Информационная безопасность банковских безналичных платежей. Часть 3 — Формирование требований к системе защиты

В предыдущих частях исследования мы обсудили экономические основы и IT-инфраструктуру банковских безналичных платежей. В этой части речь пойдет о формировании требований к создаваемой системе информационной безопасности (ИБ).

Далее мы рассмотрим:

- роль обеспечения безопасности в жизни коммерческой организации;
- место службы информационной безопасности в структуре менеджмента организации;
- практические аспекты обеспечения безопасности;
- применение теории управления рисками в ИБ;
- основные угрозы и потенциальный ущерб от их реализации;
- состав обязательных требований, предъявляемых к системе ИБ банковских безналичных платежей.

Роль обеспечения безопасности в жизни коммерческой организации

В современной российской экономической среде существует множество различных типов организаций. Это могут быть государственные предприятия (ФГУП, МУП), общественные фонды и, наконец, обычные коммерческие организации. Главным отличием последних от всех других является то, что их основная цель – получение максимальной прибыли, и все, что они делают, направлено именно на это.

Зарабатывать коммерческая организация может различными способами, но прибыль всегда определяется одинаково – это доходы за вычетом расходов. При этом, если обеспечение безопасности не является основным видом деятельности компании, то оно не генерирует доход, а раз так, то для того, чтобы эта деятельность имела смысл, она должна снижать расходы.

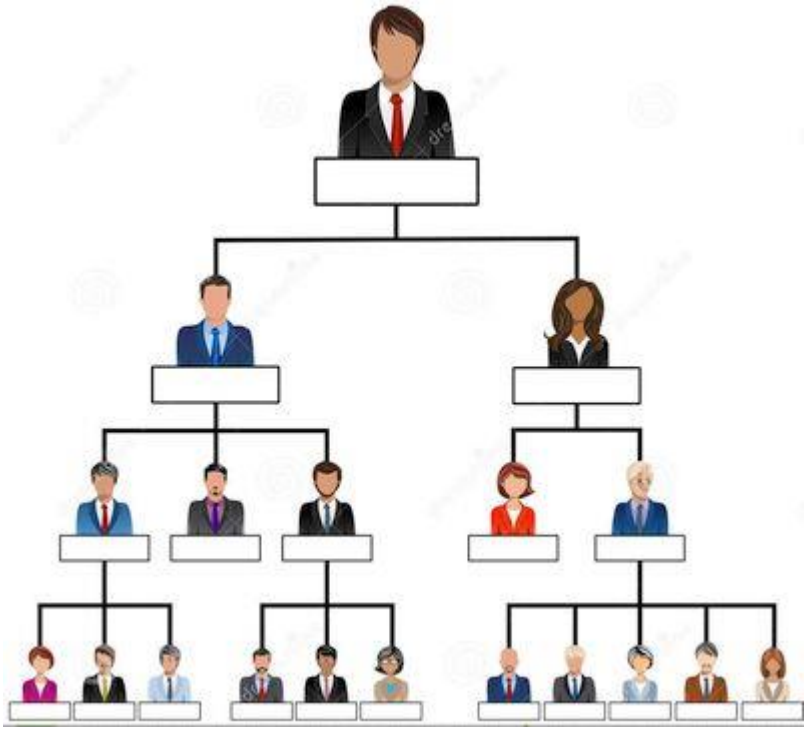
Экономический эффект от обеспечения безопасности бизнеса заключается в минимизации или полном устранении потерь от угроз. Но при этом также следует учитывать то, что реализация защитных мер тоже стоит денег, и поэтому истинная прибыль от безопасности будет равна размеру сэкономленных от реализации угроз безопасности средств, уменьшенному на стоимость защитных мер.

Однажды между собственником коммерческого банка и руководителем службы безопасности его организации состоялся разговор на тему экономического эффекта от обеспечения безопасности. Суть этого разговора наиболее точно отражает роль и место обеспечения безопасности в жизни организации:

— Безопасность не должна мешать бизнесу.
— Но за безопасность надо платить, а за ее отсутствие расплачиваться.

Идеальная система безопасности – это золотая середина между нейтрализованными угрозами, затраченными на это ресурсами и прибыльностью бизнеса.

Место службы информационной безопасности в структуре менеджмента организации



Структурное подразделение, отвечающее за обеспечение информационной безопасности, может назваться по-разному. Это может быть отдел, управление или даже департамент ИБ. Далее для унификации это структурное подразделение будем называть просто службой информационной безопасности (СИБ).

Причины создания СИБ могут быть разными. Выделим две основные:
1. **Страх**. Руководство компании осознает, что компьютерные атаки или утечки информации могут привести к катастрофическим последствия, и предпринимает усилия для их нейтрализации.
2. **Обеспечение соответствия законодательным требованиям**. Действующие законодательные требования налагают на компанию обязательства по формированию СИБ, и топ-менеджмент предпринимает усилия по их исполнению.

Применительно к кредитным организациям необходимость существования СИБ зафиксирована в следующих документах:

1. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
2. «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком России 09.06.2012 N 382-П) (ред. от 14.08.2014) (Зарегистрировано в Минюсте России 14.06.2012 N 24575).
3. «Положение о требованиях к защите информации в платежной системе Банка России» (утв. Банком России 24.08.2016 N 552-П) (Зарегистрировано в Минюсте России 06.12.2016 N 44582).
4. Требования лицензии ФСБ России на криптографию: Постановление Правительства РФ от 16.04.2012 N 313, Приказ ФАПСИ от 13.06.2001 N 152 (СИБ, как орган криптозащиты).
5. Для банков, обладающих значимыми объектами ключевой информационной инфраструктуры — Приказ ФСТЭК России от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (Зарегистрировано в Минюсте России 22.02.2018 N 50118).

Требуемый от СИБ функционал прописан в выше указанных документах. Штатная численность жестко не регламентирована, за исключением, пожалуй, лицензионных требований ФСБ России на криптографию (минимум 2 сотрудника, но они могут быть в разных подразделениях) и может выбираться организацией самостоятельно. Для обоснования размера штата рекомендуется пользоваться документом — Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности" РС БР ИББС-2.7-2015»

С точки зрения подчиненности СИБ существует только одно ограничение, прописанное в вышеуказанных положениях ЦБ РФ — «Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора», в остальном свобода выбора остается за организацией. Рассмотрим типовые варианты.

Таблица 1.

Подчиненность	Особенности
СИБ в составе IT	1. Организация защиты возможна только против внешнего злоумышленника. Основным вероятным внутренним злоумышленником является сотрудник IT. Бороться с ним в составе IT невозможно. 2. Нарушение требований Банка России. 3. Прямой диалог с IT, простое внедрение систем защиты информации
СИБ в составе службы безопасности	1. Защита от действий как внутренних злоумышленников, так и внешних. 2. СБ — единая точка взаимодействия топ-менеджмента по любым вопросам безопасности. 3. Сложность взаимодействия с IT, поскольку общение происходит на уровне глав IT и СБ, а последний, как правило, обладает минимальными знаниями в IT.
СИБ подчиняется Председателю Правления	1. СИБ обладает максимальными полномочиями и собственным бюджетом. 2. Для Председателя Правления создается дополнительная точка контроля и взаимодействия, требующая к себе определенного внимания. 3. Возможные конфликты СБ и СИБ по зонам ответственности при расследовании инцидентов. 4. Отдельный СИБ может «политически» уравновешивать полномочия СБ.

При взаимодействии с другими структурными подразделениями и топ-менеджментом банка у СИБ любой организации есть одна общая проблема — доказательства необходимости своего существования (финансирования).

Проблема заключается в том, что размер сэкономленных средств от нейтрализованных угроз информационной безопасности невозможно точно определить. Если угроза не реализовалась, то и ущерба от нее нет, а раз проблем нет, то и не нужно их решать.

Для решения этой проблемы СИБ может действовать двумя способами:

1. **Показать экономическую значимость**

Для этого ей необходимо вести учет инцидентов и оценивать потенциальный ущерб от их реализации. Совокупный размер потенциального ущерба можно считать сэкономленными денежными средствами. Для устранения разногласий по размеру оцениваемого ущерба рекомендуется предварительно разработать и утвердить методику его оценки.

2. **Заниматься внутренним PR-ом**

Рядовые работники организации обычно не знают, чем занимается СИБ, и считают ее сотрудников бездельниками и шарлатанами, мешающими работать, что приводит к

ненужным конфликтам. Поэтому СИБ должна периодически доносить до коллег результаты своей деятельности, рассказывать об актуальных угрозах ИБ, проводить обучения и повышать их осведомленность. Любой сотрудник компании должен чувствовать, что, если у него возникнет проблема, связанная с ИБ, то он может обратиться в СИБ, и ему там помогут.

Практические аспекты обеспечения безопасности

Выделим практические аспекты обеспечения безопасности, которые обязательно должны быть донесены до топ-менеджмента и других структурных подразделений, а также учтены при построении системы защиты информации:

1. Обеспечение безопасности — это непрерывный бесконечный процесс. Степень защищенности, достигаемая с ее помощью, будет колебаться с течением времени в зависимости от воздействующих вредоносных факторов и усилий, направленных на их нейтрализацию.
2. Безопасность невозможно обеспечить постфактум, то есть в тот момент, когда угроза уже реализовалась. Чтобы нейтрализовать угрозу, процесс обеспечения безопасности должен начаться до попытки ее реализации.
3. Большая часть угроз имеет антропогенный характер, то есть организации тем или иным образом угрожают люди. Как говорят компьютерные криминалисты: «Воруют не программы, воруют люди».
4. В нейтрализации угроз должны участвовать люди, чья безопасность обеспечивается, будь это собственники бизнеса или клиенты.

5. Безопасность — это производная от корпоративной культуры. Дисциплина, требуемая для реализации защитных мер, не может быть выше общей дисциплины при работе организации.

Подводя промежуточный итог под вышесказанным, отметим, что создаваемая система ИБ безналичных платежей должна иметь практическую направленность и быть экономически эффективной. Лучшим подспорьем в достижении указанных свойств является применение риск-ориентированного подхода.

Управление рисками (risk management)

Информационная безопасность — это всего лишь одно из направлений обеспечения безопасности (экономическая безопасность, физическая безопасность, пожарная безопасность, …). Помимо угроз информационной безопасности, любая организация подвержена другим, не менее важным угрозам, например, угрозам краж, пожаров, мошенничества со стороны недобросовестных клиентов, угрозам нарушения обязательных требований (compliance) и т. д.

В конечном счете для организации все равно, от какой конкретно угрозы она понесет потери, будь то кража, пожар или компьютерный взлом. Важен размер потерь (ущерб).

Кроме размера ущерба, важным фактором оценки угроз является вероятность из

реализации, которая зависит от особенностей бизнес-процессов организации, ее инфраструктуры, внешних вредоносных факторов и принимаемых контрмер.

Характеристика, учитывающая ущерб и вероятность реализации угрозы, называется риском.
Примечание. Научное определение риска можно получить в ГОСТ Р 51897-2011

Риск может быть измерен как количественно, например, путем умножения ущерба на вероятность, так и качественно. Качественная оценка проводится, когда ни ущерб, ни вероятность количественно не определены. Риск в этом случае может быть выражен как совокупность значений, например, ущерб — «средний», вероятность — «высокая».

Оценка всех угроз как рисков позволяет организации эффективным образом использовать имеющиеся у нее ресурсы на нейтрализацию именно тех угроз, которые для нее наиболее значимы и опасны.

Управление рисками является основным подходом к построению комплексной экономически эффективной системы безопасности организации. Более того, почти все банковские нормативные документы построены на базе рекомендаций по управлению рисками Базельского комитета по банковскому надзору.

Основные угрозы и оценка потенциального ущерба от их реализации

Выделим основные угрозы, присущие деятельности по осуществлению банковских безналичных платежей, и определим максимальный возможный ущерб от их реализации.

Таблица 2.

№	Угроза	Максимальный возможный ущерб
1	Прекращение (длительная остановка) деятельности	Отзыв лицензии на банковскую деятельность
2	Кража денежных средств	В размере остатка денежных средств на счетах
3	Нарушение обязательных требований к деятельности, установленных действующим законодательством и договорами с Банком России	Отзыв лицензии на банковскую деятельность

Здесь в состав анализируемой деятельности входит совокупность бизнес-процессов:

- реализация корреспондентских отношений с банками-партнерами и ЦБ РФ;
- проведение расчетов с клиентами.

В дальнейшем мы будем рассматривать только вопросы обеспечения безопасности корреспондентских отношений с Банком России. Тем не менее, полученные наработки могут быть использованы для обеспечения безопасности и других видов расчетов.

Обязательные требования к системе ИБ безналичных платежей

При рассмотрении основных угроз мы оценили их ущерб, но не оценили вероятность их реализации. Дело в том, что если максимально возможный ущерб будет одинаковым для любых банков, то вероятность реализации угроз будет отличаться от банка к банку и зависеть от применяемых защитных мер.

Одними из основных мер по снижению вероятности реализации угроз информационной безопасности будут:

- внедрение передовых практик по управлению IT и инфраструктурой;
- создание комплексной системы защиты информации.

Про IT практики здесь мы говорить не будем, затронем только вопросы обеспечения информационной безопасности.

Основным нюансом, который необходимо учитывать в вопросах обеспечения информационной безопасности, является то, что данный вид деятельности довольно жестко регулируется со стороны государства и Центрального Банка. Как бы не оценивались риски, как бы не малы были те ресурсы, которыми располагает банк, его защита должна удовлетворять установленным требованиям. В противном случае он не сможет работать.

Рассмотрим требования по организации защиты информации, налагаемые на бизнес-процесс корреспондентских отношений с Банком России.

Таблица 3.

Документы, устанавливающие требования	**Наказание за невыполнение**
Защита персональных данных. Основание – в платежных документах есть персональные данные (Ф.И.О. плательщика / получателя, его адрес, реквизиты документа, удостоверяющего личность)	
Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ	КоАП РФ Статья 13.11, КоАП РФ Статья 13.12 – до 75 тыс. руб. штраф., УК РФ Статья 137 – до 2 лет лишения свободы
Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	
Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375)	
Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации	

Документы, устанавливающие требования	Наказание за невыполнение
требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 N 33620)	
Указание Банка России от 10 декабря 2015 г. № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных”	
Обеспечение защиты информации в национальной платежной системе. Основание – кредитная организация, выполняющая переводы денежных средств, является частью национальной платежной системы.	
Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ	п.6 ст. 20 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» – отзыв лицензии
Постановление Правительства РФ от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе»	
Положение Банка России от 9 июня 2012 г. N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»	
Положение Банка России от 24 августа 2016 г. № 552-П «О требованиях к защите информации в платежной системе Банка России»	
Эксплуатационная документация на СКЗИ СКАД Сигнатура	
Обеспечение безопасности критической информационной инфраструктуры Российской Федерации. Основание – банк в силу п.8 ст. 2 ФЗ от 26.07.2017 № 187-ФЗ является субъектом критической информационной инфраструктуры	
Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	УК РФ Статья 274.1 – до 8 лет лишения свободы
Постановление Правительства РФ от 08.02.2018 N 127 »Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений"	
Приказ ФСТЭК России от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»	

Документы, устанавливающие требования	Наказание за невыполнение
(Зарегистрировано в Минюсте России 22.02.2018 N 50118)	
Приказ ФСТЭК России от 06.12.2017 N 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 08.02.2018 N 49966)	
Указ Президента РФ от 22.12.2017 N 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»	
Требования по защите информации, установленные договором об обмене электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России. Основание – данный договор заключают все кредитные организации для электронного обмена платежными документами с Банком России.	
Типовой договор обмена ЭС с приложениями. Документация на АРМ КБР, УТА (требования их использовании отражены в п.1. Приложения 3 к Договору)	п. 9.5.4 Договора – одностороннее расторжение договора по инициативе Банка России.

Обозначим также дополнительные требования к организации защиты информации. Данные требования будут распространяться лишь на некоторые банки и лишь в некоторых случаях:

1. СТО БР ИББС. Стандарт и комплекс сопутствующих документов имеет силу только в случае его добровольного принятия кредитной организацией.
2. PCI DSS. Стандарт будет действовать, только если в платежных документах передаются полные не маскированные номера платежных карт (PAN).
3. Корпоративная политика информационной безопасности. Требования актуальны для больших банковских групп, где единая политика ИБ устанавливается в отношении всех банков группы и где каждый банк должен разрабатывать на ее базе внутренние документы.

Конечными результатами применения всех этих требований должна стать система обеспечения информационной безопасности, удовлетворяющая любому из перечисленных документов. Для того, чтобы создать такую систему, требования сводят в единую таблицу и в случаях, когда есть несколько схожих требований, выбирают наиболее жесткие из них.

Здесь есть важный нюанс: требования, задаваемые в нормативных документах, как правило, не содержат жесткой конкретики. В них указывается то, как система

безопасности должна выглядеть, из каких средств состоять и какими тактическими характеристиками обладать. Исключением будут требования, исходящие из эксплуатационной документации на применяемые средства защиты информации, например, на СКЗИ СКАД Сигнатуру.

Рассмотрим, например, фрагмент требований Приказа ФСТЭК № 21

Таблица 4.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
....					
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+

Как мы видим, требования **АВЗ.1** и **АВЗ.2** говорят о том, что антивирусная защита должна быть. То, как конкретно ее настраивать, на каких узлах сети устанавливать, эти требования не регламентируют (Письмо Банка России от 24.03.2014 N 49-Т рекомендует банкам иметь на АРМах, на серверах и на шлюзах антивирусы различных производителей).

Аналогичным образом обстоят дела и с сегментацией вычислительной сети – требование **ЗИС.17**. Документ только предписывает необходимость использования этой практики для защиты, но не говорит, как организация должна это делать.

То, как конкретно настраиваются средства защиты информации, и реализуются защитные механизмы, узнают из частного технического задания на систему защиты информации, сформированного по результатам моделирования угроз информационной безопасности.

Таким образом, комплексная система информационной безопасности должна представлять собой набор защитных бизнес-процессов (в англоязычной литературе –

controls), построенных с учетом исполнения обязательных требований, актуальных угроз и практики обеспечения ИБ.