МОДЕЛИРОВАНИЕ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

Гринева Н.В.
Финансовый университет при Правительстве Российской Федерации
ngrineva@fa.ru

Аннотация: Выявлены наиболее критичные информационные системы Банка, получен список классов угроз. Предложена методика оценки вероятности реализации угроз, прогнозируемого уровня потерь и частоты реализации угрозы, ожидаемого значения ущерба в год для каждого типа нарушений. Предложена система управления рисками и выработаны рекомендации по ее применению.

Ключевые слова: оценка рисков, управление рисками, информационная безопасность, активы компании, ущерб.

Работа выполнена по гранту РФФИ №19-010-00698 на тему: «Развитие теории интеллектуального капитала и методов его оценки в условиях цифровизации экономики».

Введение

Процесс управления рисками информационной безопасности включает в себя идентификацию значимых угроз и критичных информационных систем, проведение первичной оценки, предотвращение развития риска, выбор тактики устранения риска, восстановление безопасности после инцидента, документирование риска, оценку нанесенного ущерба, выработку превентивных и корректирующих мер. В связи со всеобщей информатизацией и компьютеризацией бизнеса, значение информационной безопасности сильно возросло.

В Банке необходимо выстроить эффективную иерархичную система распределения полномочий и ответственности с точки зрения обеспечения информационной безопасности. В результате повсеместного распространения электронных платежей, банковских карт, компьютерных сетей, стремительно растущей популярности услуг, предоставляемых клиентам посредством интернет-технологий, значительно увеличилось количество угроз целью воздействия которых является влияние на информацию ограниченного доступа. Как правило, все угрозы воздействуют на три свойства информационных активов: конфиденциальность, целостность и доступность. Условно говоря, угрозы, воздействующие на информационные активы банка и приводящие к реализации информационного риска, можно разделить на две категории: угрозы, обусловленные внутренними причинами, и угрозы, обусловленные внешними причинами.

Информационный риск относится к одним из наиболее распространенных в банковской отрасли и является составной частью операционного риска. Однако, в организациях уделяют недостаточное внимание оценке информационного риска в отдельности от операционного, поскольку считают, что внедрение мер по информационной безопасности является достаточным условием для ее обеспечения. Был проведен опрос среди пользователей сайта www.iso27000.ru, в котором у специалистов в области информационной безопасности поинтересовались как они оценивают риски ИБ. Согласно опросу, доля людей, оценивающих риски информационной безопасности «на глазок» крайне высока (около 30%), также около 16% людей не оценивают риски или считают это бессмысленным [5].

Основная цель принимаемых мер по управлению рисками информационной безопасности и защите информации состоит в том, чтобы обеспечить целостность, доступность и конфиденциальность информации во всех ее видах и формах, обрабатываемую, хранимую и передаваемую в информационных системах Банка.

1 Идентификация риска

Для осуществления идентификации информационного риска, определим объект, субъект и неблагоприятные события, приводящие к его реализации.

Субъектом риска является руководство банка NNN(далее - Банк).Основная деятельность Банка включает в себя привлечение денежных средств физических и юридических лиц во вклады, открытие и ведение счетов юридических и физических лиц, осуществление кассовых и расчетных операций, кредитование юридических и физических лиц, предоставление гарантий, осуществление операций с ценными бумагами, доверительное управление денежными средствами и иным

имуществом физических и юридических лиц, а также куплю-продажу иностранной валюты в наличной и безналичной формах.

Объектом риска являются информационные активы Банка. Под информационными активами в работе будут пониматься информационные системы Банка, так как в них хранится, обрабатывается и через них передается информация ограниченного доступа. В ходе анализа деятельности Банка были выявлены наиболее критичные информационные системы:

1. Система дистанционного банковского обслуживания (ДБО).
2. Система автоматического скоринга заёмщиков.
3. Система IBSO (IB System Object).
4. СистемаSWIFT (Society of Worldwide Interbank Financial Telecommunications).
5. Корпоративная электронная почта.
6. Система предоставления доступа работников в интернет.
7. Система обслуживания банковских карт.

Неблагоприятное событие состоит в реализации угрозы, поэтому для проведения идентификации необходимо выявить наиболее актуальные угрозы и проанализировать их относительно критичных информационных систем банка. Разделим угрозы на 5 классов, сформированные относительно свойств информационных активов: конфиденциальности, целостности и доступности. При этом нарушения целостности и доступности проанализируем за два временных промежутка (1 час и 4 часа), таким образом сможем оценить, как изменяется уровень потерь в зависимости от времени. Получаем следующий список классов угроз:

- К – класс угроз, связанных с нарушением конфиденциальности информационных систем Банка;
- Ц1 – класс угроз, связанных с нарушением целостности информационных систем Банка в течение 1 часа;
- Ц2 – класс угроз, связанных с нарушением целостности информационных систем Банка в течение 4 часов;
- Д1 – класс угроз, связанных с нарушением доступности информационных систем Банка в течение 1 часа;
- Д2 – класс угроз, связанных с нарушением доступности информационных систем Банка в течение 4 часов.

Наиболее распространенным классом угроз является класс, связанный с нарушениями доступности информационных систем. Среди выявленных угроз самым распространённым видом источников угроз является антропогенный, так как он обусловлен действиями человека. Самой актуальной из внешних угроз является киберугроза.

К киберугрозам относятся угроза «фишинга» [6], угроза «фарминга», угроза внедрения вредоносных программ, таких как программные закладки, вирусы, сетевые черви, угроза внедрения кода или данных, угроза преодоления парольной защиты. Киберугроза обусловлена антропогенным внешним источником и может быть направлена на все типы нарушений (конфиденциальности/ целостности/ доступности) в информационных системах, однако наиболее распространенным является нарушение конфиденциальности системы.

По выявленным угрозам построим шаблон рисков, в котором выявлены факторы, повышающие и понижающие информационный риск для каждого класса угроз. Список угроз был сформирован при использовании документов: ГОСТ Р ИСО/МЭК 27005-2010 [1] и банка данных угроз безопасности информации, разработанный Федеральной службой по техническому и экспортному контролю России (ФТСЭК) [2]. Шаблон рисков представлен в Таблице 1.

Таблица 1. Шаблон рисков

Класс угроз/Факторы	Факторы, повышающие информационный риск	Факторы, понижающие информационный риск
К (Угрозы, связанные с нарушениями конфиденциальности информации, обрабатываемой в информационной системе)	Изъяны в механизмах идентификации/аутентификации Недостаточные меры по антивирусной защите Изъяны в протоколах маршрутизации и управления сетью	Использование проверенных механизмов идентификации и аутентификации Регулярная проверка средств антивирусной защиты Набор высококвалифицированных кадров

Класс угроз/Факторы	Факторы, повышающие информационный риск	Факторы, понижающие информационный риск
	Неконтролируемое скачивание программного обеспечения через интернет Уязвимости программного обеспечения Неадекватный набор персонала, занимающегося обслуживанием информационной системы	Мониторинг обслуживания информационной системы Контроль доступа к защищаемой информации Использование проверенных протоколов маршрутизации и управления сетью
Ц1/Ц2 (Угрозы, связанные с нарушениями целостности информации в системе в течение 1 часа/ 4 часов)	Изъяны в механизмах идентификации/аутентификации Неправильная работа технических средств информатизации Недостаточные меры по антивирусной защите Неадекватный набор персонала, занимающегося обслуживанием информационной системы	Регулярная проверка механизмов идентификации и аутентификации Мониторинг работы технических средств информатизации Мониторинг средств антивирусной защиты Контроль доступа к защищаемой информации Набор высококвалифицированных кадров
Д1/Д2 (Угрозы, связанные с нарушениями доступности информации в системе в течение 1 часа/4 часов)	Ошибки в управленческих системах Неправильная работа технических средств Плохая разводка кабелей Нестабильная электрическая сеть Недостаточные меры по антивирусной защите Отсутствие/неправильная работа средств резервного копирования	Проведение регулярных проверок распределенных систем контроля и управленческих систем Физическая и техническая защита информации Мониторинг работы телекоммуникационного оборудования Мониторинг работы электрической сети Регулярный мониторинг средств антивирусной защиты Контроль систем резервного копирования

2 Оценка риска

На первом этапе управлением риска (идентификации риска) был получен шаблон риска, то есть характеристика классов угроз, приводящих к реализации риска.

На втором этапе проведем оценку выявленных угроз, то есть определим вероятность того, что угроза произойдет, и потери, которые при этом понесет Банк. Оценка выявленных событий будет проведена относительно критичных информационных систем Банка.

Вероятности реализации угроз оцениваются по формуле (1).

$$(1) \quad P = (1 - PP)(1 - PD)(1 - C),$$

где P (Probability)– вероятность того, что угроза будет реализована в течение года; PP (Probability of protection) – вероятность предотвращения угрозы; PD (Probability of detection) – вероятность обнаружения угрозы; C (Complexity) – сложность реализации угрозы (вероятность того, что угроза не будет реализована из-за сложности реализации) [4].

Для того, чтобы провести оценку уровней потерь от реализации каждой угрозы, определим прогнозируемые частоты реализации угроз в год. Прогнозируемый уровень потерь в год (L) определяется по формуле (2):

$$(2) \quad L = D * F,$$

где L (Losses) – уровень потерь от реализации угроз (нарушений К, Ц, Д); D (Damage) – ожидаемое значение ущерба от угрозы в год; F (Frequency) – прогнозируемая частота реализации угрозы в год.

Прогнозируемая частота реализации угрозы в год (F) определяется по формуле (3):

$$(3) \quad F = P * F0,$$

где FO (Frequency of occurrence) – прогнозируемая частота возникновения угрозы в год.

Ожидаемое значение ущерба в год для каждого типа нарушений в информационных системах (конфиденциальности/ целостности/ доступности) оценивается по-разному.

По нарушениям целостности информации (К) ожидаемое значение ущерба на анализируемый год определяется по формуле (4):

$$(4) \quad DK(t) = DK(t-1) * Ik,$$

где DK – ожидаемое значение ущерба в год; Ik – среднее значение темпа роста; $t, t-1$ – текущий и предыдущий анализируемые периоды (в годах).

По нарушениям целостности информации (Ц1/Ц2) ожидаемое значение ущерба на анализируемый год определяется по формуле (5):

$$(5) \quad D\text{Ц}(t) = D\text{Ц}(t-1) * I\text{ц} * T,$$

где DЦ – ожидаемое значение ущерба в год; Iц – среднее значение темпа роста; $t, t-1$ – текущий и предыдущий анализируемые периоды (в годах); T – период влияния нарушения на деятельность Банка (в часах).

По нарушениям доступности информации (Д1/Д2) уровень потерь на анализируемый период определяется по формуле (6):

$$(6) \quad DD_j(t) = T * \sum_{j=1}^{7} Pr * Q,$$

где Pr – средняя прибыль от банковской операции в час; Q – коэффициент, учитывающий уровень влияния нарушения доступности информационного сервиса на банковские операции; j – количество информационных активов (систем) Банка.

С помощью вычисления суммы по всем информационным системам в формуле (6), получаем прибыль, которую Банк мог бы получить от реализации соответствующих банковских операций. Потерянная прибыль из-за недоступности информационных систем и есть ущерб от угроз нарушения доступности (Д1/Д2).

Для подсчета уровня потерь от выявленных угроз подставим полученный ожидаемый ущерб и прогнозируемую частоту реализации для каждого класса угроз в формулу (2). Полученные оценённые уровни потерь от нарушений доступности/ целостности/ конфиденциальности относительно информационных систем Банка на ближайший год представлены в Таблице 2.

Таблица 2. Оценка уровня потерь от реализации угроз относительно информационных систем в тыс. руб.

	К	Ц1	Ц2	Д1	Д2
Системы дистанционного банковского обслуживания (ДБО)	5169,02	115,44	461,75	1331,86	1065,49
Системы автоматического скоринга заемщиков	732,29	66,30	159,11	11855,01	9484,01
Система IBSO	601,87	1,44	3,47	48,30	38,64
Система SWIFT	81,01	2,93	11,74	51,37	61,15
Корпоративная электронная почта	1868,85	137,51	427,80	186,22	193,12
Система предоставления доступа работников в интернет	1527,77	0,00	0,00	102,18	136,24
Система обслуживания банковских карт	3767,96	2202,88	8811,52	8979,60	5541,70

Анализ таблицы показывает, что, потери для двух угроз (Ц1/Ц2) относительно системы предоставления доступа работников в интернет равны нулю, это объясняется тем, что вероятности для этих угроз также равны нулю, поскольку нарушение целостности не является характерным для системы предоставления доступа работников в интернет. Отметим, что наибольшие потери по нарушению конфиденциальности возникают в системе ДБО, для нарушения целостности – в системе обслуживания банковских карт, а для нарушения доступности – в системе автоматического

скоринга заемщиков. При анализе полученных данных необходимо обратить пристальное внимание именно на те угрозы, при реализации которых потери являются наибольшими относительно других угроз. Для определения того, какие угрозы представляют реальную опасность для Банка, нужно сопоставить две характеристики для каждой угрозы: вероятность ее реализации и потери, которые при этом понесет Банк.

Для того, чтобы оценить совокупное влияние всех выявленных угроз необходимо сделать общую оценку возможных потерь по ним (при их одновременной реализации):

$$(7) \quad Sum = \sum_{j=1}^{n} \max\left(Ld_{i,j}\right) + \sum_{j=1}^{n} \max\left(Lц_{i,j}\right) + \sum_{j=1}^{n} Lk_j,$$

где Sum – совокупная величина возможных потерь; $\max(Ld_{i,j})$ – максимальная величина возможных потерь из двух типов угроз $Д1, Д2$; $\max(Lu_{i,j})$ – максимальная величина возможных потерь из двух типов угроз $Ц1, Ц2$; i – количество типов угроз Д или Ц; j – количество информационных активов (систем) Банка.

В формуле (7) берем максимум из двух классов угроз для нарушений целостности и доступности, так как, очевидно, что одновременно угрозы Д1 и Д2, а также Ц1 и Ц2, для одинаковых информационных систем реализовываться не могут, поэтому берется наибольшее значение потерь по каждому конкретному активу.

Полученная совокупная оценка риска соотносится с размером капитала (собственных средств) Банка и устанавливается лимит максимально допустимой величины риска:

$$(8) \quad Lim = \frac{Sum}{Kb} * 100\,,$$

где Lim – лимит максимально допустимый величины риска; Kb– капитал (собственные средства) Банка.

На момент проведения оценки лимит установлен в размере 1%. Для вычисления суммарных потерь воспользуемся формулой (7):

$Sum = 55\,260{,}334 \text{тыс. руб.}$

Полученную совокупную оценку риска соотнесем с размером капитала (собственных средств) Банка.

Предположим, что на заданную дату собственные средства Банка (Kb) составляют 10020769 тыс. руб., а максимально допустимый лимит величины риска составляет не более 1% от собственных средств Банка. Подсчитаем значение лимита по формуле (8):

$$Lim = \frac{55260{,}334}{10020769} * 100 \approx 0{,}551\%$$

Получили значение 0,551%, что меньше установленного лимита (1%), следовательно, совокупное влияние всех выявленных угроз не является критичным в отношении размера капитала Банка и мероприятия стоит разрабатывать только в отношении угроз, находящихся в критичной зоне.

Все вышеперечисленные формулы при их объединении в одну систему по своей сути представляют собой методику по оценке вероятности и уровня потерь от реализации угроз. Объединим их в одну систему и отметим, что при условии зависимости параметров от времени уравнения образуют предикативную экономико-математическую модель, которая выглядит следующим образом:

$$(9)\begin{cases} Pk(t) = (1 - PPk)(1 - PDk)(1 - Ck), \\ Fk(t) = Pk(t) * FOk, \\ Lk(t) = Dk * Fk(t), \\ DK(t) = DK(t-1) * Ik, \\ P\text{ц}_i(t) = (1 - PP\text{ц}_i)(1 - PD\text{ц}_i)(1 - C\text{ц}_i) \\ F\text{ц}_i(t) = P\text{ц}_i(t) * FO\text{ц}_i, \\ L\text{ц}_i(t) = D\text{Ц}_i(t) * F\text{ц}_i(t), \\ D\text{Ц}_i(t) = D\text{Ц}_i(t-1) * I\text{ц} * T_i, \\ Pd_i(t) = (1 - PPd_i)(1 - PDd_i)(1 - Cd_i), \\ Fd_i(t) = Pd_i(t) * FOd_i, \\ Ld_{i,j}(t) = DD_{i,j}(t) * Fd_i(t), \\ DD_{i,j}(t) = T_i * \sum_{j=1}^{n} Pr_j * Q_j\,, \\ Sum = \sum_{j=1}^{n} \max\left(Ld_{i,j}(t)\right) + \sum_{j=1}^{n} \max\left(L\text{ц}_{i,j}(t)\right) + \sum_{j=1}^{n} Lk_j\,(t), \\ Lim = \frac{Sum}{Kb} \\ i = 1{,}2; n = 7; T_i = \begin{cases} 1, i = 1 \\ 4, i = 2 \end{cases} \end{cases}$$

где $Pk, P\text{ц}, Pd$ – вероятность того, что угроза (нарушение К, Ц, Д) соответственно будет реализована;

$PPk, PP\text{ц}, PPd$– вероятность того, что угроза (нарушение К, Ц, Д) соответственно будет предотвращена;

$PDk, PD\text{ц}, PDd$– вероятность того, что угроза (нарушение К, Ц, Д) соответственно будет обнаружена;

$Ck, C\text{ц}, Cd$ – вероятность того, что угроза (нарушение К, Ц, Д) не будет реализована из-за сложности реализации;

$Fk, F\text{ц}, \mathrm{F}d$ – прогнозируемая частота реализации угрозы (нарушение К, Ц, Д) в год;

$FOk, FO\text{ц}, FOd$ – прогнозируемая частота возникновения угрозы (нарушение К, Ц, Д) в год;

$DD, DK, D\text{Ц}$ – ожидаемое значение ущерба от реализации угрозы в год (нарушений К, Ц, Д);

$Lk, L\text{ц}, Ld$ – уровень потерь от реализации угрозы (нарушений К, Ц, Д);

T – период влияния нарушения на деятельность Банка (в часах);

Pr – средняя прибыль от банковской операции в час;

Q – коэффициент, учитывающий уровень влияния нарушения доступности информационной системы на банковские операции;

$t, t-1$ – текущий и предыдущий анализируемые периоды; i – количество типов угроз Д или Ц;

j – количество информационных активов (систем) Банка.

Таким образом, общий алгоритм оценки вероятности и уровня потерь при реализации угрозы относительно критичных информационных активов Банка состоит из следующих пунктов:

1. на основании модели на заданный период времени оцениваются риски в разрезе информационных активов / угроз с точки зрения вероятности их реализации и величины возможных потерь. Полученные значения вероятности и потерь выносятся на карты риска, сформированные по классам событий и информационным активам Банка;
2. угрозы, попавшие в критичную зону, рассматриваются как опасные, то есть требующие срочных мер по снижению, поэтому рассчитывается эффективность мер и принимаются решения по нивелированию опасных угроз;
3. оценивается совокупная величина информационного риска и проверяется выполнение лимита. Если лимит выполняется, то мероприятия разрабатываются только для выявленных угроз в критичной зоне; если лимит не выполняется, то дополнительно нивелируются угрозы из зоны допустимых и неопасных угроз, после чего снова осуществляется проверка выполнения лимита и. т.д. до тех пор, пока лимит не будет выполнен.

3 Управление риском

Для выявленных опасных угроз разработаем меры, с помощью которых возможно снизить частоту реализации угрозы в год и потери, которые понесет Банк в случае ее реализации. Начнем с угрозы нарушения доступности системы обслуживания банковских карт в течение 1 часа (угроза Д1). С целью обеспечения бесперебойной доступности информационной системы, принимаем

решение о дополнительных инвестициях в необходимое оборудование – покупка дополнительного оборудования для повышения мощности сервера позволит минимизировать количество простоев банкоматов / терминалов по обслуживанию банковских карт, что минимизирует упущенную выгоду (прибыль по банковским операциям) и, как следствие, потери Банка.

Проведем оценку предлагаемой инвестиции. Оценка эффективности осуществляется на основе стандартного блока показателей [3].

1. Чистая приведенная (дисконтированная) стоимость (NPV) проекта представляет собой разность дисконтированных на один момент времени (обычно на год начала реализации проекта) показателей доходов и расходов (капитальных вложений). NPV вычисляется при заданной норме доходности (ставке дисконтирования) по формуле:

$$(10)\quad NPV = -IC + \sum_{i=1}^{n} \frac{CF_i}{(1+r)^i},$$

где NPV – чистая приведенная стоимость, ден. ед.; CF_i – денежный поток от проекта в i-*ый* период; n – срок инвестиционного проекта (в периодах, например, в годах); r – норма доходности (ставка дисконтирования).

2. Индекс рентабельности инвестиций (PI) рассчитывается следующим образом:

$$(11)\quad PI = \frac{\sum_{i=1}^{n} \frac{CF_i}{(1+r)^i}}{IC},$$

где PI – индекс рентабельности инвестиций, ден. ед.; IC – объем первоначальных инвестиций, ден. ед.

3. Период окупаемости (PP) инвестиционного проекта. Для определения этого показателя используется следующий алгоритм:

- определяется накопленный чистый денежный поток как кумулятивная величина;
- определяется промежуток времени между периодами проекта, в которых отрицательное значения накопленного денежного потока переходит в положительное;
- для получения более точного значения PP используется формула:

$$(12)\quad PP = n, \text{при } \sum_{i=1}^{n} CF_i = IC,$$

где PP – период окупаемости проекта (годы, мес.).

4. Дисконтированный период окупаемости (DPP):

$$(13)\quad DPP = n, \sum_{i=1}^{n} DCF_i = IC,$$

где DPP – дисконтированный период окупаемости проекта (годы, мес.); DCF_i – дисконтированный денежный поток от проекта в i- *ый* период.

Дисконтированный денежный поток в i-*ом* периоде равен:

$$(14)\quad DCF_i = \frac{CF_i}{(1+r)^i}.$$

5. Внутренняя норма доходности (англ. Internal rate of return – IRR) – показатель, позволяющий оценить степень привлекательности альтернативного размещения ресурсов. С экономической точки зрения IRR является граничной ставкой ссудного процента, разделяющей эффективные и неэффективные инвестиционные проекты. IRR – такое значение ставки дисконтирования, при котором $NPV = 0$:

$$(15)\qquad NPV = 0, \sum_{i=1}^{n} \frac{CF_i}{(1+IRR)^i} - IC = 0.$$

Предполагается, что необходимо сделать единовременные инвестиции на сумму 10 350,0 тыс. руб. Внедрение соответствующего оборудования позволит снизить потери от реализации угрозы Д1 (нарушения доступности системы обслуживания банковских карт в течение 1 часа) на 9 030,911 тыс. руб. ежегодно. Тогда экономия на потерях вследствие реализации угрозы в течение ближайших трех лет выглядит следующим образом (Таблица 3).

Таблица 3. Данные о денежных потоках вследствие инвестиции в оборудование для системы обслуживания банковских карт в целях нивелирования угрозы нарушения доступности

	Инвестиции	I (2019)	II (2020)	III (2021)
Доход / экономия				
Снижение потерь	0	9030,911	9030,911	9030,911
Итого	0	9030,911	9030,911	9030,911

	Инвестиции	I (2019)	II (2020)	III (2021)
Расходы				
Затраты на информационную защиту для системы по обслуживанию банковских карт	10350,0			
Допустимые потери (реализация рисков информационной безопасности по системе обслуживания банковских карт)		1 500,0	1 500,0	1 500,0
Итого расходов	10 350,0	1 500,0	1 500,0	1 500,0
Прибыль/убыток	-10350,0	7 530,911	7 530,911	7 530,911
Нарастающим итогом	-10350,0	-2 8919,09	4 711,82	12 242,73

Предварительно оценим, что без учета дисконтирования инвестиция является достаточно эффективной для Банка именно как инвестиция, а не только мера по снижению уровня угрозы недоступности. С учетом дисконтирования она останется эффективной, т.к. NPV проекта имеет положительное значение 6 425,94 тыс. руб. (таблица 4). Ключевые показатели эффективности по инвестиции представлены в Таблице 4.

Таблица 4. Показатели эффективности инвестиции в оборудование для системы обслуживания банковских карт в целях нивелирования угрозы нарушения доступности

$R, \%$	16,5
$NPV,$ тыс. руб.	6 425,94
$IRR, \%$	52,07%
$PP,$ лет	2
$DPP,$ лет	4
PI	162,09%

Ключевые показатели (NPV и IRR) положительны в течение рассматриваемого периода, это говорит об эффективности инвестиции. Кроме того, окупаемость проекта составляет всего два года, что тоже говорит в его пользу. Однако, учитывая тот факт, что Банк, в первую очередь, интересует такая мера как снижение угрозы Д1 относительно системы обслуживания банковских карт, то рассчитаем потери от ее реализации после внедрения закупаемого оборудования:

$$18010510 - 9030911 = 8979599 \text{ руб.} \ = \ 8979{,}599 \text{ тыс. руб.}$$

Таким образом, с помощью предлагаемой инвестиции, Банк сможет снизить потери чуть больше чем в 2 раза за счет того, что снизит частоту реализации угрозы Д1 в год (вместо 7,02 получаем 3,5) посредством установки покупаемого оборудования в рамках проекта.

Для устранения угрозы нарушения конфиденциальности относительно системы обслуживания банковских карт (К) пойдем по уже рассмотренному пути и инвестируем в требуемое оборудование и системы защиты информации. Оценка строится аналогично: при затратах на инвестиции в 1350,0 тыс. руб. экономия на потерях составит 1130,388 тыс. руб. ежегодно. Как инвестиция предлагаемый проект окупится за 2 года (таблицы 5,6).

Таблица 5. Данные о денежных потоках вследствие инвестиции в оборудование для системы обслуживания банковских карт в целях нивелирования угрозы нарушения конфиденциальности

	Инвестиции	I (2019)	II (2020)	III (2021)
Доход / экономия				
Снижение потерь	0	1130,39	1130,39	1 130,39
Итого	0	1 130,39	1 130,39	1 130,39
Расходы				

	Инвестиции	I (2019)	II (2020)	III (2021)
Затраты на информационную защиту для системы по обслуживанию банковских карт	1 350,0			
Допустимые потери (реализация рисков информационной безопасности по системе обслуживания банковских карт)		350,0	350,0	350,0
Итого расходов	1 350,0	350,0	350,0	350,0
Прибыль/убыток	-1 350,0	780,388	780,388	780,388
Нарастающим итогом	-1 350,0	-569,612	210,776	991,164

Ключевые показатели эффективности по инвестиции представлены в Таблице 6.

Таблица 6. Показатели эффективности инвестиции в оборудование для системы обслуживания банковских карт в целях нивелирования угрозы нарушения конфиденциальности

$R, \%$	16,5
NPV, тыс. руб.	388,40
$IRR, \%$	33,52%
PP, лет	2
DPP, лет	4
PI	128,77%

По аналогии с предыдущей инвестицией ключевые показатели (NPV и IRR) положительны в течение рассматриваемого периода, что говорит об эффективности инвестиции. Кроме того, окупаемость проекта составляет всего два года, что тоже говорит в его пользу. Рассчитаем потери от реализации угрозы К после внедрения закупаемого оборудования:

$$3\,767\,961 - 1130988 = 2636973 \text{ руб.} = 2636{,}973 \text{ тыс. руб.}$$

Таким образом, с помощью предлагаемой инвестиции, Банк сможет снизить потери по угрозе К относительно системы обслуживания банковских карт чуть больше, чем на 30% за счет того, что снизит частоту реализации угрозы в год (вместо 0,7 получаем 0,49).

С точки зрения нарушения доступности в течение 1 часа относительно системы автоматического скоринга заемщиков (угроза Д1) на основе анализа непосредственно событий было выявлено, что угроза исходит из того, что не выполняется процедура очередности заявок и основной сервер не выдерживает масштабного одновременного сброса нескольких сотен заявок от кредитных экспертов. В рамках устранения угрозы принимается следующее решение: в течение месяца внутренними силами (сотрудниками подразделения информационной безопасности совместно с сотрудниками ИТ-подразделения будет разработан продукт, обеспечивающий выполнение очередности заявок и одномоментную максимальную нагрузку на сервер не более 50 заявок в минуту.

Затраты на разработку продукта включают в себя только дополнительно оплачиваемые часы ответственным сотрудникам и составят 350 тыс. руб. Ожидаемый эффект от реализации разработки будет заключаться в снижении частоты сбоев сервера практически в 2 раза. Рассчитаем возможные потери от реализации угрозы после внедрения программы:

$$11855010 - 5927505 = 5927505 \text{руб.} = 5927{,}505 \text{ тыс. руб.}$$

Таким образом, с помощью предлагаемой разработки Банк сможет снизить потери по угрозе Д1 относительно системы автоматического скоринга заемщиков в 2 раза за счет того, что снизит частоту реализации угрозы в год (вместо 1,62 получаем 0,81). Ожидаемый эффект от реализации разработки с учетом затрат на разработку программы составит:

$$5927{,}505 - 0{,}350 = 5\,927{,}155 \text{ тыс. руб.}$$

Убедимся, что предложенные меры действительно снизили уровень потерь для ранее опасных угроз. Рассчитаем общую сумму риска с учетом нивелирования угроз и переоценки уровня рисков по соответствующим информационным системам:

$$Sum = 42\,728{,}033 \text{ тыс. руб.}$$

Рассчитаем ее отношение к капиталу Банка и проверим, насколько далеко граница лимита в 1% от полученного значения.

$$Lim = \frac{42728.033}{10020769} * 100 \approx 0{,}426\%.$$

Получили значение 0,426%, что меньше установленного лимита (1%) и меньше полученного ранее значения в 0,551% без нивелирования критичных угроз.

Выводы

Для любых защищаемых данных и документов в каждый конкретный момент времени в Банке должен быть определен круг лиц, которым санкционирован доступ к информационным системам, который необходим этим лицам для исполнения своих должностных обязанностей.

Защищаемая информация должна использоваться сотрудниками только в служебных целях и в рамках полномочий, определенных для отведенной им роли. На рабочем месте должен быть введен запрет на использование информационных ресурсов, ИТ-сервисов и устройств, применение которых не связано с исполнением сотрудником своих служебных обязанностей.

При обработке информации ограниченного доступа каждым сотрудником должны выполняться следующие минимальные требования безопасности:

- доступ в помещения, в которых обрабатывается информация ограниченного доступа, контролируется (не только техническая, но и физическая защита данных);
- пользователи конфиденциальных документов на бумажных носителях должны быть обеспечены надежными металлическими запираемыми шкафами или сейфами для хранения этих документов, а также средствами уничтожения их в случае необходимости;
- для управления доступом к информации ограниченного доступа применяются надежные механизмы аутентификации и идентификации, а также должна проводиться регулярная проверка их;
- при передаче информации ограниченного доступа по открытым каналам должны применяться средства криптографической защиты информации;
- на рабочих местах пользователей должны применяться проверенные средства антивирусной защиты информации;
- должна быть обеспечена подотчетность (протоколирование) действий пользователей и процессов, осуществляющих доступ к информация ограниченного доступа.

Для всех основных информационных систем банка должен регулярно проводится анализ и оценка существующих угроз, связанных с нарушениями доступности/ целостности/ конфиденциальности информационных систем, которые могут привести к значительному ущербу и влиянию на бизнес-процессы.

Для нивелирования последствий опасных угроз и обеспечения своевременного возобновления наиболее существенных бизнес-операций должны быть разработаны планы восстановления соответствующих технологических участков информационной инфраструктуры.

Построение системы управления рисками информационной безопасности в качестве составной части системы управления информационной безопасности имеет целью минимизацию потерь, которые могут быть нанесены вследствие нарушений в информационных системах Банка.

Все описанные действия помогут предотвратить или снизить частоту возникновения нарушений информационной безопасности, а также, в случае их возникновения, своевременно выявлять и нивелировать существующие угрозы.

Для снижения уровня критических угроз необходимо разрабатывать и внедрять комплекс соответствующих мероприятий в соответствие с политиками, законами и стандартами по информационной безопасности.

В работе проведен значительный блок расчетов по всем предлагаемым видам угроз и по всем информационным системам, выделенным для анализа: были оценены такие показатели как вероятность возникновения угрозы, вероятность предотвращения угрозы, вероятность реализации угрозы, сложность реализации угрозы, частота реализации угрозы, ущерб от реализации угрозы и другие.

На основе предлагаемой методики оценки информационного риска Банка сделаны рекомендации по совершенствованию системы обеспечения информационной безопасности Банка, среди которых к наиболее важным стоит отнести построение системы четкого разграничения полномочий сотрудников Банка к информационным системам, обеспечение наличия современных средств информационной защиты (и соответствующего оборудования) для функционирования информационных систем Банка в непрерывном режиме.

Литература

1. ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»(утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 375-ст).
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. 14.02.2008 ФСТЭК России).
3. *Гринева Н. В.* Методологические основы управления рисками инвестиционно-инновационного проекта // Экономика и управление: теория и практика. – 2018. – Т. 4, № 4-1. – С. 50–55.
4. *Гринева Н.В.* Моделирование оценки убытков от информационных угроз в банковской отрасли //Актуальные проблемы прикладной математики, информатики и механики :сборник трудов Международной научной конференции, Воронеж, 17–19 декабря 2018 г. – Воронеж : Издательство «Научно-исследовательские публикации», 2019. –720-726с.
5. http://www.iso27000.ru/golosovaniya/plonepopoll.2007-02-01.0594390779
6. https://fstec.ru/