А. К. Плешков
Московский инженерно-физический институт (государственный университет)

ПРИНЦИПЫ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ К ИТ-РЕШЕНИЯМ В КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ РФ

Представлен один из подходов к формированию типовых требований по обеспечению защиты информации в автоматизированных системах, которые планируется дорабатывать и/или внедрять в кредитно-финансовых организациях. Указаны основные направления развития требований по ИБ, в соответствии с положениями стандарта Банка России СТО БР ИББС-1.0-2006, которые могут лечь в основу внутренних нормативных документов в типовом финансовом институте.

Введение

В настоящее время на рынке программно-аппаратных решений, реализующих новый для кредитной организации функциональный финансовый продукт, представлено много похожих на первый взгляд законченных продуктов промышленного уровня, качество которых, как правило, подтверждено большим количеством сертификатов, в том числе по информационной безопасности. Типичные организации-интеграторы, предлагающие к внедрению продукты известных мировых производителей, пытаются любыми средствами убедить представителей заинтересованных организаций выбрать именно их решение, поскольку оно, по словам менеджеров по продажам, существенно повысит общий уровень защищенности в организации. К сожалению, технически несостоятельные аргументы, а порой придуманные на ходу ответы «неспециалистов» не всегда отражают реальное положение вещей.

Известно, что крупные кредитно-финансовые организации в России являются желанным клиентом для ИТ-интегратора любого уровня и направления, конкуренция на рынке ИТ-безопасности яркое тому подтверждение. Обладая знанием о том, что в настоящее время требуется крупному и платежеспособному финансовому институту, менеджеры по продажам ИТ-интегратора пойдут на многое, чтобы стать «единственным подходящим» среди дюжины таких же. Ситуация усугубляется многократно с точки зрения технического эксперта, когда вопрос о выборе конкретного технически завершенного решения и/или интегратора поднимается на уровень руководства кредитно-финансовой организации. В этом случае качество и технические особенности предлагаемого к внедрению программно-аппаратного комплекса зачастую не рассматриваются как основной критерий для выбора.

Многие организации для уменьшения субъективности в таких ситуациях стараются проводить открытые тендеры, правила и условия которых заранее известны, опубликованы и зависят от специфики работы организации и типа выбираемого решения. В рамках тендера выбирается поставщик программно-аппаратного решения, тогда как решение вопроса о выборе подходящего по техническим параметрам комплекса ложится на плечи техническим специалистам заказчика [1].

Каким образом среди десятков на первый взгляд одинаковых продуктов суметь выбрать единственное техническое решение, которое будет полностью удовлетворять по всем позициям, в том числе по функциональности и уровню обеспечения информационной безопасности, технических экспертов и представителей всех задействованных при выборе подразделений и направлений, в том числе бизнес-блок? Ответ на этот вопрос становится тем сложнее найти, чем с большей скоростью появляются новые банковские продукты, потребность в наличии которых диктуется быстро развивающимися российским и мировым финансовыми рынками.

В рамках данной статьи рассматривается поставленный выше вопрос в части выбора продукта, удовлетворяющего требованиям по информационной безопасности, предъявляемым к программно-аппаратным решениям, призванным реализовать и обеспечить новую для кредитно-финансовой организации функциональность.

В соответствии с положением п.8. стандарта Банка России [2] все программно-аппаратные комплексы, реализующие информационные системы в кредитно-финансовых организациях, должны обладать подсистемой обеспечения информационной безопасности, требования к составу и характеристикам которой формируются подразделениями, ответственными за обеспечения информационной безопасности в организации. Это обстоятельство помогает экспертами по информационной безопасности в организации как минимум принимать участие в выборе решений, а иногда оказывать влияние на окончательный выбор и аргументировано отставить позиции, закрепленные в «Политике информационной безопасности организации» [1, 3].

С точки зрения экспертов по информационной безопасности, алгоритмическая и программная реализация функциональных компонентов любого информационного решения является менее интересной и значимой по сравнению с реализацией компонентов, ответственных за обеспечение информационной безопасности информационной системы. В каждом конкретном случае особенности и количество компонентов по ИБ зависят от типа предлагаемого функционального решения. При этом в любой информационной системе выделяются основные универсальные модули, наличие которых рекомендовано и регулируется требованиями стандарта [2] для любого комплекса программно-технических средств и организационных решений в рамках системы защиты информации от несанкционированного доступа.

Универсальный перечень включает в себя модули управления доступом, регистрации и учета, обеспечения целостности и достоверности, криптографический, администрирования системы защиты информации.

Этот минимальный набор компонентов, обеспечивающих соответствие подсистемы защиты информации в типовом программно-аппаратном решение требованиям стандарта Банка России, при более детальном рассмотрении является достаточно сложным для реализации. Он покрывает большинство типовых недоработок, встречающихся в «коробочных» продуктах известных мировых лидеров рынка программных решений для финансовых учреждений [2].

Далее освещается ответ на вопрос, что должен включать в себя каждый из перечисленных ранее модулей в типовой информационной системе (далее — ИС)?

1. Модуль управления доступом

В состав требований по реализации модуля управления доступом должны включаться следующие важные положения, о которых часто забывают производители промышленных «коробочных» решений, однако наличие их обязательно для обеспечения безопасного функционирования ИС.

Наличие идентификации (имя учетной записи) и аутентификации (пароль для доступа к ИС) при работе с ИС в многопользовательском режиме. В любом программно-аппаратном решении, реализующем какой-либо банковский продукт, должен быть представлен интерфейс заведения пользователей (как минимум трех типов: администратор системы, администратор безопасности и пользователь).

При работе в удаленном режиме персональные данные пользователей системы, а также данные, относящиеся к коммерческой и банковской тайне, должны передаваться от рабочего места пользователя до центрального ядра ИС в защищенном от внешнего перехвата виде.

При обработке вне ядра подсистемы обеспечения информационной безопасности все пользовательские данные должны быть защищены от принудительной модификации внешними по отношению к ИС средствами. Целостность этих данных должна обеспечиваться средствами самой ИС.

Для значений, используемых пользователями ИС в качестве паролей для доступа к ИС, должны быть предусмотрены гибко настраиваемые правила и шаблоны, такие как длина, срок действия, алфавит, повторное использование одного и того же пароля, контроль попыток неуспешного ввода пароля, время блокировки учетной записи при достижении заданного числа неправильного ввода пароля и другие.

Пароли для доступа к ИС должны храниться в защищенном (хешированном) виде, при этом одинаковые пароли для различных пользователей должны иметь различные хэш-значения. Доступ к хранилищу паролей средствами, отличающимися от программных интерфейсов ИС, должен быть запрещен.

Операции по смене пароля пользователю должны быть доступны самому пользователю и администратору информационной системы, но при этом подтверждена администратором безопасности (правило «четырех рук»).

В ИС должны быть предусмотрены групповые политики управления доступов и назначения прав пользователям, а также возможности по созданию типовых профилей и ролей для пользователей, при этом любые права должны назначаться администратором информационной системы и подтверждаться администратором безопасности.

В ИС должны быть реализованы объекты и субъекты доступа. Права доступа субъектов к объектам доступа должны назначаться в матрице доступа. Контроль доступа должен осуществляться в соответствии с правилами, описанными в матрице доступа.

Доступ пользователей должен быть ограничен списком оборудованных интерфейсом клиентского приложения и идентифицированных (лицензией и/или внутренним наименованием) терминалов.

Модуль управления доступом должен быть оснащен единой консолью (программным интерфейсом) управления доступом, в которой должны быть отражены все указанные ранее модули.

2. Модуль регистрации и учета

Требования по реализации модуля регистрации и учета должны включать в себя положения, связанные с наличием в системе журнала регистрации событий, его структуре и формату хранения записей.

ИС должна иметь в своем составе программные средства, протоколирующие в том числе следующие событии: действия по управлению учетными записями, жизненный цикл объектов и субъектов доступа, ошибки в работе ИС, внешние и внутренние действия с ИС, запросы от имени пользователя в системе и т. д.

Модуль протоколирования событий в системе должен предполагать хранение старые и новые значения объектов, а также измененные свойства объектов.

Модификация записей, когда-либо занесенных в журнал, должна быть запрещена для любого пользователя, в том числе администратора системы и администратора безопасности. Целостность записей в журнале должна контролироваться на уровне ИС.

Подсистема журналирования должна предоставлять интерфейс просмотра событий в режиме реального времени в рамках консоли (программного интерфейса) контроля доступа администратора безопасности.

Формат записей в журнале регистрации событий должен предполагать наличие следующих обязательных полей: уникальный порядковый номер, обеспечивающий целостность записи в рамках журнала; идентификатор пользователя или процесса, который стал причиной события; дата и время события в относительных единицах времени; идентификатор события, связанный со словарем событий в ИС; идентификатор результата события; контрольную сумму записи, вычисляемую непосредственно при занесении записи в журнал, необходимую для обеспечения целостности журнала.

Модуль регистрации должен обеспечивать учет и хранение всех событий информационной безопасности.

3. Модуль обеспечения целостности и достоверности

Требования по наличию в ИС модуля обеспечения целостности и достоверности предполагают существование инструментов контроля успешного завершения операций в системе, наличие средств выполнения резервного копирования и восстановления, а также программных и аппаратных интерфейсов диагностики и тестирования ИС.

В ИС должны быть реализованы инструменты выполнения резервного копирования и оперативного восстановления компонентов ИС на определенный момент времени. Срок хранения резервных копий должен определяться функциональными требованиями. Инструменты выполнения резервного копирования могут быть внешними по отношению к ИС.

ИС должна иметь возможность работы в режиме отказоустойчивого кластера. Режим работы кластера должен определяться функциональными требованиями.

Для любой операции с объектами в ИС должна быть предусмотрена возможность «отката» на момент времени «до» совершения операции.

В ИС должен быть предусмотрен инструментарий, позволяющий проводить оперативное тестирование и диагностику компонентов, входящих в состав ИС.

Интерфейсы управления процедурой резервного копирования и восстановления модулей ИС должны быть выведены на консоль управления администратора системы и администратора безопасности.

Любой объект в ИС должен содержать в своем составе полный набор параметров, характеризующих его текущее состояние, в том числе метку целостности, контроль за состоянием которой осуществляет ядро ИС.

4. Криптографический модуль

В соответствии с п. 1 Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, в информационных системах, обрабатывающих персональные данные граждан РФ, а также работающих с финансовой информацией, составляющей Банковскую тайну (Статья 26 Федерального Закона «О банках и банковской деятельности»), должны использоваться только сертифицированные ФСБ России средства криптографической защиты передаваемой и обрабатываемой информации. В этой связи к криптографическому модулю в числе прочего должны предъявляться следующие требования.

Средства криптографической защиты должны быть реализованы на основе алгоритмов, соответствующим национальным стандартам РФ (ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001) и совместимы на уровне криптографических вычислений, представления данных и средств электронно-цифровой подписи со средствами криптографической защиты, используемыми Федеральным Удостоверяющим центром Российской Федерации.

Должно осуществляться шифрование всей конфиденциальной информации, передаваемой по внешним (в обязательном порядке) и внутренним (опционально) каналам связи.

Секретные ключи шифрования должны храниться на съемных носителях.

В ИС должна быть предусмотрена возможность построения иерархической многоуровневой схемы распределения и использования ключей, а также ведение и обновление справочников открытых ключей и списков отозванных сертификатов.

Средства криптографической защиты должны допускать их встраивание в технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов.

5. Модуль администрирования системы защиты информации

В ИС должна быть реализована консоль управления администратора безопасности (рабочее место администратора безопасности), в интерфейс которого сведены инструменты управления доступом, целостностью, криптографическим модулем и подсистемы протоколирования. К рабочему месту администратора безопасности в том числе должны предъявляться следующие требования.

На рабочем месте администратора безопасности должны быть предусмотрены интерфейсы оперативного контроля работы пользователей (список активных пользователей, информация по учетным записям), информация по блокированным учетным записям, список инцидентов, нарушающих внутреннюю политику и т. д.

С рабочего места администратора безопасности должен быть доступен журнал регистрации событий с интерфейсами навигации по списку хранимых в нем записей, а также реализована возможность гибкого составления отчетов по событиям и инцидентам информационной безопасности в ИС.

Администратор безопасности должен иметь возможность получить права на чтение любого объекта, аналогичные правам любого пользователя в ИС.

Администратор безопасности должен иметь возможность оперативной блокировки и/или изменения прав доступа пользователя к объектам ИС.

В ИС должна быть предусмотрена возможность доработки интерфейса рабочего места администратора безопасности по требованию Заказчика с учетом расширения списка отображаемых событий.

6. Заключение

Представленные выше требования не являются полным универсальным списком требований, которые возможно будет предъявить к любой ИС. Составить полный список без знания специфики работы кредитно-финансовой организации и типа выбираемого технического решения достаточно сложно. Приведенные пункты требований — это обозначенные крупными масками позиции, которые очень часто забываются при формировании требований по обеспечению информационной безопасности, которые предъявляются к выбираемым или планируемым к внедрению в финансовых институтах ИТ-решениям. Для каких-то ИС даже этот малый список требований будет избыточным, для других — недостаточным и/или малоприменимым — это надо понимать и уметь кастомизировать и адаптировать требования по информационной безопасности с учетом специфики работы конкретной кредитно-финансовой организации.

Что же касается ответа на поставленный в начале статьи вопрос, хочется сказать следующее: очень часто возникают сложности с составлением требований по защите информации, которые должны предъявляться к какому-либо неизвестному решению. Эти сложности вызваны в большей степени отсутствием времени у сотрудников. В меньшей это вызвано отсутствием экспертов по информационной безопасности, имеющих возможность четко и быстро сформулировать полный перечень технических и организационных положений, на основе которых можно было бы составить что-либо похожее на спецификацию требований по информационной безопасности, не забыв при этом деталей и особенностей работы организации. В таких ситуациях очень часто приходится обращаться к услугам внешних организаций, выполняющих оплачиваемые работы по сбору и формированию спецификации требований пользователей, в том числе по информационной безопасности. С одной стороны это удобно и сравнительно быстро, с другой — в таких ситуациях приходится открывать сотрудникам внешней по отношению к кредитно-финансовому институту организации многие внутренние особенности функционирования собственной инфраструктуры, которые по ряду причин должны быть скрыты от «внешних глаз».

Поэтому в большинстве ситуаций, связанных с выбором программно-аппаратных решений, предлагаемых внешним ИТ-интегратором, для экспертов по информационной безопасности в кредитно-финансовых организациях выгодно иметь универсальный перечень требований, пусть избыточный, но содержащий «крупными мазками» полный список рекомендованных стандартами и законами РФ требований по обеспечению информационной безопасности.

Но при формировании подобных требований никогда не стоит забывать об извечной конфликте функционального удобства ИТ-решения и защищенности обрабатываемой внутри него информации. Именно поэтому сформированные требования по информационной безопасности не должны идти наперекор бизнес-функциональности предлагаемого ИТ-решения.

В рамках данной статьи экспертам по информационной безопасности, работающим в кредитно-финансовых учреждениях и государственных институтах, предлагается дополнительное направление деятельности, связанное с осуществлением контроля обеспечения информационной безопасности и защиты информации на этапах проектирования и внедрения ИТ-решений в организациях. Ведение такого рода деятельности позволяется минимизировать операционные риски, связанные с отсутствием у заказчика требований по обеспечению защиты информации, и, как следствие, отсутствие или частичная реализация подсистемы обеспечения зашиты информации в комплексных функционально востребованных решениях крупных компаний-производителей программного обеспечения. Ориентация на особого потребителя в

маркетинговых политиках компании-производителей и интеграторов промышленных решений, а также специфика работы и адаптации к условиям законодательства Российской Федерации в области защиты информации накладывают на предполагаемые к внедрению решения целый ряд ограничений. Устранение этих недостатков является совместной задачей экспертов по информационной безопасности, представителей ИТ-блока и бизнес-подразделений.

СПИСОК ЛИТЕРАТУРЫ:

1. *Курило А. П. [и др.]*. Обеспечение информационной безопасности бизнеса. М, 2005. — 512 с.
2. Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
3. Информационная безопасность компьютерных систем с сетей: учебное пособие М., 2008. — 416 с.

А. К. Плешков
Московский инженерно-физический институт (государственный университет)

ФАКТОРЫ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

В статье рассмотрен термин «инсайдер» (внутренний нарушитель политики информационной безопасности). Предложены к обсуждению внешние и внутренние факторы, способные оказать влияние на изменению уровня «инсайдерской» деятельности в кредитно-финансовой организации Российской Федерации. Продемонстрирован подход к рассмотрению терминов «инсайдер» и «внутренний нарушитель» в контексте основных положений стандарта Банка России СТО БР ИББС-1.0-2006.

За последнее время в лексиконе экспертов по информационной безопасности появилось и укрепилось огромное число новых, ранее неиспользуемых терминов, определяющих субъекты и объекты отношений различного рода, а также действия в отношении каждого из участников: «фишинг» (от англ. — «phishing» — разновидность атак класса «социальной инженерии»), «фрод» (от англ. — «fraud» — мошенничество), «дефейс» (от англ. «deface» — разбор интерфейса на составные части), «досить» (от англ. «Denail of Service» — отказ в обслуживании) и т. д. Особое место в словаре занимает термин «инсайдер» (от англ. «insider» — кто-либо работающий внутри).

Рассмотрим последний термин более подробно применительно к обеспечению информационной безопасности в кредитно-финансовых организациях Российской Федерации.

В сфере торговли ценными бумагами существует следующее частное определение: «инсайдер» — лицо, имеющее доступ к внутренней информации организации в силу: своего служебного положения; договора с организацией, выполнения государственных контрольных функций или иной профессиональной деятельности; а также родственных и иных связей с другим лицом, располагающим такой информацией.

В соответствии с федеральным законом «О рынке ценных бумаг» в редакции 1996 года к «инсайдерам» — лицам, располагающим служебной информацией, — относятся: члены органов управления или профессионального участника рынка ценных бумаг, связанного с этим эмитентом договором; физические лица — профессиональные участники рынка ценных бумаг; аудиторы; служащие государственных органов, имеющие в силу контрольных, надзорных и иных полномочий доступ к