# DeviceLock для соответствия Стандартам Банка России по Информационной Безопасности


**Оглавление:**



## Введение

Защита информации в банковском бизнесе регулируется целым рядом нормативных актов и надзорных органов. Так, Россвязькомнадзор контролирует безопасность персональных данных в соответствии с федеральным законом № 152 «О персональных данных», а международные платежные системы Visa и Mastercard следят за соответствием стандарту PCI DSS[1] (Payment Card Industry Data Security Standard) для защиты информации о банковских картах.

Однако ключевыми нормативами, регулирующими информационную безопасность (ИБ) в российской банковской отрасли, являются следующие Стандарты Банка России:

- «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Общие положения**» (в дальнейшем – «Общие положения»);

- «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Аудит информационной безопасности**» (в дальнейшем – Стандарт по аудиту);

- «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Методика оценки соответствия** информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС – 1.0 - 2006» (в дальнейшем – «Методика оценки соответствия»).

По состоянию на начало 2009 года все три Стандарта Банка России по-прежнему носят рекомендательный характер. Однако, де-факто Стандарты рассматриваются многими действующими в России банками как обязательные. Некоторые финансовые организации уже реализовали соответствие требованиям Стандартов, другие – находятся в начале этого пути. При этом практически все кредитные организации уже ознакомились с положениями документов и запланировали работы по внедрению стандартов и аудиту соответствия.

[1] https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf.

Еще одним важным фактором для внедрения Стандартов Банка России является соглашение Basel II, согласно которому банки обязаны управлять операционными рисками, включающими в себя риски ИБ, и резервировать под них капитал. В этой связи положения Стандартов Банка России можно рассматривать как «дорожную карту» для эффективного управления операционным риском и обеспечения соответствия нормативам более высокого уровня.

В данном документе будут рассмотрены положения трех ключевых Стандартов Банка России, а также возможности программного продукта DeviceLock производства компании Смарт Лайн Инк, при помощи которого организация сможет гораздо эффективнее достичь соответствия этим Стандартам. Документ состоит из трех основных частей.

Во второй главе документа («Структура и область применения Стандартов») приводится общее описание Стандартов: их терминология, структура, взаимосвязь, а также основная концепция (парадигма).

В следующей главе («Обзор продукта DeviceLock») описываются функциональные возможности продукта DeviceLock без привязки к требованиям Стандартов.

Четвертая глава документа («Стандарты Банка России и система защиты информации DeviceLock») является ключевой и содержит в себе последовательное описание требований трех основных Стандартов Банка России и функциональных возможностей продукта DeviceLock применительно к этим требованиям.

В пятой главе («Выводы») резюмируются результаты предыдущих разделов и формулируются основные итоги.

В последующих главах документа приведены два приложения к документу («Основные изменения СТО БР ИББС – 1.0 – 2008» и «Методика расчета оценки соответствия»), а также информация о компании Смарт Лайн Инк и контактные сведения.

**История, структура и область применения Стандартов**

Первая версия «Общих положений» Стандарта Банка России по ИТ-безопасности (СТО БР ИББС-1.0 2004) была представлена Банком России в конце 2004 года. При подготовке этого Стандарта была проведена всесторонняя работа по изучению лучших зарубежных практик, и, как следствие, уже в первой версии документа прослеживались характерные черты различных иностранных нормативов. В частности, Стандарт использовал подходы, заложенные в американских актах SOX[1] (Sarbanes-Oxley Act) и GLBA[2] (Gramm-Leach-Bliley Act), международных стандартах по управлению ИБ (ISO 17799[3], 13335[4]) и даже методиках управления рисками OCTAVE[5] и CRAMM[6].

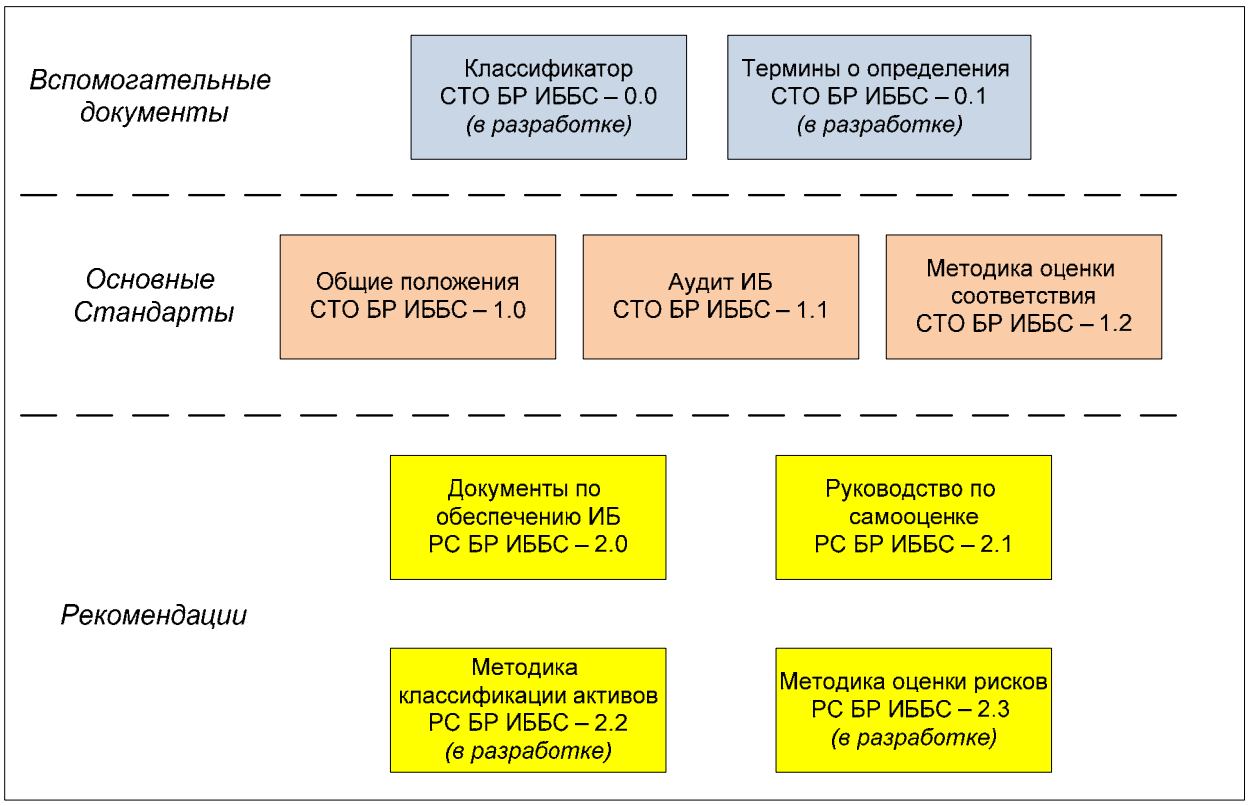
Изначально был разработан только основной нормативный документ («Общие положения»), вторая версия которого была представлена в начале 2006 года. В следующем 2007 году был опубликован ряд поясняющих документов: Стандарт по аудиту ИБ, Методика оценки соответствия, а также рекомендации к документации по обеспечению ИБ и проведению самооценки. Наконец, в конце 2008 года был представлен проект последней на сегодняшний день версии основного Стандарта - «Общих положений».

---

[1] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf
[2] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf
[3] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612
[4] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066
[5] http://www.cert.org/octave
[6] http://www.cramm.com/

Таким образом, общая современная структура Стандартов Банка России приняла вид, представленный на рис. 1. Большинство указанных на схеме документов уже официально опубликованы, а остальные пока находятся в разработке.

**Рис. 1. Структура Стандартов Банка России по ИТ-безопасности[1]. Источник: ABISS.**




Согласно «Общим положениям» (глава 1), «[…] стандарт распространяется на организации банковской системы Российской Федерации (далее — организации БС РФ) и устанавливает положения по обеспечению информационной безопасности в организациях БС РФ». На данный момент Стандарт имеет рекомендательный характер: «положения настоящего стандарта применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена действующим законодательством Российской Федерации, нормативным правовым актом Банка России или условиями договоров, заключенными организациями БС РФ». При этом отдельно подчеркивается, что «[…] стандарт может быть введен в действие организацией БС РФ в качестве обязательного к исполнению в случае, если такая необходимость существует».

Основным органом, регулирующим применение Стандартов, является Банк России. Вместе с тем, говорить о внедрении Стандартов невозможно без упоминания Сообщества ABISS[2] (Association for Banking Information Security Standards). Это самодеятельное российское сообщество организаций, деятельность которого направлена на развитие и продвижение Стандартов а также регулирование работы организаций-участников по оценке соответствия «Общим положениям» Стандарта. В состав Сообщества ABISS входят российские и международные консалтинговые компании, образовательные учреждения, системные интеграторы, а также сами российские банки, которые планируют внедрять Стандарт. Сообщество ABISS имеет утвержденные регламенты взаимодействия с Банком России, и его члены готовы консультировать и обучать банки по вопросам внедрения

[1] По состоянию на начало 2009 года.
[2] http://abiss.ru/

Стандартов. Более того, только оценка соответствия Стандарту, выполненная консультантами ABISS, будет принята Банком России, как заслуживающая доверия.

**Терминология Стандартов**

Прежде, чем говорить о конкретных требованиях регулирующих документов, необходимо определиться с терминологией. Планируется, что термины Стандартов будут прописаны в отдельном документе, однако на данный момент он находится в разработке. Тем не менее, предварительный список основных определений уже опубликован в главе 3 «Общих положений» Стандарта, а наиболее важные из них приводятся в таблице 1:

**Таб. 1. Терминология Стандартов Банка России по ИБ**

| Термин (в соответствии с нумерацией Стандарта) | Определение |
|---|---|
| 3.20. Угроза | Опасность, предполагающая возможность потерь (ущерба). |
| 3.21. Риск | Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы. |
| 3.23. Информационный актив | Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации банковской системы Российской Федерации; находящаяся в распоряжении организации БС РФ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме. |
| 3.37. Система информационной безопасности (СИБ) | Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение. |
| 3.38. Система менеджмента информационной безопасности (СМИБ) | Часть менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ. |
| 3.39. Система обеспечения информационной безопасности (СОИБ) | Совокупность СИБ и СМИБ организации БС РФ |
| 3.43. Угроза ИБ | Угроза нарушения свойств ИБ - доступности, целостности или конфиденциальности информационных активов организации БС РФ. |
| 3.44. Уязвимость ИБ | Слабое место в инфраструктуре организации БС РФ, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ. |
| 3.45. Ущерб [ИБ] | Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации БС РФ, наступивший в результате реализации угроз ИБ через уязвимости ИБ. |
| 3.46. Инцидент ИБ | Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, т.е. реализацию нарушения свойств ИБ информационных активов организации БС РФ. |

| | |
|---|---|
| 3.47. Нарушитель ИБ | Субъект, реализующий угрозы ИБ организации БС РФ, нарушая предоставленные ему полномочия по доступу к активам организации банковской системы Российской Федерации или по распоряжению ими. |
| 3.48. Модель нарушителя ИБ | Описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей. |
| 3.49. Модель угроз ИБ | Описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба. |

**Общая концепция (парадигма) Стандартов**

Суть и основная концепция Стандартов Банка России неразрывна связана с его основными задачами, которые формулируются в вводной главе «Общих положений». По мнению составителей документа, «особенности БС РФ таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов». Именно поэтому организации БС РФ должны «обеспечить достаточный уровень ИБ», а «деятельность, относящаяся к обеспечению ИБ, должна контролироваться». В связи с этим, «Банк России является сторонником регулярной оценки уровня ИБ в организациях БС РФ, оценки риска нарушения ИБ и принятия мер, необходимых для управления этим риском».

Другими словами, Стандарты Банка России представляют собой набор рекомендаций по управлению рисками ИБ в организациях БС РФ, а также методик проверки соответствия этим рекомендациям. Именно проблематика управления рисками, а не информационной безопасности как таковой, прослеживается практически во всех нормативных документах Банка России. Стандарты не предписывают организациям внедрять конкретные технологии или использовать конкретные инструментальные средства – они действуют на более высоком уровне, выдвигая требования к общему риск-ориентированному подходу. В дальнейшем каждая организация может реализовать этот подход по-разному, принимая, отклоняя или минимизируя риски с помощью тех или иных средств защиты.

Строгое определение риска информационной безопасности дается на базе определений 3.20, 3.21, 3.22, 3.43 (см. таб. 1). Риск информационной безопасности – это некая мера, учитывающая вероятность реализации угрозы нарушения свойств ИБ (доступности, целостности или конфиденциальности) информационных активов кредитной организации. Под «информационным активом» понимается информация, обладающая следующими свойствами:

- наличие реквизитов, позволяющих ее идентифицировать;
- ценность для организации БС РФ;
- местонахождение на неком материальном носителе в пределах БС РФ.

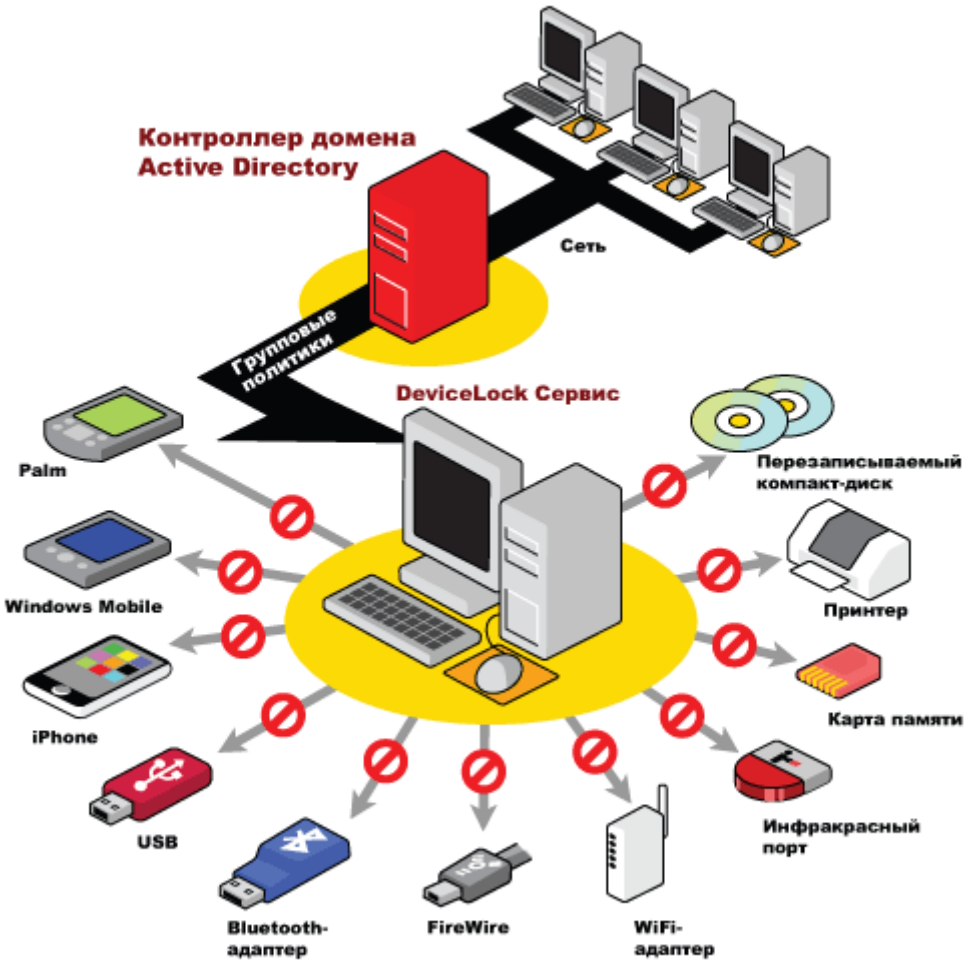
Таким образом, с каждым риском информационной безопасности ассоциированы сразу несколько атрибутов: угроза информационной безопасности, информационный актив, а также нарушитель информационной безопасности. Чтобы достичь соответствия Стандартам, организация должна построить систему управления рисками ИБ, то есть – она должна знать свои информационные активы, понимать угрозы и следить за возможными

нарушителями ИБ. Все перечисленные задачи решаются с помощью всеобъемлющей Системы Обеспечения ИБ (СОИБ), которая состоит из низкоуровневой СИБ (Системы ИБ) и высокоуровневой СМИБ (Системы Менеджмента или Управления ИБ).

### Обзор продукта DeviceLock от компании Смарт Лайн Инк

Программный комплекс DeviceLock производства российской компании Смарт Лайн Инк – это система централизованного контроля доступа пользователей корпоративных информационных систем (ИС) к периферийным устройствам и портам ввода-вывода персональных компьютеров и серверов под управлением операционных систем Microsoft Windows. С помощью DeviceLock предприятия любого масштаба могут обеспечить всесторонний контроль над данными, покидающими корпоративную сеть через порты рабочих станций, сменные накопители и беспроводные сети, а также эффективно противодействовать инсайдерским утечкам информации ограниченного доступа с персональных компьютеров сотрудников и серверов организации.

**Рис. 2. Схема работы DeviceLock.**




С функциональной точки зрения, комплекс DeviceLock состоит из трех частей:

- 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.

- 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.

- 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.

К основным функциям контроля DeviceLock относятся управление доступом к операциям передачи данных и форматирования носителей, событийное протоколирование действий пользователей и администраторов, теневое копирование передаваемых с компьютера данных, а также обнаружение и блокировка работы аппаратных USB и PS/2 кейлоггеров. В дополнение к основным функциям при наличии на защищаемом компьютере совместимых средств криптографической защиты (СКЗИ) DeviceLock предотвращает несанкционированное копирование нешифрованных данных на съемные устройства памяти.

Относящийся к классу контекстных (context-aware) систем предотвращения утечек данных с оконечных вычислительных устройств (Endpoint Data Leak Prevention), DeviceLock позволяет управлять доступом пользователей ко всем типам интерфейсов и периферийных устройств компьютеров корпоративной информационной системы (ИС), включая USB, FireWire, COM, LPT, IrDA порты, а также жесткие диски, флоппи-дисководы, CD/DVD-приводы, съемные накопители, КПК и смартфоны, локальные и сетевые принтеры, устройства Wi-Fi, Bluetooth и т.п.

DeviceLock обеспечивает контроль всех видов локальных каналов потенциальной утечки данных с компьютеров, включая операции файловой системы со съемными накопителями и другими типами PnP устройств, обмен данными по протоколам синхронизации с КПК и смартфонами, а также канал печати документов.

В DeviceLock поддержаны времязависимые политики, что позволяет контролировать доступ пользователей и их групп к устройствам и портам ввода-вывода с точностью до часа и дня в рамках недельного графика. Кроме того, для каждого пользователя или их группы можно задать индивидуальный «белый список» USB устройств (USB white listing), доступ к которым будет всегда разрешен вне зависимости от установленных политик доступа для других устройств аналогичных типов. Устройства в «белом списке» идентифицируются с точностью до модели и уникального экземпляра – с использованием его серийного номера. Также в DeviceLock поддержан «белый список» носителей: для каждого пользователя или группы можно идентифицировать индивидуальный CD/DVD-диск на основе записанных на него данных и разрешить его использование, даже если CD/DVD-привод заблокирован. Даже если с агентом DeviceLock невозможно установить сетевое соединение, пользователю можно обеспечить временный доступ к определенным периферийным устройствам, сообщив ему короткий буквенно-цифровой код разблокировки по телефону или иным средствам связи.

DeviceLock поддерживает разграничение операций обмена данными на уровне их типов: версия 6.4 продукта принципиально повышает уровень контроля за привилегиями и действиями пользователей за счет поддержки функции детектирования и фильтрации типов файлов для операций файловой системы. Используемый бинарно-сигнатурный метод позволяет определить тип файла по его реальному содержимому, а не по меткам или служебным метаданным - то есть, детектируется подлинная форма представления данных внутри файла. Технология обеспечивает распознавание более 3000 форматов и

легко расширяема. DeviceLock 6.4 поддерживает перехват, экстракцию, детектирование типа и блокирование файловых объектов во всех локальных каналах потенциальной утечки данных на компьютерах: через любые устройства хранения информации, а также при локальной синхронизации с мобильными устройствами и смартфонами на базе Windows Mobile. Для любого из этих каналов DeviceLock позволяет не только устанавливать ограничения на типы передаваемых файлов, но и задавать гибкие избирательные политики событийного протоколирования а также теневого копирования с точностью до типа файла.

Отличительной особенностью DeviceLock является способность фильтровать протоколы локальной синхронизации данных с любыми типами КПК и смартфонов под управлением ОС Windows Mobile® и Palm® OS вне зависимости от интерфейсов их подключения (USB, COM, IrDA, Bluetooth, WiFi). При этом обмен данными можно блокировать или разрешать на уровне типов объектов – таких, как файлы, контакты, почта, записи в календаре и т.д. С такой же гранулированностью поддерживается событийное протоколирование и теневое копирование операций локальной синхронизации.

Другая уникальная характеристика DeviceLock – поддержка централизованного контроля доступа пользователей к локальным, сетевым и виртуальным принтерам вне зависимости от интерфейса их подключения к компьютеру, включая любые не-USB интерфейсы. Для каждого отдельного компьютера в сети или их групп DeviceLock позволяет задать гибкие правила, определяющие кому, когда и на каких принтерах разрешено печатать. Разные прав доступа могут быть установлены к реальным (локальным и сетевым) и виртуальным принтерам – например, программам конвертации в PDF. Дополнительная степень гибкости достигается за счет возможности задать разные политики для принтеров, подключенных к разным интерфейсам: USB, LPT, Bluetooth, Wi-Fi. При подключении по USB разные правила доступа могут быть определены для каждой модели и каждого отдельного принтера.

В комплексе с несколькими популярными СКЗИ, включая продукты компаний Инфотекс, PGP, TrueCrypt и Lexar, DeviceLock позволяет предотвратить несанкционированный экспорт данных с корпоративных компьютеров на съемные устройства памяти в нешифрованном виде. Шифрование данных и все административные криптографические функции в таких интегрированных решениях реализуются совместимыми СКЗИ, а DeviceLock контролирует доступ пользователей к шифрованным и нешифрованным данным на внешних носителях. При этом DeviceLock распознает зашифрованные устройства хранения данных и позволяет централизованно устанавливать специальные права доступа к ним пользователей компьютера. С помощью таких политик можно, например, разрешить определенным пользователям запись только зашифрованных данных на съемные устройства и запретить запись незашифрованных данных. Одновременно и независимо от политик «шифрованного» доступа администратор безопасности может установить для тех же пользователей иные права доступа к нешифрованным съемным устройствам памяти, таким образом не ограничивая их штатное, в соответствии с установленной политикой ИБ организации, использование в служебных целях.

Гибкое и оперативное управление политиками доступа, протоколирования и теневого копирования агентов DeviceLock, установленных на защищаемых компьютерах, а также полным комплексом администрирования их жизненного цикла обеспечивается централизованно либо с выделенной платформы управления на базе одного или нескольких компонентов DeviceLock Enterprise Server, либо, если в организации используется платформа системного управления Microsoft Active Directory, через ее групповые политики (Group Policy Objects), для чего предоставляется специальная GPO-оснастка DeviceLock Group Policy Manager (GPM), полностью интегрированная в инфраструктуру Microsoft AD. Одно из принципиальных преимуществ DeviceLock GPM состоит в том, что его пользователи не должны выделять дополнительные финансовые и трудовые ресурсы на установку и эксплуатацию отдельной серверной платформы для

управления агентами DeviceLock, и, что не менее важно, масштабируемость DeviceLock GPM полностью определяется масштабом развернутой в организации Microsoft AD, таким образом автоматически обеспечивая потребности владельца.

Кроме того, в DeviceLock поддержано полнофункциональное задание исполняемых на агентах политик контроля доступа в режиме offline, когда компьютер находится вне корпоративной сети или серверы управления недоступны. При этом переключение между режимами онлайн и офлайн осуществляется агентом DeviceLock автоматически.

Событийное протоколирование и теневое копирование являются столь же важными функциональными характеристиками комплекса DeviceLock, как и управление доступом к интерфейсам и устройствам, поскольку позволяют администрации ИБ отслеживать поведение пользователей и административного персонала, проводить централизованный аудит а также обеспечивать доказательную базу для расследования инцидентов ИБ и участия в судебных разбирательствах.

DeviceLock поддерживает детальное протоколирование действий пользователей и административного персонала, а также теневое копирование с автоматическим централизованным сбором и хранением всех данных, копируемых с защищаемых компьютеров, в базе данных DeviceLock Enterprise Server. При этом политики сбора данных аудита и теневого копирования задаются централизованно с консоли DeviceLock Group Policy Manager или DeviceLock Enterprise Server – в зависимости от того, применяется ли у пользователя платформа Microsoft Active Directory. К уникальным преимуществам DeviceLock относится поддержка исполнительным агентом алгоритма автоматического выбора оптимального для передачи собранных протокольных данных на лог- сервер при наличии в системе нескольких таких серверов, а также возможность задать для агентов пределы пропускной способности (traffic shaping) канала передачи данных теневого копирования и лог-файлов в центральную базу данных.

Устанавливаемый на защищаемых компьютерах агент DeviceLock полностью защищен от удаления или выведения из строя в результате нештатных или деструктивных действий пользователей и локальных системных администраторов, а надежность, масштабируемость и высокое качество технической поддержки продукта подтверждены многолетней промышленной эксплуатацией в производственных условиях крупных российских и зарубежных организаций из самых разных отраслей экономики.

## Стандарты Банка России и система защиты информации DeviceLock

В следующих разделах документа приводятся конкретные требования различных Стандартов Банка России, а также функционал продукта DeviceLock применительно к этим требованиям. В общей сложности, будут рассмотрены три Стандарта – «Общие положения» (СТО БР ИББС – 1.0), «Аудит информационной безопасности» (СТО БР ИББС - 1.1) и «Методика оценка соответствия» (СТО БР ИББС – 1.2).

### Требования Стандарта «Общие положения»

Документ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Общие положения**» является базовым нормативом Банка России и содержит в себе высокоуровневые рекомендации к построению риск-ориентированной СОИБ. Последняя редакция[1] (СТО БР ИББС – 1.0 – 2008) документа состоит из введения и девяти основных глав, краткое описание которых приведено в таблице 2:

[1] Описание основных изменений СТО БР ИББС – 1.0 – 2008 по сравнению с СТО БР ИББС – 1.0 – 2006 приведено в приложении 1 к настоящему документу.

| Таб. 2. Структура Стандарта СТО БР ИББС – 1.0 – 2008 | |
|---|---|
| **Глава** | **Описание / краткое содержание** |
| Введение | Основные цели и задачи Стандарта, а также обоснование его необходимости |
| 1. Область применения | Область применения стандарта |
| 2. Нормативные ссылки | Ссылки на нормативные документы, использованные при создании Стандарта |
| 3. Термины и определения | Список терминов и определений, которые используются в Стандарте |
| 4. Обозначения и сокращения | Список обозначений и сокращений, которые используются в Стандарте |
| 5. Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций БС РФ | Ключевой раздел Стандарта, описывающий общую концепцию обеспечения информационной безопасности в организациях БС РФ. Задает базовые определения и положения риск-ориентированного подхода. Следующие разделы (6-8) конкретизируют концептуальные требования для разработки моделей угроз и нарушителей, а также создания СИБ и СМИБ организаций. |
| 6. Модели угроз и нарушителей информационной безопасности организаций БС РФ | Требования к моделям угроз и нарушителей, а также рекомендации для ее создания |
| 7. Система информационной безопасности организаций БС РФ | Требования к системе информационной безопасности (СИБ), а также рекомендации для ее построения |
| 8. Система менеджмента информационной безопасности организаций БС РФ | Требования к системе менеджмента информационной безопасности (СМИБ), рекомендации для ее построения, а также рекомендации к созданию и функционированию службы ИБ организации |
| 9. Проверка и оценка информационной безопасности организации БС РФ | Требования к процессам проверки и оценки соответствия положениям Стандарта. |

Из таб. 2 следует, что суть Стандарта сконцентрирована в пятой главе, которая описывает его общую концептуальную схему (парадигму). Некоторые положения этого раздела уже были сформированы в главе «Общая концепция (парадигма) Стандарта» данного документа. Тем не менее, на отдельных тезисах пятой главы следует остановиться подробнее:

- (основной принцип построения модели угроз – 1 , 5.4) **«Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами, либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности. Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ»**. Стандарт явно указывает, что значительные проблемы информационной безопасности организаций БС РФ связаны с деятельностью их собственных сотрудников;

- (определение важности модели угроз и нарушителей, 5.7) **«Один из главных инструментов собственника в обеспечении ИБ – основанный на опыте прогноз (составление модели угроз и модели нарушителя). Чем обоснованнее и точнее сделан прогноз, тем потенциально ниже риски нарушения ИБ организации БС РФ при минимальных ресурсных затратах».** Данное положение определяет разработку модели угроз и нарушителей как главный инструмент обеспечения ИБ в банковской организации;

- (определение важности политик ИБ, 5.8) **«Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации БС РФ – разработать политику ИБ организации БС РФ и в соответствии с ней реализовать, эксплуатировать и совершенствовать СОИБ организации БС РФ»**. Политики информационной безопасности являются вторым важнейшим элементом для построения СОИБ после модели угроз и нарушителей;

- (основной принцип построения модели угроз – 2 , 5.12) **«При разработке моделей угроз и моделей нарушителя необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все операции в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации должны особенно тщательно контролироваться»**. Данный тезис тесно перекликается с положением 5.4, однако носит более конкретный характер и подчеркивает важность контроля действий персонала;

- (принцип непрерывного совершенствования СОИБ, 5.23) **«СОИБ должна быть определена, спланирована и регламентирована в организации БС РФ. Однако, даже правильно выстроенные процессы и используемые защитные меры в силу объективных причин со временем имеют тенденцию к ослаблению своей эффективности. Это неминуемо ведет к деградации системы защиты и возрастанию рисков нарушения ИБ. Для поддержания системы защиты на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Менеджмент событий и инцидентов безопасности, полученных в результате мониторинга, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов»**. Согласно данному тезису, создание СОИБ является не однократным, а непрерывным действием, одним из элементов которого является мониторинг событий и инцидентов СИБ.

В следующих главах (6-8) Стандарта приводятся более конкретные требования к разработке моделей угроз и нарушителей и построению системы ИБ. В данном документе эти требования подробно не рассматриваются, поскольку они конкретизируют основные положения пятой главы (см. выше). Тем не менее, некоторые из них будут приведены при сопоставлении функционала DeviceLock с требованиями «Общих положений».

#### Возможности DeviceLock применительно к Стандарту «Общие положения»

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, настройки и политики DeviceLock легко подвержены аудиту, а сам продукт не создает дополнительных рисков информационной безопасности.

Использование DeviceLock в корпоративной среде позволяет обеспечить соответствие трем ключевым требованиям «Общих положений»:

- **(модель угроз и нарушителей, а также управление рисками)** Согласно положению 5.7, построение модели угроз и управление рисками являются основополагающими инструментами для создания системы обеспечения ИБ организации. Применение эффективных политик продукта DeviceLock по контролю доступа пользователей к локальным интерфейсам и периферийным устройствам рабочих станций позволяет минимизировать риски ИБ, связанные с угрозами внутренних – инсайдерских – утечек информационных активов. Это позволяет существенно упростить разработку адекватной модели угроз и, как следствие, повысить эффективность управление рисками ИБ;

- **(политики ИБ)** Согласно положению 5.8, политики информационной безопасности являются наиболее эффективным способом снизить возникающие риски. Продукт DeviceLock обеспечивает реализацию политик ИБ практически любой сложности и гибкости, связанных с доступом пользователей к съемным носителям, принтерам, мобильным устройствам и беспроводным сетям;

- **(совершенствование и мониторинг системы обеспечения ИБ)** Согласно положению 5.23, для поддержания эффективной системы защиты необходим постоянный мониторинг событий и инцидентов ИБ. Механизмы всестороннего событийного протоколирования и теневого копирования, поддержанные в DeviceLock, создают базис для эффективного мониторинга всех действий пользователей, связанных с копированием информации на съемные носители, использованием принтеров, а также синхронизацией данных с персональными мобильными устройствами.

В таблице далее (таб. 3) просуммирована функциональность DeviceLock в соответствии с требованиями «Общих положений»:

**Таб. 3. Функциональность DeviceLock применительно к требованиям Стандарта Банка России «Общие положения»:**

| Требования «Общих положений» | DeviceLock |
|---|---|
| **5.7.** Один из главных инструментов собственника в обеспечении ИБ – основанный на опыте прогноз (составление модели угроз и модели нарушителя). Чем обоснованнее и точнее сделан прогноз, тем потенциально ниже риски нарушения ИБ организации БС РФ при минимальных ресурсных затратах. | Составление модели угроз и нарушителей является комплексной задачей, которая пронизывает все бизнес-процессы организации. Зачастую для решения этой задачи компании не хватает собственной компетенции, и ей приходится нанимать специализированных консультантов.<br><br>Использование продукта DeviceLock позволяет обеспечить комплексный контроль действий пользователей в пределах рабочих станций, что, в свою очередь существенно упрощает построение модели угроз и нарушителей. Например, если политика безопасности компании запрещает копирование информации на съемные устройства, то использование DeviceLock минимизирует риск утечки через данный канал из общей модели угроз. |
| **6.1.** Модели угроз и нарушителей должны быть основным инструментом организации БС РФ при развертывании, поддержании и совершенствовании СОИБ. | |
| **6.11**. Хорошей практикой в организациях БС РФ является разработка моделей угроз и нарушителей ИБ для организации в целом, а также, при необходимости, для ее отдельных банковских процессов. | |

| | |
|---|---|
| **5.4.** Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами, либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности. Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ. | Стандарт Банка России совершенно справедливо обращает внимание на проблему инсайдеров. Многие банки пытаются не замечать угрозы со стороны внутренних нарушителей, однако игнорирование риска утечки персональных и/или финансовых сведений клиентов или злоупотребление ими может привести к многомиллионным потерям и испорченной репутации. Система DeviceLock ориентирована на решение именно этой наиболее важной, с точки зрения модели рисков и угроз, проблемы. Благодаря использованию DeviceLock минимизируются возможности внутренних нарушителей по хищению информации через порты рабочих станций, беспроводные сети, принтеры и мобильные устройства, а поддержка DeviceLock событийного протоколирования и теневого копирования обеспечивает юридическую документируемость и доказательность фактов попыток доступа и копирования конкретных данных.<br><br>С помощью DeviceLock компания может одним служащим разрешить доступ к съемным устройствам, а другим запретить. Такие внешние устройства являются средствами и системами автоматизации, а потому должны тщательно контролироваться. Благодаря DeviceLock все полномочия по работе с внешними носителями распределяются в соответствии с политикой ИБ, принципом минимальных привилегий и бизнес-ролями пользователей корпоративной ИС. При этом у компании создается необходимая документальная база для подтверждения достаточности внедренных процедур. Таким образом, DeviceLock является эффективным элементом системы внутреннего контроля ИБ банка. |
| **5.12.** При разработке моделей угроз и моделей нарушителя необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все операции в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации должны особенно тщательно контролироваться. | |
| **5.14.** Любой целенаправленной деятельности (бизнесу) свойственны риски. Это - объективная реальность и понизить эти риски можно лишь до определенного остаточного уровня. Оставшаяся (остаточная) часть риска, определяемая, в том числе, факторами среды деятельности организации БС РФ, должна быть признана приемлемой и принята, либо отклонена. В этом случае от риска следует либо уклониться (изменить среду деятельности), либо перевести на кого-нибудь (например, застраховать). Таким образом, уровень защищенности интересов (целей) организации БС РФ определяется, во–первых, величиной принятых ею остаточных рисков, а во-вторых, эффективностью работ по поддержанию принятых рисков на допустимом, низком (остаточном) уровне. | Использование продукта DeviceLock позволяет снизить риски организаций, связанные с угрозами информационной безопасности в пределах рабочих станций. Типичным примером таких угроз является утечка (нарушение конфиденциальности) информационных активов банка через съемные носители, мобильные устройства, принтеры или беспроводные сети. DeviceLock позволяет либо исключить угрозы (посредством блокировки соответствующих каналов), либо контролировать связанные с ними риски с помощью архивов теневого копирования.<br><br>Таким образом, продукт DeviceLock существенно упрощает и повышает эффективность процесса управления рисками в банковской организации в соответствии с требования Стандарта. |
| **8.4.1**. В организации БС РФ должна быть принята/корректироваться методика оценки рисков нарушения ИБ/подход к оценке рисков нарушения ИБ. | |

| | |
|---|---|
| **5.8.** Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации БС РФ – разработать политику ИБ организации БС РФ и в соответствии с ней реализовать, эксплуатировать и совершенствовать СОИБ организации БС РФ. | Использование продукта DeviceLock позволяет организациям БС РФ внедрять политики безопасности любой сложности и гибкости для контроля доступа пользователей к съемным носителям, принтерам, беспроводным сетям и мобильным устройствам. Система DeviceLock обеспечивает выполнение этих политик, а система событийного протоколирования и теневого копирования – контроль результатов их применения.<br><br>Очевидно, что комплексная политика безопасности ИТ организации БС РФ должна в любом случае базироваться на положениях парадигмы Стандарта (5.4), в соответствии с которой внутренние нарушители представляют наибольшую опасность для банка. В этой связи банк должен взять под контроль риски внутренней информационной безопасности: минимизировать угрозы утечки персональных и/или финансовых данных клиентов или злоупотребления этими сведениями со стороны внутренних нарушителей. Использование продукта DeviceLock позволяет снизить риски утечки, что дает финансовой компании достаточные основания, чтобы задокументировать этот факт в разработанной согласно Стандарту политике ИБ. |
| **7.2.4.** В организации БС РФ должны быть документально определены и выполняться процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющими получить контроль над защищаемым информационным активом организации БС РФ. | |
| **7.4.3.** В организации БС РФ должны быть документально определены и утверждены руководством, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий. | |
| **5.23.** Для поддержания системы защиты на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Менеджмент событий и инцидентов безопасности, полученных в результате мониторинга, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов. | Ключевой особенностью DeviceLock является возможность не только существенно снизить риски утечки информации ограниченного доступа со стороны авторизованных пользователей, но и сохранить точную копию данных, которые покидают ИС организации через локальные соединения рабочей станции. При помощи системы теневого копирования DeviceLock банк всегда сможет верифицировать факт утечка и выявить, какие конкретно данные были скомпрометированы.<br><br>Таким образом, DeviceLock в значительной мере способствует решению той части задачи контроля и мониторинга ИБ, которая связана с действиями пользователей в пределах рабочих станций. |
| **7.4.4.** В организации БС РФ необходимо документально определить процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Для проведения процедур мониторинга и анализа данных регистрации, действий и операций рекомендуется использовать специализированные программные и(или) технические средства. | |
| **7.6.2.** В организации БС РФ должен быть документально определен порядок подключения и использования ресурсов сети Интернет, включающий в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственных за обеспечение ИБ. | Продукт DeviceLock контролирует доступ пользователей к беспроводным сетям. Не секрет, что практически каждый современный ноутбук имеет встроенный беспроводной адаптер и, зачастую, использование этого адаптера является нарушением политики безопасности.<br><br>В частности, находясь в офисе организации, пользователь может одновременно подключиться к публичной точке беспроводного доступа и получить несанкционированный выход в сеть Интернет. Решение на базе DeviceLock позволяет исключить такой сценарий и проконтролировать доступ пользователей к беспроводным сетям. |

**Требования Стандарта Банка России по аудиту ИБ**

Следующим нормативным актом, который будет рассмотрен в настоящем документе, является Стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Аудит информационной безопасности**» (СТО БР ИББС – 1.1 – 2007). Данный Стандарт, опубликованный в 2007 году, определяет основные положения, касающиеся методологии проведения аудита, программы аудита, а также взаимоотношений между аудитором и проверяемой организацией. Структура документа СТО БР ИББС – 1.1 – 2007 приведена в таблице 4:

**Таб. 4. Структура Стандарта СТО БР ИББС – 1.1 – 2007**

| **Глава** | **Описание / краткое содержание** |
|---|---|
| Введение | Основные цели и задачи Стандарта, а также обосновывается его необходимость |
| 1. Область применения | Область применения стандарта |
| 2. Нормативные ссылки | Ссылки на нормативные документы, использованные при создании Стандарта |
| 3. Термины и определения | Список терминов и определений, которые используются в Стандарте |
| 4. Исходная концептуальная схема (парадигма) аудита информационной безопасности организаций БС РФ | Ключевые разделы Стандарта, задающие базовые концепции проведения аудита в организациях БС РФ. Все остальные разделы (6-7) конкретизируют концептуальные требования к аудиту в области управления программами аудита, взаимоотношения аудиторов и проверяемых организаций, а также конкретным этапам аудиторских проверок |
| 5. Основные принципы проведения аудита информационной безопасности организаций БС РФ. | |
| 6. Менеджмент программы аудита информационной безопасности | Требования к управлению программами аудита информационной безопасности |
| 7. Проведение аудита информационной безопасности | Требования к взаимоотношениям аудитора и проверяемой организации, а также требования к этапам проведения аудита |
| 8. Проведение самооценки информационной безопасности | Требования к процессам самооценки соответствия положениям Стандарта |

Цели и задачи аудита ИБ логично вытекают из целей и задачей «Общих положений» и формируются в первом разделе документа («Введение»). Составители указывают, что «основным из видов проверки уровня ИБ в организациях БС РФ является аудит ИБ. Мировой опыт в области обеспечения ИБ определяет аудит ИБ как важнейший процесс в непрерывном цикле процессов менеджмента ИБ организации». Кроме того, «Банк России является сторонником регулярного проведения аудита ИБ в организациях БС РФ», а сам аудит позволяет повысить уровень доверия к банкам и оценить степень соответствия Стандарту.

Область применения Стандарта СТО БР ИББС – 1.1 – 2007 («Аудит информационной безопасности») не отличается от области применения Стандарта СТО БР ИББС – 1.0 – 2008 («Общие положения»).

Перед тем, как говорить об основных концепциях Стандарта по аудиту ИБ, приведем определение свидетельств аудита, которое является основополагающим термином

документа. Согласно п. 3.12, «Свидетельства аудита ИБ – это записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита (самооценки) информационной безопасности и могут быть проверены». В дальнейшем (п. 7.2.10) это понятие конкретизируется посредством определения «источников» свидетельств и «методов получения» свидетельств. Так, источниками свидетельств могут являться:

- документы проверяемой организации и третьих лиц, относящиеся к обеспечению ИБ организации;
- устные высказывания и письменные ответы сотрудников проверяемой организации в процессе проводимых опросов;
- результаты наблюдений аудиторов за деятельностью организации в области ИБ.

А методами получения свидетельств:

- проверка и анализ документов, касающихся обеспечения ИБ организации;
- наблюдение за деятельностью организации в области ИБ;
- опрос сотрудников проверяемой организации и независимой (третьей) стороны.

Ключевые принципы сбора и анализа свидетельств аудита в организациях БС РФ приводятся в четвертой и пятой главах документа. Остановимся на них подробнее:

- (принцип реализации аудита, 4.4) **«Оценка соответствия ИБ организации БС РФ критериям аудита ИБ проводится на основе документов по обеспечению ИБ и фактов, свидетельствующих о выполнении, частичном выполнении или невыполнении установленных требований ИБ»**. Подчеркнем, что фактами, свидетельствующими о выполнении или невыполнении требований ИБ, могут являться наблюдения аудиторов о деятельности организации;
- (Оценка на основе свидетельств аудита ИБ, 5.3) **«При периодическом проведении аудита ИБ оценка на основе свидетельств аудита ИБ является единственным способом, позволяющим получить повторяемое заключение по результатам аудита ИБ, что повышает доверие к такому заключению. Для повторяемости заключения свидетельства аудита ИБ должны быть проверяемыми»**. Ключевой тезис, определяющий важнейшую роль свидетельств аудита ИБ;
- (Достоверность свидетельств аудита ИБ, 5.4). **«У аудиторов должна быть уверенность в достоверности свидетельств аудита ИБ. Доверие к документальным свидетельствам аудита ИБ повышается при подтверждении их достоверности третьей стороной или руководством организации БС РФ. Доверие к фактам, полученным при опросе сотрудников проверяемой организации, повышается при подтверждении данных фактов из различных источников. Доверие к фактам, полученным при наблюдении за деятельностью проверяемой организации в области ИБ, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов»**. Данный тезис частично дублирует принцип реализации аудита 4.3 и разделяет свидетельства аудита по уровню доверия.

В следующих главах (6-7) приводятся более конкретные требования к разработке и реализации программы аудита, а также взаимоотношениям между аудитором и проверяемой организаций. В данном документе эти требования не приводятся, поскольку они конкретизируют и дополняют положения четвертой и пятой главы. Тем не менее, некоторые этих положений будут приведены при сопоставлении функционала DeviceLock с требованиями Стандарта по аудиту ИБ.

**Возможности DeviceLock применительно к Стандарту по аудиту ИБ**

Использование DeviceLock в корпоративной среде помогает добиться соответствия ключевому требованию Стандарта по аудиту ИБ, связанному со сбором свидетельств аудита:

- Согласно положениям 4.4, 5.3 и 5.4, сбор свидетельств аудита является ключевым процессом для оценки соответствия уровня ИБ организации требованиям Стандарта. Продукт DeviceLock позволяет собирать фактические свидетельства (факты) о реализации политики ИБ в организациях БС РФ. Так, непосредственное наблюдение за рабочей станцией, которая защищена с помощью DeviceLock, является прямым свидетельством реализации политик ИБ на рабочей станции, а поддержка продуктом всестороннего событийного протоколирования и теневого копирования позволяет проводить ретроспективный анализ (расследование) и сбор доказательной базы по инцидентам ИБ, связанным с утечками информационных активов организации через съемные носители, мобильные устройства, принтеры и беспроводные сети.

В таблице далее (таб. 5) просуммирована функциональность DeviceLock в соответствии с требованиями Стандарта по аудиту ИБ:

**Таб. 5. Функциональность DeviceLock применительно к требованиям Стандарта Банка России по аудиту ИБ:**

| Требования «Аудита ИБ» | DeviceLock |
|---|---|
| **4.4.** Оценка соответствия ИБ организации БС РФ критериям аудита ИБ проводится на основе документов по обеспечению ИБ и фактов, свидетельствующих о выполнении, частичном выполнении или невыполнении установленных требований ИБ. | Использование ограничительных политик DeviceLock является фактом, свидетельствующим о выполнении установленных требований ИБ в области контроля действий пользователей в пределах рабочих станций.<br><br>Доверие к данному свидетельству аудита может быть повышено в том случае, если сотрудники аудиторской организации будут наблюдать за деятельностью проверяемой организации непосредственно при функционировании проверяемых процедур или процессов.<br><br>Кроме того, функциональность DeviceLock в части событийного протоколирования и теневого копирования позволяет проверяемой организации предоставить юридически значимые свидетельства для проведения аудита. Тем самым, процесс аудита становится значительно проще и понятнее, как для аудиторской компании, так и для проверяемой организации. |
| **5.3.** При периодическом проведении аудита ИБ оценка на основе свидетельств аудита ИБ является единственным способом, позволяющим получить повторяемое заключение по результатам аудита ИБ, что повышает доверие к такому заключению. Для повторяемости заключения свидетельства аудита ИБ должны быть проверяемыми. | |
| **5.4**. У аудиторов должна быть уверенность в достоверности свидетельств аудита ИБ. […] Доверие к фактам, полученным при опросе сотрудников проверяемой организации, повышается при подтверждении данных фактов из различных источников. Доверие к фактам, полученным при наблюдении за деятельностью проверяемой организации в области ИБ, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов. | |
| **7.2.8.** Проведение аудита ИБ на месте должно включать следующие работы: […]<br><br>— сбор дополнительных свидетельств аудита ИБ;<br><br>— оценка свидетельств аудита ИБ. […] | |
| **7.2.10.** Основными источниками свидетельств аудита ИБ должны являться: […]<br><br>— результаты наблюдений аудиторов за деятельностью организации в области ИБ. | |

| | |
|---|---|
| Основными методами получения свидетельств аудита ИБ должны являться: […]<br><br>— наблюдение за деятельностью организации в области ИБ; […] | |

**Методика оценки соответствия Стандарту**

Документ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. **Методика оценка соответствия** […]» (СТО БР ИББС - 1.2 – 2007) является опросником, который позволяет провести численную оценку соответствия Стандарту «Общие положения». Заполнив данный документ, аудиторская организация получает совокупность метрик, характеризующих уровень зрелости системы ИБ банковской организации.

В общей сложности «Методика оценка соответствия» содержит несколько сотен частных показателей (единичных вопросов анкеты), которые сгруппированы в 32 групповых показателя. Аудиторская организация выставляет оценку для каждого частного показателя, на базе которых формируются 32 оценки групповых показателей. На базе полученных оценок групповых показателей подсчитывается семь групповых метрик, а также три финальных оценки соответствия – в области системы ИБ, системы управления ИБ и осознания ИБ. Минимальная из этих оценок является результатом аудита и показывает общий уровень соответствия процессов обеспечения ИБ требованиям Банка России и определяет уровень соответствия проверяемой организации.

Подробная схема подсчета всех показателей в соответствие с «Методикой оценки соответствия» приведена в приложении 2 к данному документу.

**Возможности DeviceLock применительно к оценке соответствия**

Прежде, чем говорить о соответствии продукта DeviceLock частным показателям «Методики оценки соответствия», отметим тот факт, что большинство этих показателей предполагают внедрение не только технических, но и административных мер защиты. Другими словами, внедрение любой технической системы не сможет обеспечить соответствие даже части требований Стандарта без реализации сопутствующих административных мер.

В таблице далее (таб. 6) просуммирована функциональность DeviceLock в соответствии с частными показателями «Методики оценки соответствия».

**Таб. 6. Функциональность DeviceLock применительно к частным показателям «Методики оценки соответствия»**

| Частные показатели «Методики оценки соответствия» | DeviceLock |
|---|---|
| **М3.5.** Выполняется ли контроль доступа пользователей к ресурсам всех ЭВМ и/или ЛВС, задействованных в технологических процессах? | Продукт DeviceLock является унифицированным инструментом, который позволяет централизованно контролировать доступ пользователей к съемным носителям, беспроводным сетям, принтерам и мобильным устройствам. |

| | |
|---|---|
| **M5.7.** Контролируется ли подразделениями (лицами) в организации, ответственными за обеспечение ИБ, подключение и использование ресурсов сети Интернет? | DeviceLock контролирует доступ пользователей к беспроводным сетям. Не секрет, что каждый современный ноутбук имеет встроенный беспроводной адаптер, и зачастую, использование этого адаптера является нарушением политики безопасности.<br><br>В частности, находясь в офисной сети организации, пользователь одновременно может подключиться к публичной точке беспроводного доступа и получить несанкционированный выход в сеть Интернет. Система DeviceLock позволяет исключить такой сценарий и проконтролировать доступ пользователей к беспроводным сетям. |
| **M5.8.** Санкционируется ли руководством функционального подразделения организации любое подключение и использование сети Интернет? | |
| **M19.6.** Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля использования ресурсов сети Интернет? | |
| **M10.1.** Осуществляется ли в организации оценка рисков ИБ, в том числе связанных с неисполнением требований нормативных актов Банка России, имеющих отношение к ИБ, а также связанных с угрозами нарушения процессов управления ИБ? | Использование продукта DeviceLock позволяет управлять рисками, связанными с угрозами ИБ в пределах рабочих станций. Типичным примером таких угроз является утечка (нарушение конфиденциальности) информационных активов банка через съемные носители, мобильные устройства, принтеры или беспроводные сети. DeviceLock позволяет либо отразить такие угрозы (посредством блокировки соответствующих каналов), либо проконтролировать данные риски с помощью базы данных событийного протоколирования и архивов теневого копирования.<br><br>Таким образом, продукт DeviceLock существенно упрощает и повышает эффективность процесса управления рисками ИБ в банковской организации в соответствии с требования Стандарта. |
| **M10.5.** Выполнена ли идентификация информационных активов и их уязвимостей? | |
| **M10.6.** Выполнена ли оценка потенциального ущерба бизнесу организации в случае реализации угроз ИБ? | |
| **M10.7.** Анализируется ли и учитывается ли при оценке рисков ИБ степень актуальности угроз? | |
| **M10.9.** Анализируется ли и учитывается ли при оценке рисков ИБ степень актуальности уязвимостей информационных активов? | |
| **M10.12.** Учитываются ли данные об инцидентах ИБ при оценке рисков ИБ? | |
| **M3.7.** Регистрируются ли действия сотрудников и пользователей, влияющие на ИБ, в специальном электронном журнале либо регистрация обеспечивается организационными и/или административными мерами? | 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. При помощи системы теневого копирования DeviceLock банк всегда сможет верифицировать факт утечки и определить какие конкретно данные были компрометированы.<br><br>Таким образом, DeviceLock в значительной мере способствует решению той части задачи контроля и мониторинга ИБ, которая связана с действиями пользователей в пределах рабочих станций. |
| **M3.8.** Предоставлен ли доступ к электронному журналу регистрации действий пользователей и сотрудников только администратору ИБ и отсутствует ли возможность редактирования записей данного электронного журнала? | |
| **M19.2.** Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля изменений и использования прав доступа пользователей? | |
| **M19.3.** Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля средств и подсистем управления доступом и регистрации? | |

| | |
|---|---|
| **M19.4.** Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля использования оборудования и выявления нештатных (или злоумышленных) действий в организации, а также выявления потенциальных нарушений ИБ? | |
| **M20.2.** Используются ли при анализе эффективности СМИБ результаты мониторинга ИБ и сведения относительно инцидентов ИБ? | |
| **M21.3.** Используются ли при проведении внутреннего аудита ИБ данные мониторинга ИБ (в том числе журналы регистрации инцидентов ИБ)? | |
| **M11.2.** Существуют ли утвержденные руководством организации документы, определяющие частные политики ИБ? | Использование продукта DeviceLock позволяет организациям БС РФ внедрять политики безопасности любой сложности для контроля доступа пользователей к съемным носителям, принтерам, беспроводным сетям и мобильным устройствам. Система контроля доступа DeviceLock обеспечивает выполнение этих политик, а система событийного протоколирования и теневого копирования – контроль результатов их применения.<br><br>Очевидно, что комплексная политика ИТ-безопасности должна в любом случае базироваться на положениях парадигмы Стандарта (5.4), в соответствии с которой внутренние нарушители представляют наибольшую опасность для банка. В соответствии с этим банк должен взять под контроль риски внутренней ИБ: минимизировать угрозу утечки персональных и/или финансовых данных клиентов или злоупотребления этими сведениями со стороны внутренних нарушителей. Использование DeviceLock позволяет управлять рисками утечки, что дает финансовой компании достаточные основания, чтобы задокументировать этот факт в разработанной в соответствии со Стандартом политике ИБ. |
| **M11.6.** Учитываются ли в положениях политики ИБ организации результаты оценки рисков ИБ? | |
| **M28.2.** Определены ли в организации модель угроз и модель нарушителя, обеспечивающие прогнозирование развития возможных проблем, связанных с ИБ? | Составление модели угроз и нарушителей является комплексной задачей, которая пронизывает все бизнес-процессы организации. Зачастую, для решения этой задачи компании не хватает собственной компетенции, и ей приходится нанимать специализированных консультантов.<br><br>Использование продукта DeviceLock позволяет обеспечить комплексный контроль действий пользователей в пределах рабочих станций, что, в свою очередь существенно упрощает построение модели угроз и нарушителей. Например, если политика безопасности компании запрещает копирование информации на съемные устройства, то использование DeviceLock в значительной степени исключает угрозу утечки через данный канал из общей модели угроз. |

**Выводы**

Проведенный анализ показывает, что продукт DeviceLock производства компании Смарт Лайн Инк помогает организациям БС РФ существенно упростить процесс достижения соответствия отраслевым Стандартам СТО БР ИББС. Внедрение DeviceLock влияет на соответствие целому ряду требований, описанных в рассмотренных выше Стандартах Банка России.

Прежде всего, DeviceLock позволяет финансовой организации **управлять рисками ИБ** в пределах рабочей станции. Благодаря использованию DeviceLock существенно упрощается модель угроз, а значит – упрощается и процесс управления рисками, который является основополагающим критерием для соответствия «Общим положениям». Кроме того, DeviceLock обеспечивает реализацию политик безопасности и контроль доступа пользователей к съемным носителям, беспроводным сетям, принтерам и мобильным устройствам.

Не менее важным фактором является уникальная функциональность всестороннего событийного протоколирования и теневого копирования, реализованная в продукте DeviceLock. Эта функциональность, позволяющая проводить ретроспективный анализ событий ИБ, отвечает еще одной важнейшей группе требований – в области **совершенствования системы управления ИБ**.

Согласно ключевой парадигме Стандартов, наибольшие угрозы ИБ исходят от собственных сотрудников компаний. Система DeviceLock ориентирована на борьбу именно **с внутренними нарушителями** и потому является приоритетным инструментом обеспечения информационной безопасности для организации, желающей успешно реализовать требования и пройти аудит соответствия Стандартам Банка России.

**Приложение 1. Основные изменения СТО БР ИББС – 1.0 – 2008**

В последней редакции Стандарта СТО БР ИББС – 1.0 – 2008 «Общие положения» был внесен ряд существенных изменений по сравнению с предыдущей версией СТО БР ИББС – 1.0 – 2006. Поскольку привести все изменения (в том числе и изменения формулировок) в рамках данного документа невозможно, то будут рассмотрены только наиболее значительные из них:

- В последней редакции Стандарта практически полностью исчез раздел «Нормативные ссылки», в котором остались только ссылка на Стандарт «ГОСТ Р ИСО 9001–2001 Система менеджмента качества. Требования». В предыдущей версии раздел содержал более 20 ссылок;

- В последней редакции Стандарта существенно расширен раздел «Термины и определения». Теперь в нем содержится 68 определений – ровно в 4 раза больше, чем в версии 2006 года;

- Раздел «Исходная концептуальная схема (парадигма) […]» был существенно переработан. В частности, в нем появились более детальные требования по управлению рисками ИБ;

- Раздел «Основные принципы обеспечения информационной безопасности», который присутствовал в СТО БР ИББС – 1.0 – 2006, был упразднен;

- Термин «политика ИБ» был заменен на «система ИБ» (соответственно, был изменен и релевантный раздел требований). Вместе с тем, содержание требований к системе ИБ практически не изменилось;

- Однако самое значительное изменение связано с резким расширением требований к системе управления ИБ. Раздел Стандарта, соответствующий этим требованиям, был кардинально (практически в 6 раз) расширен. Добавим, что новые требования, которые появились в последней редакции Стандарта, не противоречат положениям предыдущей версии, а конкретизируют их.

**Приложение 2. Методика расчета оценки соответствия**

В общей сложности «Методика оценка соответствия» содержит несколько сотен частных показателей (единичных вопросов анкеты), которые сгруппированы в 32 групповых показателя. Аудиторская организация выставляет оценку для каждого частного показателя, на базе которых формируются 32 оценки групповых показателей. Каждый частный показатель имеет определенный вес, причем сумма весов частных показателей в рамках одного и того же группового показателя всегда равна единице. Таким образом, справедлива формула (1):

$$\sum_j \alpha_{i,j} = 1$$

(1) , где $i = 1,2, \ldots ,32$ – номер группового показателя, а $\alpha_{i,j}$ – вес $j$-го частного показателя в $i$-ом групповом показателе.

Легко понять, что значение $i$-ого группового показателя определяется по формуле (2):

$$EV_i = \sum_j \alpha_{i,j} * EV_{i,j}$$

(2) , где $i = 1,2, \ldots ,32$ – номер группового показателя, $\alpha_{i,j}$ – вес $j$-го частного показателя в $i$-ом групповом показателе, а $EV_{i,j}$ – оценка частного показателя, которая определяется аудиторами. Полный список групповых показателей приводится в таблице 7.

**Таб. 7. Перечень групповых показателей для оценки соответствия Стандарту**

| Идентификатор | Описание |
|---|---|
| $EV_1$ | Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу |
| $EV_2$ | Обеспечение ИБ автоматизированных банковских систем на стадиях жизненного цикла |
| $EV_3$ | Обеспечение ИБ при управлении доступом и регистрации |
| $EV_4$ | Обеспечение ИБ средствами антивирусной защиты |
| $EV_5$ | Обеспечение ИБ при использовании ресурсов сети Интернет |
| $EV_6$ | Обеспечение ИБ при использовании средств криптографической защиты информации |
| $EV_7$ | Выполнение правил обеспечения ИБ банковских платежных технологических процессов |
| $EV_8$ | Выполнение правил обеспечения ИБ банковских информационных тех. процессов |
| $EV_9$ | Определение/уточнение области действия СМИБ и выбор подхода к оценке рисков ИБ |
| $EV_{10}$ | Анализ и оценка рисков ИБ, варианты обработки рисков ИБ |
| $EV_{11}$ | Определение/уточнение политики ИБ организации БС РФ |
| $EV_{12}$ | Выбор/уточнение целей ИБ и защитных мер |

| | |
|---|---|
| $EV_{13}$ | Принятие руководством организации БС РФ остаточных рисков и решения о реализации и эксплуатации/совершенствовании СМИБ |
| $EV_{14}$ | Разработка плана обработки рисков ИБ |
| $EV_{15}$ | Реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СМИБ |
| $EV_{16}$ | Реализация программ по обучению и осведомлению ИБ |
| $EV_{17}$ | Обнаружение и реагирование на инциденты безопасности |
| $EV_{18}$ | Обеспечение непрерывности бизнеса и восстановления после прерываний |
| $EV_{19}$ | Мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ |
| $EV_{20}$ | Анализ эффективности СМИБ, анализ уровней остаточного и приемлемого рисков ИБ |
| $EV_{21}$ | Внутренний аудит СМИБ |
| $EV_{22}$ | Анализ СМИБ со стороны высшего руководства |
| $EV_{23}$ | Внешний аудит СМИБ |
| $EV_{24}$ | Реализация тактических улучшений в СМИБ |
| $EV_{25}$ | Реализация стратегических улучшений СМИБ. Использование опыта |
| $EV_{26}$ | Информирование об изменениях и их согласование с заинтересованными сторонами |
| $EV_{27}$ | Оценка достижения поставленных целей |
| $EV_{28}$ | Своевременность обнаружения проблем, прогноз развития проблем ИБ и оценка их влияния на бизнес-цели |
| $EV_{29}$ | Определенность целей, адекватность выбора защитных мер, их эффективность и контролируемость |
| $EV_{30}$ | Непрерывность обеспечения ИБ и использование опыта при принятии и реализации решений |
| $EV_{31}$ | Знание своих клиентов и служащих, персонификация и адекватное разделение ролей и ответственности, адекватность ролей функциям и процедурам |
| $EV_{32}$ | Доступность услуг и сервисов, наблюдаемость и оцениваемость обеспечения ИБ |

Согласно п.6.3 «Методики оценки соответствия», частные показатели должны оцениваться на базе следующих критериев (таблица 8) и свидетельств аудита (определение свидетельств аудита было дано в предыдущем Стандарте):

**Таб. 8. Критерии оценки частных показателей**

| Оценка | Степень документального подтверждения требований частного показателя | Степень реального выполнения требований частного показателя |
|---|---|---|
| 0 | Не подтверждены | Не выполняются |
| 0 | Подтверждены частично | Не выполняются |
| 0,25 | Подтверждены полностью | Не выполняются |
| 0,25 | Не подтверждены | Выполняются в неполном объеме |
| 0,25 | Подтверждены частично | Выполняются в неполном объеме |
| 0,5 | Подтверждены полностью | Выполняются в неполном объеме |
| 0,5 | Не подтверждены | Выполняются в полном объеме |
| 0,75 | Подтверждены частично | Выполняются в полном объеме |
| 1 | Подтверждены полностью | Выполняются в полном объеме |

Таким образом, значение оценки каждого частного показателя EVi, j может принимать значения в интервале *[0,1]*. В совокупности с формулами (1) и (2) это означает, что

значение каждого группового показателя $EV_1$, $EV_2$, …, $EV_{32}$ также лежит в интервале *[0,1]*, причем значение 0 соответствует невыполнению требований частных показателей, а значение 1 – полному соответствию всем требованиям.

Оценив каждый из групповых показателей, аудиторы оценивают 7 основных метрик, показывающих уровень информационной безопасности в организации БС РФ. Каждая групповая метрика определяется по формуле (3):

(3) $$EV = AVG\,(EV_i)$$, где *AVG()* – функция среднего значения, а индексы *i* принадлежат некой группе групповых показателей.

Согласно положениям документа, при оценке соответствия Стандарту, должны быть подсчитаны следующие групповые метрики (таб. 9):

**Таб. 9. Групповые метрики оценки соответствия Стандарту**

| Оценка | Описание метрики | Номера групповых показателей |
|---|---|---|
| $EV_{БПТП}$ | Безопасность платежных технологических процессов | i = 1,2, … , 6, 7 |
| $EV_{БИТП}$ | Безопасность информационных технологических процессов | i = 1,2, … , 6, 8 |
| $EV_{ПЛ}$ | Уровень процессов планирования СМИБ | i = 9, 10, … , 13 |
| $EV_{Р}$ | Уровень процессов реализации и эксплуатации СМИБ | i = 14, 15, … , 18 |
| $EV_{ПР}$ | Уровень процессов проверки СМИБ | i = 19, 20, … , 23 |
| $EV_{С}$ | Уровень процессов совершенствования СМИБ | i = 24, 25, … , 27 |
| $EV_{ОИБ}$ | Уровень осознания информационной безопасности | i = 28, 29, … , 32 |

Наконец, на финальном этапе численного аудита подсчитываются окончательные оценки соответствия Стандарту. В общей сложности, Стандарт предусматривает четыре таких оценки, которые приведены в таблице 10:

**Таб. 10. Финальные оценки соответствия Стандарту**

| Оценка | Описание метрики | Формула |
|---|---|---|
| EV1 | Уровень информационной безопасности | $EV1 = Min\,(EV_{БПТП}, EV_{БИТП})$ |
| EV2 | Уровень процессов СМИБ | $EV2 = Min\,(EV_{ПЛ}, EV_{Р}, EV_{ПР}, EV_{С})$ |
| EV3 | Уровень осознания информационной безопасности | $EV3 = EV_{ОИБ}$ |
| R | Общая оценка соответствия Стандарту | $R = Min\,(EV1, EV2, EV3)$ |

В зависимости от значений полученных оценок, проверяемой организации присваивается один из шести уровней (от нулевого до пятого) по каждому из направлений EV1, EV2, EV3, R. Критерий присвоения уровней приводятся в таблице 11:

**Таб. 11. Соответствие оценок и уровней**

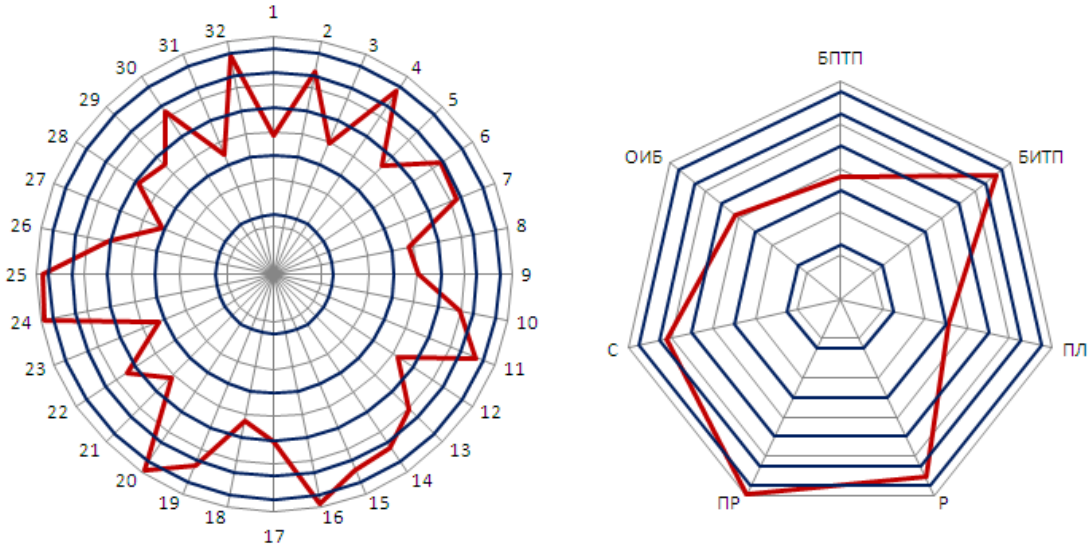
| Уровень | Оценка |
|---|---|
| 0 | Менее 0,25 |

| | |
|---|---|
| 1 | От 0,25 до 0,5 |
| 2 | От 0,5 до 0,7 |
| 3 | От 0,7 до 0,85 |
| 4 | От 0,85 до 0,95 |
| 5 | Более 0,95 |

Согласно п. 10.4 «Методики оценки соответствия», значения общей оценки R четвертого и пятого уровней «являются рекомендованными Банком России, а значения от нулевого до третьего уровня – «не являются рекомендованными». Другими словами, чтобы заявить о соответствии Стандарту, финальная оценка соответствия (а значит – и каждая из групповых метрик на таб. 7) должна превышать значение 0,85.

Добавим, что Банк России рекомендует изображать полученные оценки групповых показателей, групповых метрик и финальных оценок на круговых диаграммах. Примеры таких диаграмм приведены на рис. 3.

**Рис. 3. Примеры диаграмм оценки соответствия Стандарту[1].**




## 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 58 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 4 000 000 компьютерах. В число клиентов компании входят Центральный Банк РФ, Сбербанк России, ОАО "Силовые 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.

[1] Красная линия – оценка проверяемой организации, синие линии – критерии принадлежности к уровням соответствия.

**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