределении капитала и анализе рисков.

Использование усовершенствованной методики (АМА) также предполагает регулярное представление отчетности об операционных рисках и убытках менеджменту бизнес-подразделений, старшему менеджменту и совету директоров. Другими словами, банк должен отслеживать реализацию операционного риска и иметь возможность оценить нанесенный ущерб.

Более того, банк должен иметь процедуру принятия мер в соответствии с информацией, содержащейся в управленческих отчетах. Следовательно, банковская система управления операционными рисками должна быть хорошо документирована, а сам банк должен иметь механизм соблюдения документированных внутренних стратегий, процедур контроля и управления операционными рисками, включая меры на случай их несоблюдения.

Особую роль Базельский Комитет отводит внутренним или внешним аудиторам, которые должны регулярно проверять процессы управления и систем оценок операционных рисков. При этом проверяется деятельность как бизнес-подразделений, так и самостоятельного подразделения по управлению операционным риском.

Чем более сложную систему управления операционным риском использует банк в рамках Basel II, тем точнее ему удастся оценить потенциальные убытки вследствие реализации этого риска и тем меньше величина этих возможных убытков. Другими словами, банку выгодно двигаться вдоль цепочки возможных подходов по мере разработки более продвинутых систем и практики измерения операционного риска.

## **DeviceLock от Смарт Лайн Инк**

Продукт DeviceLock разработан российской компанией ЗАО «Смарт Лайн Инк». Он предназначен в первую очередь для минимизации рисков внутренней информационной безопасности и, помимо этого, помогает компаниям достичь соответствия наиболее сложным требованиям нормативных актов.

С помощью DeviceLock предприятия любого масштаба могут обеспечить всесторонний контроль над информацией, покидающей корпоративную сеть через порты рабочих станций, беспроводные сети и внешние накопители. Продукт также включает в себя защиту от аппаратных шпионов, подсоединяющихся между клавиатурой и системным блоком компьютера и использующихся для кражи ценной информации с рабочих станций

---

<sup>5</sup> Принципы распределения видов деятельности банка по бизнес-линиям изложены в Приложении 6 соглашения Basel II.

служащих. Таким образом, DeviceLock минимизирует наиболее опасную часть операционных рисков.

Ключевой особенностью DeviceLock является не только контроль над локальными коммуникациями компьютеров в соответствии с заданными политиками, но еще и полное теневое копирование всех исходящих данных. В отличие от огромного количества решений для хранения почтовой корреспонденции, DeviceLock позволяет собирать и анализировать информацию, покинувшую корпоративную сеть через порты рабочей станции. Таким образом, продукт регистрирует все необходимые записи для аудита в соответствии с Basel II и учета инцидентов в результате реализации угроз информационной безопасности. Тем самым обеспечивая банку информационную базу для оценки убытков и выявления причин реализации риска.

Следует отметить гибкость DeviceLock в работе с мобильными устройствами (КПК, смартфонами и различными коммуникаторами). Продукт не просто поддерживает теневое копирование всех данных, передаваемых на 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.

Таким образом, DeviceLock 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 и портов: USB-устройства, дисководы, CD/DVD-приводы, FireWire, инфракрасные, параллельные и последовательные порты, Wi-Fi и Bluetooth-адаптеры, ленточные накопители, КПК и смартфоны, любые внутренние и внешние сменные накопители и жесткие диски. DeviceLock обеспечивает 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

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

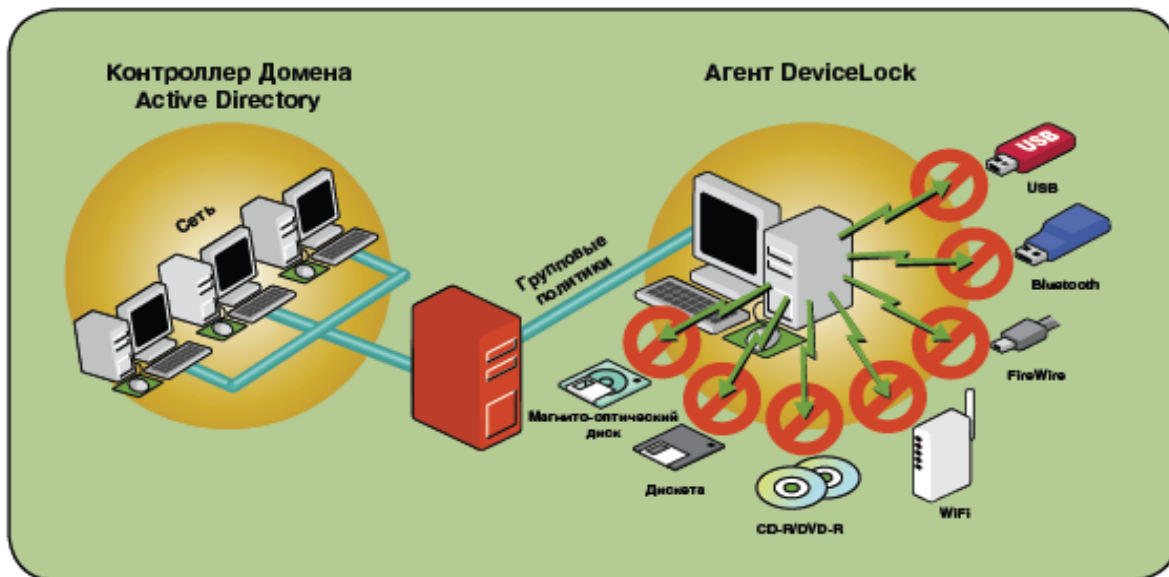


Рис. 1. Схема работы DeviceLock

При помощи DeviceLock предприятия могут легко защищать от неконтролируемых утечек данных десятки и сотни тысяч удаленных компьютеров, используя интегрированное управление через групповые политики Active Directory.

### Возможности DeviceLock в рамках Basel II

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, использование DeviceLock само по себе не создает дополнительных операционных рисков в банке, а все операции по конфигурированию и настройке политик продукта полностью регистрируются для аудита, что очень важно в контексте требований Basel II.

В целом, использование DeviceLock в корпоративной среде позволяет обеспечить соответствие двум ключевым положениям Basel II:

- **DeviceLock позволяет взять под контроль угрозы внутренней информационной безопасности, составляющие существенную часть операционного риска.** Как уже было показано ранее, действия инсайдеров, направленные на кражу конфиденциальной или приватной информации, входят в состав операционных рисков. Реализация таких угроз ведет к возникновению репутационных рисков, что лишь усугубляет ущерб. DeviceLock позволяет взять под контроль места и процессы взаимодействия пользователей с информационной системой через локальные коммуникации персональных компьютеров, эффективно противодействовать утечке данных и минимизировать этот ключевой элемент операционного риска.
- **DeviceLock позволяет собирать и анализировать информацию, покинувшую корпоративную сеть через рабочую станцию.** При помощи теневого копирования DeviceLock банк может легко отследить перемещение конфиденциальной информации, персональных и финансовых данных в случае, если они покинули сеть через съемные носители, мобильные устройства или подключения к беспроводным сетям. Тем самым банк может отследить реализацию операционного риска и в случае необходимости

оценить нанесенный ущерб. Эти сведения являются ключевыми для отчетности по рискам и нанесенным убыткам, которая должна быть реализована в соответствии с методиками Basel II.

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

<b>Таб. 1. Функциональность DeviceLock применительно к положениям Basel II</b>	
<b>Положения Basel II</b>	<b>Возможности DeviceLock</b>
<p><b>§40.</b> Расчет общих минимальных требований к капиталу [осуществляется] под кредитные, рыночные и операционные риски.</p>	<p>Если раньше банки управляли только кредитными и рыночными рисками, то теперь им следует взять под контроль еще и операционные риски. DeviceLock минимизирует наиболее опасную часть операционных рисков – угрозы информационной безопасности. При помощи DeviceLock банк может минимизировать риски утечки персональных и финансовых данных, конфиденциальной информации, а также попадания в корпоративную сеть нежелательных типов данных.</p>
<p><b>§644.</b> Операционный риск определяется как риск убытка в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий. Это определение включает юридический риск, но исключает стратегический и репутационный риски.</p>	<p>В соответствии с определением, угрозы информационной безопасности составляют существенную часть операционного риска. Более того, особое внимание Basel II уделяет внутренним угрозам, вызванным случайными или умышленными действиями персонала. Именно здесь на помощь банку приходит DeviceLock. С его помощью риски утечки информации можно взять под контроль. Тем самым банк заранее страхует себя от дополнительных репутационных рисков, которые, зачастую, являются следствием утечки приватных данных клиентов.</p>
<p><b>§645.</b> [Basel II] представляет три метода расчета требований к капиталу под операционный риск в процессе возрастания сложности и чувствительности к риску: базовый индикативный подход, стандартизованный подход и «усовершенствованные» подходы (AMA).</p>	<p>Чем сложнее методика, тем точнее удастся оценить риск и тем большую экономию получает банк. При помощи DeviceLock банк минимизирует часть операционного риска и создает механизмы аудита и отслеживания случаев наступления риска, например, при утечке конфиденциальной информации. Тем самым в распоряжении банка аккумулируются сведения, необходимые для ведения отчетности по операционным рискам и убыткам. Между тем, это необходимое требование для использования более сложных методик.</p>
<p><b>§666.</b> Банк должен удовлетворять следующим качественным стандартам, чтобы получить разрешение на использование AMA для расчета капитала под операционные риски:</p> <p><b>(с)</b> Отчетность об операционных рисках и убытках должна регулярно представляться менеджменту бизнес-подразделений, старшему менеджменту и совету директоров. Банк должен иметь процедуру принятия мер в соответствии с информацией, содержащейся в управленческих отчетах.</p>	<p>Теневое копирование DeviceLock позволяет сохранить копию всей информации, покинувшей корпоративную сеть, а также понять, кто, когда и каким образом эти сведения скопировал с рабочей станции. Этой информации достаточно, чтобы оценить ущерб от реализации операционного риска, что является важным требованием Basel II для банков, желающих перейти на использование самой эффективной методики оценки операционного риска.</p>

<p><b>§732.</b> В процессе оценки достаточности капитала должны учитываться все существенные риски, с которыми сталкивается банк, в том числе (согласно <b>§742</b>), репутационные риски.</p>	<p>Использование DeviceLock позволяет минимизировать репутационные риски банка, природа которых, во многом, зависит от операционных рисков. При помощи DeviceLock банк может минимизировать самую опасную операционную угрозу – утечку конфиденциальной информации. Между тем, именно кража, несанкционированное разглашение и утечка чувствительных сведений служат источником наиболее опасных репутационных рисков, в некоторых случаях граничащих с банкротством.</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 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](mailto:sales@devicelock.com)

Тех. поддержка: [support@devicelock.com](mailto:support@devicelock.com)