



Код безопасности
ГК «Информзащита»

Выполнение требований СТО БР ИББС-1.0-2010 с помощью решений компании «Код Безопасности»

Максим Илюхин, заместитель генерального директора ООО «Код Безопасности»

Выполнение требований СТО БР ИББС-1.0-2010 с помощью решений компании «Код Безопасности»

152-ФЗ можно назвать «событием 2009 года» в сфере ИБ России. Весьма вероятно, что именно Федеральный закон «О персональных данных» вызвал рост сектора информационной безопасности на фоне кризиса остальных отраслей в 2009 году. Однако рост сектора ИБ был вызван не объективными причинами, такими как осознание проблем информационной безопасности менеджментом компаний и широкое внедрение безопасных интернет-технологий и защищенных корпоративных сетей, а беспрецедентно жесткими обязательными к исполнению требованиями регуляторов (федеральных служб, призванных контролировать исполнение 152-ФЗ: ФСТЭК, ФСБ, Роскомнадзор).

Ряд требований руководящих документов выполнить было практически невозможно. Например, получить лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации полагалось всем медицинским учреждениям, банкам, операторам связи, предприятиям ЖКХ и другим операторам персональных данных, но справиться с подобным наплывом «желающих» ФСТЭК была просто не в состоянии (за весь 2009 год ФСТЭК выдала всего 217 подобных лицензий).

Чтобы учесть интересы различных категорий операторов персональных данных, были разработаны отраслевые рекомендации по выполнению требований 152-ФЗ и руководящих документов регуляторов.

Комплекс стандартов Банка России состоит из:

- Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) включает в себя в данный момент четыре документа:

- СТО БР ИББС-1.0–2010 (4 редакция) «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;

- СТО БР ИББС-1.2–2010 (3 редакция) «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС»;

- РС БР ИББС-2.4–2010. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая част-

ная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации»;

1. РС БР ИББС-2.3–2010. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации»;

А также:

- Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ, разработанные совместно Банком России, АРБ и Ассоциацией региональных банков России (Ассоциацией «Россия»).

Обзор требований СТО БР ИББС, аудит выполнения стандарта

Письмо шестерых

Ввести альтернативу требованиям ФСТЭК и ФСБ в области защиты персональных данных призвано решение председателя ЦБ РФ от 28.06.2010 (письмо «шестерых»: ЦФ РФ, АРБ, Ассоциация региональных банков России, ФСБ, ФСТЭК, Роскомнадзор). Решение председателя ЦБ РФ закрепляет за организациями банковской системы право выбора между исполнением требований ФСБ, ФСТЭК и требований СТО БР ИББС. До 31 декабря 2010 года организация БС, принявшая добровольное решение о внедрении комплекса СТО БР ИББС, должна провести комплекс мероприятий по внедрению стандарта:

- сообщить о принятом решении в ЦБ РФ;
- выполнить весь комплекс мероприятий по приведению в соответствие требованиям стандарта СТО БР ИББС-1.0;
- применять методические рекомендации по выполнению законодательных требований при обработке персональных данных;
- провести оценку соответствия организации БС РФ требованиям Стандарта Банка России СТО БР ИББС-1.0 силами организации-аудитора. В случае невозможности проведения оценки соответствия силами сторонней организации – провести оценку самостоятельно;
- выпустить документ, подтверждающий соответствие требованиям стандарта в целом и по направлениям регуляторов – ФСТЭК, ФСБ и Роскомнадзора;

- не позднее 31 декабря 2010 года направить этот документ в адрес Банка России и территориальных органов регуляторов;
- в дальнейшем направлять этот документ в Банк России и регуляторам один раз в три года.

Это отнюдь не облегчает банкам работу по приведению в соответствие бизнес-процессов требованиям 152-ФЗ и РД регуляторов, а скорее наоборот: СТО БР ИББС разработан с учетом требований более жесткого «четверокнижия» (руководящих документов ФСТЭК, утвержденных Заместителем директора ФСТЭК России 15 февраля 2008 г.), часть требований которого была пересмотрена в сторону послабления, а часть и вовсе отменена в февральском Приказе ФСТЭК №58 .

В силу тесной взаимосвязи организаций банковской системы РФ между собой негативные последствия реализации угроз, направленных на активы даже отдельной организации, могут привести к негативным последствиям банковской сферы РФ. И именно поэтому обеспечение безопасности информации как актива является для организаций БС РФ одним из основополагающих аспектов их деятельности.

Для установления единых требований и повышения эффективности мероприятий по обеспечению информационной безопасности организаций банковской системы РФ был разработан комплекс стандартов Банка России (СТО БР ИББС-1.0-2010 и другие). Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» является базовым для развивающей и обеспечивающей его группы документов, составляющих комплекс стандартов Банка России.

Положения Стандарта Банка России СТО БР ИББС-1.0-2010 определяют ряд общих требований к обеспечению информационной безопасности, которые включают в себя:

- концептуальную схему обеспечения информационной безопасности;
- модели угроз и нарушителей информационной безопасности;
- организационные и технические аспекты создания системы информационной безопасности;
- вопросы менеджмента информационной безопасности;
- порядок проверки и оценки информационной безопасности.

Остановимся подробнее на требованиях, включа-

ющих обеспечение информационной безопасности техническими средствами. При построении комплексной системы информационной безопасности перед организацией банковской системы РФ стоят задачи выбора средств защиты информации, отвечающих следующим критериям:

- соответствие требованиям Стандарта Банка России СТО БР ИББС-1.0-2010;
- качество применяемых технических решений;
- совместимость решений, обеспечивающих различные аспекты информационной безопасности;
- масштабируемость решений;
- возможность получения квалифицированной технической поддержки в процессе эксплуатации.

Какие риски существуют для компаний БС при принятии решения об использовании тех или иных средств защиты в ИС, обрабатывающих ПДн?

Выбор сертифицированного решения

При построении системы защиты информации перед каждым руководителем рано или поздно возникает вопрос: использовать ли сертифицированные ФСТЭК (ФСБ) средства российских разработчиков или использовать продукты не прошедшие процедуры сертификации? В стандарте Банка России п. 7.4.2 говорится о том, что рекомендовано использовать сертифицированные средства, а так же в п.9.4 написано, что для проведения работ по контролю и надзору привлекаются ФСТЭК и ФСБ в части их касающейся. Таким образом, делая выбор в пользу сертифицированных продуктов российских производителей, руководители минимизируют риски, связанные с доверием к средствам защиты в части заложенных на этапе разработки этих средств недеklarированных возможностей, наличие которых может привести к серьезному ущербу для всей информационной структуры как отдельной организации, так и для банковской сферы. При выборе сертифицированных средств защиты минимизируются риски, связанные с прохождением аттестаций информационных систем и прохождением контрольных проверок.

Одним из основных постулатов при построении системы информационной безопасности в соответствии с СТО БР ИББС является использование сертифицированных ФСТЭК (ФСБ) средств защиты информации (в том числе криптографии).

Большинство зарубежных производителей при проведении процедуры сертификации своих продуктов забывают указывать в своих рекламных материалах информацию о том, что сертифицированы лишь

отдельные образцы программных и аппаратных решений или их небольшие партии. В таких случаях сертификат придется продлевать через три года самостоятельно. Поэтому компаниям, принимающим решение о выборе средств защиты информации при ее обработке в ИС, необходимо обращать внимание на те программные и аппаратные продукты, которые сертифицированы наиболее правильным и надежным способом. Это позволит избежать рисков, связанных с повторным выделением бюджетов на переаттестацию системы обработки персональных данных. Также необходимо уделять особое внимание сертификации на отсутствие недекларированных возможностей (НДВ) (РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»). Для сертификации по уровню НДВ необходимо предоставить исходные коды программного обеспечения. Далеко не все производители готовы предоставлять исходные коды сертифицирующим органам, аргументируя это разными доводами, но отказ от предоставления исходных кодов контролирующим органам позволяет усомниться в отсутствии программных закладок ПДн.

Решения компании «Код Безопасности» для выполнения требований защиты персональных данных в банковском секторе.

Компания «Код Безопасности» – российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, коммерческой и государственной тайны. «Код Безопасности» стремится предоставить компаниям качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая специализируется в области обеспечения безопасности информационных систем и более 15 лет является лидером российского рынка информационной безопасности. ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России. Высокое качество продуктов компании

Выбор мультивендорного или моновендорного подхода

Очевидно, что наиболее приемлемым для организаций БС будет решение об использовании средств защиты тех вендоров, которые зарекомендовали себя на рынке информационной безопасности успешной реализацией крупных проектов.

Использование внешних средств защиты информации, помимо встроенных в инфраструктурные платформы средств защиты

Зачастую компании считают наиболее экономичным решением использование внутренних, встроенных в инфраструктурные платформы средств защиты, что не является оптимальным решением. При таком подходе каждое обновление платформы требует дополнительной переаттестации, до завершения которой система не считается выполняющей требования законодательства. Тогда как использование внешнего ПО или оборудования не влечет таких дополнительных затрат и процедур.

подтверждают сертификаты на средства защиты информации, выданные ФСТЭК, Министерством обороны и ФСБ России. Более 2500 государственных и коммерческих организаций в России и странах СНГ доверили продуктам «Кода Безопасности» обеспечение информационной безопасности своих автоматизированных систем. Компания «Код Безопасности» стремится соответствовать высоким стандартам качества и инноваций при разработке новых программных средств защиты и является технологическим партнером ряда ведущих международных компаний – лидеров мирового рынка программного обеспечения и оборудования, таких как Microsoft, VMware, Citrix, IBM, Oracle, Cisco.

Для выполнения каких задач, изложенных в СТО БР ИББС-1.0-2010, могут применяться продукты компании «Код Безопасности»?

1. Все продукты компании «Код Безопасности» создаются и развиваются в соответствии с законодательствами, нормативно-правовыми актами и требованиями регулирующих органов, действующих на рынке информационной безопасности, тем самым выполняется требование: «...В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицирован-

ные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД и средства криптографической защиты информации». Стоит заметить что, вся линейка продуктов сертифицируется во ФСТЭК РФ и ФСБ РФ.

2. Такие известные на российском рынке СЗИ от НСД «SecretNet» Secret Net и электронный замок ПАК «Соболь» разработки ООО «Код Безопасности» могут применяться для процедур идентификации, аутентификации, авторизации, управления доступом, контроля целостности, регистрации событий и действий. Тем самым в ИС банков минимизируются риски, связанные с защитой информации от НСД и утечек информации по техническим каналам.

3. Одним из острых вопросов в банковской сфере является использование удаленных терминалов (банкоматов), которые находятся в общественных местах и работают по общедоступным каналам связи. При этом не контролируется доступ к самому устройству и, как показывает мировая практика, злоумышленники активно этим пользуются. Для минимизации рисков подмены информации в канале между удаленными устройствами «... «...должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии». А также при работе удаленных терминалов должны обеспечиваться защитные меры, направленные на предотвращение возможности подмены авторизованного клиента злоумышленником в рамках сеанса работы. Также при обрыве или потере сеанса необходимо обеспечивать повторное выполнение процедур идентификации. Все эти и другие возможности

функции выполняет аппаратно-программный комплекс шифрования «Континент», предназначенный для защиты информации, передаваемой по открытым каналам связи, разработки ООО «Код безопасности».

4. Все большее распространение получают технологии виртуализации, и БС не остается в стороне от этого «мэйнстрима», царящего в ИТ.

В то же время ни методические рекомендации, ни материалы регуляторов по обеспечению безопасности персональных данных не учитывают различий между физической и виртуальной средой обработки информации. Вместе с тем обработка информации и ее защита в виртуальной среде имеют свои специфические особенности. Для защиты информации и приведения систем обработки информации в соответствие законодательства в виртуальных средах используется программное решение vGate разработки компании «Код Безопасности».

vGate – это средство защиты информации, предназначенное для обеспечения безопасности виртуальной инфраструктуры на базе систем VMware Infrastructure 3 и VMware vSphere 4. Применение vGate дает возможность легитимного использования в виртуальных средах информационных систем, обрабатывающих персональные данные, и помогает провести аттестацию ИС.

Учитывая вышесказанное, программные и аппаратные решения компании «Код Безопасности» могут быть использованы в системах защиты конфиденциальной информации организаций БС для обеспечения защиты информации и для выполнения требований СТО БР ИББС.



Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества Info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.