УПРАВЛЕНИЕ РИСКОМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЭЛЕКТРОННОГО БАНКИНГА[1]

Бердюгин А.А.[2]

Аннотация: *Банковский бизнес развивается в условиях, которые носят неопределённый характер. Финансовые организации должны выстраивать целостную систему управления всеми выявляемыми банковскими рисками. Статья посвящена разработке и формализации подсистемы управления риском нарушения информационной безопасности в рамках общей системы управления рисками кредитно–финансовой организации. Даётся определение информационного общества. Приводятся вычисления на основе статистики Росстата и Банка России. Рассматриваются мотивы, движущие нарушителем информационной безопасности коммерческого банка. Проведён динамический анализ количества устройств, предназначенных для осуществления операций с использованием и без использования платёжных карт, расположенных в России.*

Исследуются виды угроз системе защиты информации коммерческого банка, к которым относятся инсайдерские инциденты, внешние кибератаки и приёмы социальной инженерии. Работа привлекает наше внимание к реализации реинжиниринга бизнес–процессов в банковской информационной безопасности. С учётом современных условий возникновения рисков проанализирована схема древнеримского учёного Квинтиллиана, которая предназначена для описания любой проблемы. Приведён примерный перечень вопросов, позволяющих получить информацию о качестве управления риском нарушения информационной безопасности в коммерческом банке. Делаются соответствующие выводы об оптимизации качества управления риском нарушения защиты информации в банках.

Ключевые слова: *управление рисками, финансовая организация, информационная безопасность, дистанционное банковское обслуживание, компьютерные инциденты.*

DOI: 10.21681/2311-3456-2018-1-28-38

Развитие и регулирование информационного общества

Представление «Информационное общество» не закрепилось в современном мире, как «Гражданское общество», для которого важным вопросом остаётся независимость гражданского общества от прямого вмешательства и произвольной регламентации со стороны государственной власти и бизнеса [1]. Тем не менее, образное понимание информационного общества даёт следующая схема (рис. 1):

Темпы прогресса электронной коммуникации в обществе приводят к необходимости исследования особенностей развития информационных технологий и их влияния на все жизненные сферы общества и человека. Предоставляя новые возможности, IT-инновации одновременно создают новые проблемы и риски. Информационная безопасность превращается в одну из глобальных проблем человечества, приобретающих психологический, экономический, социологический и политический характер, поскольку возрастает необходимость защиты человека и общества в информационной сфере. Проблема поддержки информационной безопасности носит междисциплинарный характер и требует совместных усилий специалистов различных научных направлений [2, 3].

Рис.1*. Информационное общество. Составлено автором*

1 Статья подготовлена по результатам исследований, выполненных за счёт бюджетных средств по государственному заданию Финансового университета на 2017 год.

2 Бердюгин Александр Александрович, аспирант кафедры «Информационная безопасность», Финансовый университет при Правительстве Российской Федерации, Москва. Россия. E-mail: a40546b@gmail.com

Таблица 1.

Число персональных компьютеров в организациях. Данные Росстата

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Число персональных компьютеров в обследованных организациях – всего, тыс. шт.	4150,5	4558,3	5709,6	6684	7528,4	8267,3	8743,7	9288,1	9972,2	10807,5	11438,0	11740,8	11992,3	12422,1
из них:														
имевшие доступ к глобальным информационным сетям	1204,0	1513,4	2032,0	2606,3	3267,5	3873,5	4313,5	4997,1	5663,2	6508,1	7220,8	8157,5	8362,0	8782,2
в том числе к сети «Интернет»	986,0	1218,8	1686,1	2232,0	2888,4	3411,5	3866,4	4553,3	5198,3	6066,5	6764,4	7277,6	7561,5	8117,9
Поступило персональных компьютеров в отчётном году, тыс. шт.	656,2	743,8	984,2	1170,9	1257,9	1159,2	890,6	999,9	1251,6	1454,1	1351,5	1177,7	952,2	986,7
Число персональных компьютеров на 100 работников – всего, шт.	18	20	23	26	29	32	35	36	39	43	44	47	49	49
в том числе с доступом к сети «Интернет»	4	5	7	9	11	13	15	18	21	24	26	29	31	32

Таблица 2.

Потери в финансовой системе России в 2016 году, млрд руб.

	Похищено	Сохранено	Всего	Эффективность хищений, %
Физ. лица	1,23	1,24	2,48	50
Юр. лица	0,38	1,12	1,51	26
АРМ КБР*	1,20	1,67	2,87	42
Итого:	2,82	4,04	6,86	41

*Автоматизированное рабочее место клиента Банка России

Согласно статистике, предоставленной Росстатом (табл. 1), за 13 лет произошёл прирост количества информационно-коммуникационных технологий (ИКТ) в организациях в $\frac{12422,1-4150,5}{4150,5} \approx 2$ раза, что подтверждает темпы прогресса. Интерес представляет процент количества персональных компьютеров, имевших доступ к сети «Интернет» в общем числе персональных компьютеров в обследованных организациях, возросший с $\frac{986,0}{4150,5} \cdot 100\% \approx 23,8\%$ в 2003 году до $\frac{8117,9}{12422,1} \cdot 100\% = 65,4\%$ в 2016 году.

По подсчётам[3] Банка России из финансовой системы России в 2016 году киберпреступниками было похищено почти 6,7 млрд руб. (табл. 2). Для сравнения: минимальный размер оплаты труда с 1 июля 2016 года составлял 7500 рублей в месяц. Таким образом $\frac{6,86 \cdot 10^9}{7,5 \cdot 10^3} \approx 915$ тысяч МРОТов. Кредитно-финансовым организациям понадобятся серьёзные технологии защиты от компьютерных атак и непосредственного физического взлома приспособлений. Однако защита информации – это не только прерогатива специалистов, но и задача пользователей дистанционного банковского обслуживания (ДБО).

Дистанционное взаимодействие всех систем и участников денежной банковско-финансовой системы – возможность цивилизации. Предоставление ссуд по сети «Интернет» и открытие депозитных счетов без визита в офис, интернет-трейдинг (онлайн-торговля), дистанционные объединённые счета (Omnibus Account), индивидуальные финансовые порталы и др. – не новинка, а необходимость сегодняшнего дня [4-8].

На рис. 2 перечислены основные причины, заставляющие человека нарушить систему защиты информации организации кредитно-финансовой сферы (ОКФС).

Единичные компьютерные нарушения хакеров-любителей уходят в прошлое. Настоящие кибернетические войны ведут организации и государства.

3 ЦБ готовит банки к компьютерным и информационным атакам. URL: http://www.vedomosti.ru/finance/articles/2016/12/07/668512-tsb-otrazheniyu-atak#/galleries/140737493044801/normal/1 (дата обращения 16 августа 2017 года).

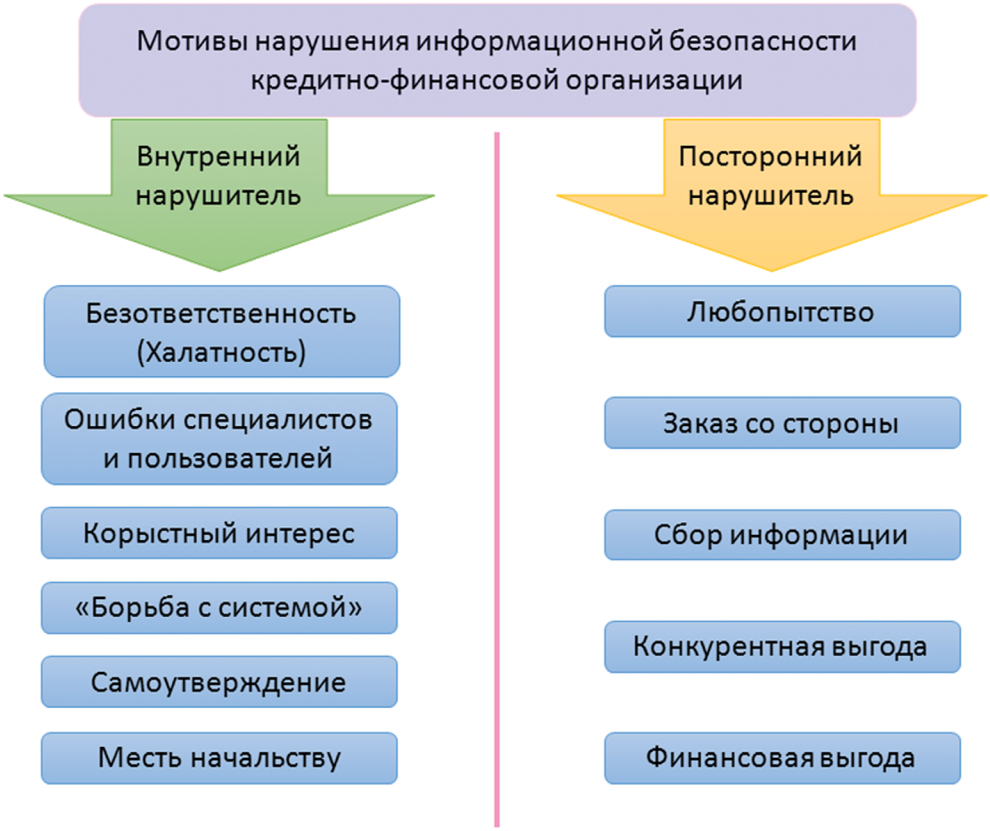

***Рис. 2**. Мотивы, движущие нарушителем информационной безопасности банка*

Информационные услуги и виды угроз системе защиты информации банка

Значение защищённости автоматизированной банковской системы (АБС) представляет собой функцию взаимодействия основных параметров защиты: доступности, целостности и конфиденциальности:

$$S_{защ} = F(S_{дст}, S_{цлс}, S_{кнф}) \quad (1)$$

Доступность информации показывает возможность реализации пользователями информации своих прав доступа. Целостность данных показывает их неизменность[4] при выполнении операций с ними, будь то передача, использование или хранение информации. Конфиденциальность информации представляет собой запрет на её разглашение неуполномоченным лицам без предварительного согласия сторон.

Информационная безопасность финансовых сведений влияет на стабильность ресурсов и качество предоставляемых услуг. В современном банковском бизнесе именно качество услуг – это один из основных факторов успеха. Низкое качество (в том числе по причине неудовлетворительного обеспечения информационной безопасности) является источником операционных, финансовых и репутационных рисков для банка (возможности потери доверия клиентов). Цифровое взаимодействие между пользователем банковскими услугами и финансовой организацией должно быть безопасным, комфортным и доступным по цене [4].

Проведём динамический анализ количества устройств [9], предназначенных для осуществления операций с использованием и без использования платёжных карт с 2010 по 2017 годы (табл. 3) по данным предоставленным Банком России[5].

Из отрицательной динамики количества импринтеров следует вывод: импринтеры уходят в прошлое. Ведь посредством импринтера невоз-

4 Примером целостности информации служат «швы» авторучкой на закрывающем клапане почтового конверта с письмом, свидетельствующие об отсутствии нежелательных вмешательств.

5 Статистика национальной платёжной системы. URL: https://www.cbr.ru/statistics/?PrtId=psrf (дата обращения 10 октября 2017 года).

Таблица 3.
Анализ динамики количества платёжных устройств в России. Рассчитано автором

Сведения об устройствах, расположенных в стране и предназначенных для осуществления операций с использованием и без использования платёжных карт				На 01.01.10 год, ед.	На 01.07.17 год, ед.	Прирост, %
Количество банкоматов и платёжных терминалов	Итого			155 161	203 684	31,27%
	банкоматов с функцией выдачи наличных денег	всего		92 481	125 813	36,04%
		из них	с функцией оплаты товаров и услуг	86 888	123 089	41,66%
	банкоматов и платёжных терминалов с функцией приёма наличных денег	всего		82 015	129 806	58,27%
		из них	платёжных терминалов	52 961	9 836	– 81,43%
			банкоматов	35 497	119 970	237,97%
Количество электронных терминалов	установленных в организациях торговли (услуг)			406 484	1 900 693	367,59%
	электронных терминалов удалённого доступа			9 379	17 177	83,14%
	в пунктах выдачи наличных			90 019	170 716	89,64%
Количество импринтеров	установленных в организациях торговли (услуг)			31 363	17 441	– 44,39%
	в пунктах выдачи наличных			4 387	1 003	– 77,14%

можно принимать к оплате электронные карты. Значительный рост количества электронных терминалов, установленных в организациях торговли (услуг) свидетельствует о развитии рыночной экономики. То же можно сказать о банкоматах с функцией приёма наличных денег. Хотя банкоматы – это не самый совершенный способ проведения транзакций, но это не только платёжный терминал, а ещё и сейф. Возможно, этим обусловлено снижение количества платёжных терминалов с функцией приёма наличных денег.

Аналогичные сведения об устройствах в территориальном разрезе не приводятся из соображений экономии места в статье. Тем не менее, на современном этапе почти все банки оказывают одинаковые услуги (проделывают одни и те же банковские операции) и отличать их может только качество предоставления услуг.

Банковская отрасль является одной из отраслей, наиболее уязвимых для инсайдерских инцидентов. Любой клиент кредитно-финансовых организаций внимательно относится к банковской тайне[6], и потому утечка информации может не просто серьёзно отразиться, а даже, без преувеличения, разрушить бизнес банка. Рис. 3 иллюстрирует рост количества внутренних утечек, не уступающий информационным нарушениям извне[7].

В 2015 году общая сумма вреда, причиной которого стали ошибочные и злонамеренные действия сотрудников, составила 450 млн рублей, в 2016 году показатель вырос почти вдвое и достиг 850 млн рублей (+89%). По итогам 2017 года ущерб, нанесённый банкам их сотрудниками, составит 900 млн рублей, прогнозирует Zecurion[8].

За десять лет прирост количества утечек составил $\frac{1556-198}{198} \cdot 100 \approx 686\%$. Согласно таблице 1, число персональных компьютеров $\frac{12422{,}1-6684}{6684} \cdot 100 \approx 86\%$ период возросло на . При этом в 2009-2011 годах рост инцидентов замедлился (с 2009 на 2011 год прирост $\frac{801-747}{747} \cdot 100 \approx 7{,}2\%$).

К наиболее распространённым типам внешних компьютерных атак, влекущие серьёзные угрозы для финансовых организаций, относятся: «Отказ в обслуживании» (Denial of Service, DoS-атака), «Распределённый отказ в обслуживании» (Distributed Denial of Service, DDoS-атака), «Логические бомбы», «Фишинг» (англ. phishing, от fishing – рыбная ловля, выуживание), «Метод фишинга», «Троян-

6 Банковская тайна – это юридический принцип в законодательствах некоторых стран, в соответствии с которым банки не имеют права предоставлять властям информацию о личных счетах своих клиентов при определённых условиях (например, в случае возбуждения уголовного дела).

7 Глобальное исследование утечек конфиденциальной информации в 2016 году. URL: https://www.infowatch.ru/analytics/reports/17479 (дата обращения 26 августа 2017 года).

8 Банки недосчитались 420 млн руб. из-за утечки данных. URL: http://www.vestifinance.ru/articles/88315 (дата обращения 23 сентября 2017 года).

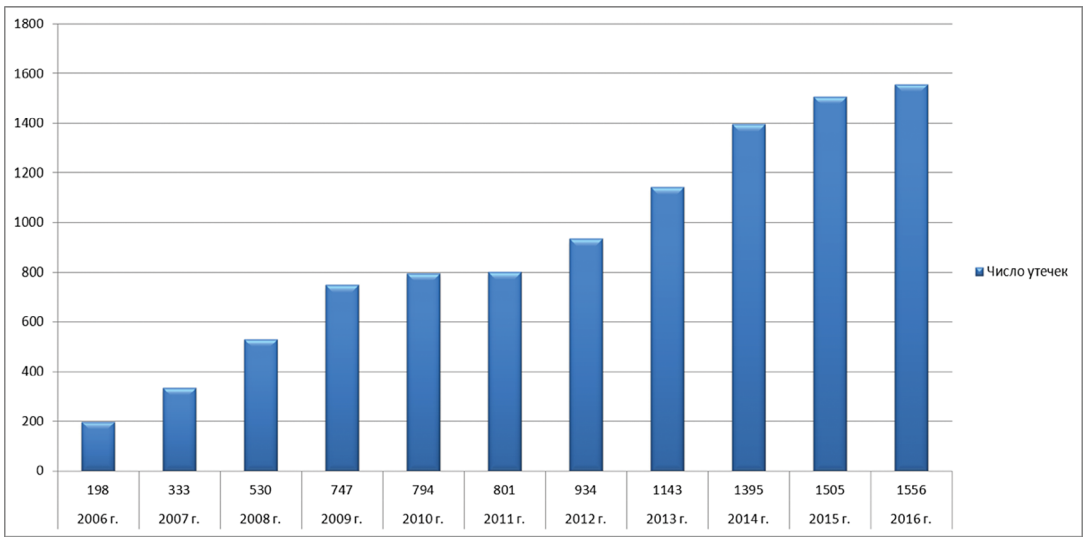

***Рис. 3**. Число зарегистрированных утечек информации в мире, 2006-2016 годы. Аналитический центр InfoWatch*

ские программы», «Вирусы», «Черви» и «Атака нулевого дня» (Zero Day attack).

Согласно подсчётам экспертов, в 2016 году критичным был каждый девятый инцидент. В 2017 году серьёзную опасность влечёт каждое шестое происшествие. Такая динамика связана с общим повышением активности массовых и целевых атак на организации.

В первом полугодии основными инструментами компьютерных преступников являлись атаки на web-приложения (34,2%), компрометация конфиденциальных данных клиентов сервисных предприятий (23,6%) и вредоносное программное обеспечение (19,2%)[9].

Пожалуй, в отдельную категорию можно отнести компьютерные нарушения, связанные с социальной инженерией. Социальная инженерия заключается в использовании социальных масок, лингвистических ухищрений и психологических трюков, позволяющих заставить компьютерных пользователей помогать хакерам в их незаконном вторжении или использовании компьютерных систем и сетей [10-15].

Самое уязвимое звено в АБС безопасности – это человек, которому свойственны недостатки, а воображение мошенника, специализирующегося на поиске слабостей человеческого фактора безгранично.

Примером социальной инженерии служит следующая уловка. Абоненту на баланс мобильного телефона переводят 200 рублей. После чего звонит бабушка и сообщает, что хотела положить деньги дочери, но ошиблась и просит перевести эти деньги назад. Может и «дочь» позвонить с номера, похожего на номер жертвы. Вскоре они вернут эти 200 рублей по квитанции об оплате через оператора. Поэтому возвращать самостоятельно не стоит.

Таким образом, социальная инженерия – это одно из самых сильных орудий в арсенале злоумышленников. Ведь гораздо проще обмануть кого-то в том, что он предоставляет свой пароль или деньги для положительного результата, чем тратить усилия на взлом информационной системы.

Управление риском нарушения информационной безопасности

Согласно Федеральному Закону ФЗ-184 «О техническом регулировании», понятие риска определяется как «вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учётом тяжести этого вреда».

Без высокой организации сервиса управления риском нарушения информационной безопасности (РНИБ) коммерческий банк понесёт не только финансовые, но и репутационные убытки. Именно клиенты банка определяют надёжность и устойчивость ресурсной базы финансовой организации [6].

Зачастую сотрудники служб безопасности банков рассчитывают на то, что комфорт и защита клиента не входит в задачи специалистов, безопасное управление информацией должно происходить на уровне Apple, Microsoft, Google, Facebook и PayPal (аутсорсинг). Методы информационной безопасности банков должны включать:

• брандмауэр для контроля и фильтрации проходящих через него сетевых пакетов;

9 WannaCry и Petya – массовые, но не самые опасные атаки. URL: http://www.banki.ru/news/lenta/?id=10034166 (дата обращения 01 октября 2017 года).

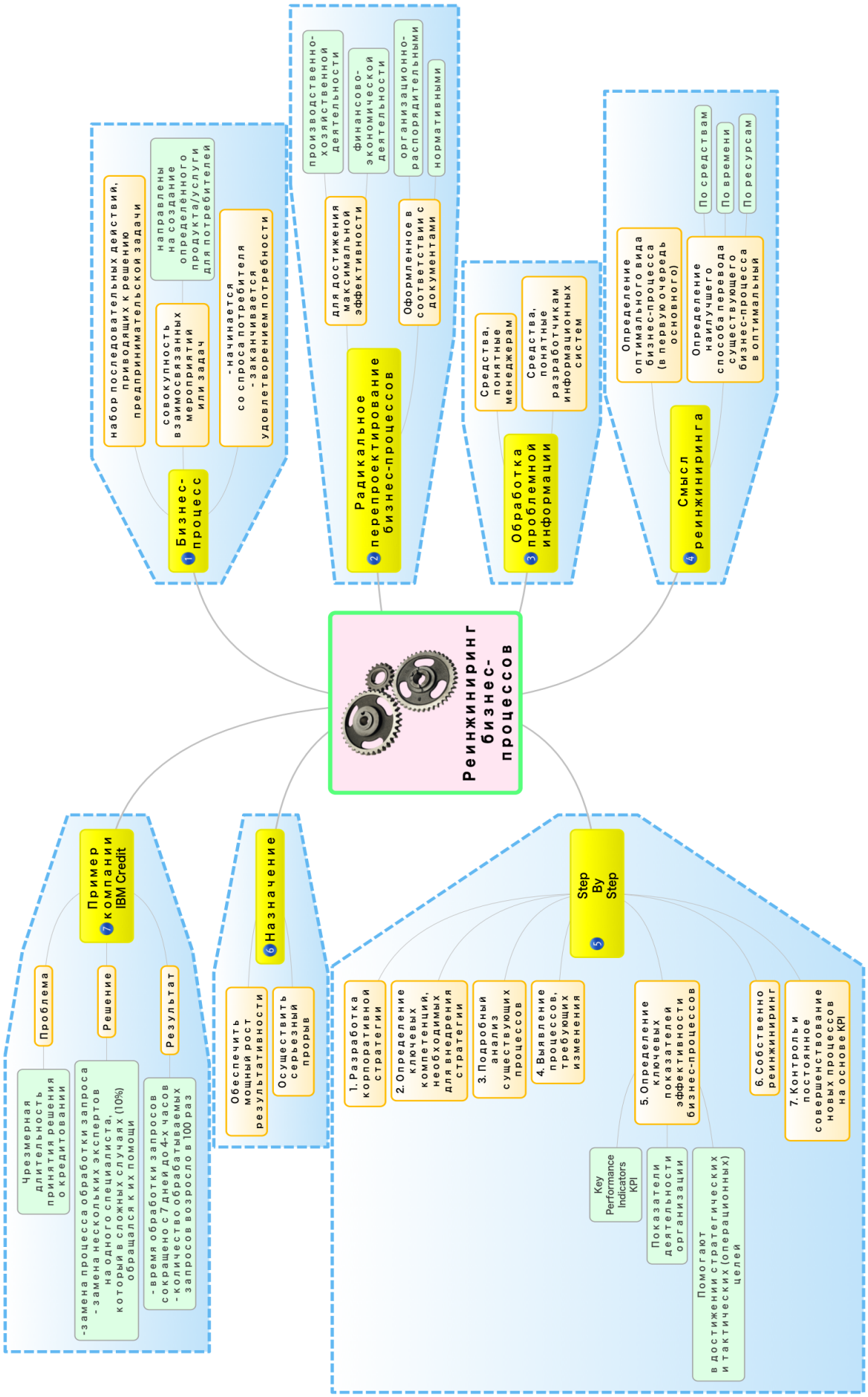

***Рис. 4**. Реинжиниринг бизнес-процессов (англ. Business process reengineering). Составлено автором*

Таблица 4.
Схема Квинтиллиана

Признак проблемы	Вопрос	1. Кто?	2. Что?	3. Когда?	4. Где?	5. Как?	6. Чем?	7. Зачем?
Субъект	1. Кто?		Кто – что?	Кто – когда?	Кто – где?	Кто – как?	Кто – чем?	Кто – зачем?
Объект	2. Что?			Что – когда?	Что – где?	Что – как?	Что – чем?	Что – зачем?
Время действия	3. Когда?				Когда – где?	Когда – как?	Когда – чем?	Когда – зачем?
Место действия	4. Где?					Где – как?	Где – чем?	Где – зачем?
Способ	5. Как?						Как – чем?	Как – зачем?
Средство	6. Чем?							Чем – зачем?
Цель	7. Зачем?							

• безопасную регистрацию и двухфакторную аутентификацию с возможностью определения местоположения;

• отслеживание и анализ бизнес-процессов в режиме реального времени [16].

Автор статьи, будучи финансистом по образованию, считает нужным уделить внимание реинжинирингу бизнес-процессов, результаты анализа которого представлены на рис. 4. В отличие от управления непрерывностью бизнеса, суть которого заключается в принятии и улучшении имеющихся процессов, реинжиниринг нацелен на перепроектирование существующих процессов в новые.

Рассматриваемые ситуации в книге [16] и подобных (например, «Bank 3.0» Бретта Кинга) – это, скорее, реинжиниринг, нежели автоматизация, вызванная научно-техническим прогрессом (НТП).

Применение клиентами банковских продуктов НТП замедляет три аспекта:

1. Отсутствие доверия у клиентов к технологиям ДБО;

2. Недостаточная финансовая и цифровая грамотность населения;

3. Низкое качество электронных банковских услуг [4].

Можно предположить, что 1 влияет на 2 и зависит от 3. В свою очередь 2 в целом влияет на развитие 3. Тогда как 2 и 3 становится причиной инцидентов.

В своё время древнеримский учёный Квинтиллиан придумал простую схему для описания любой проблемы. Эта схема включает в себя семь ключевых вопросов, а также их возможные сочетания (табл. 4).

Применив эту схему к процессу управления информационным риском проекта, можно получить следующие вопросы и ответы на них. Например, задав вопрос: «Кто является бенефициаром[10] проекта?», можно ответить так: «Кредиторы, заказчики, поставщики, инвесторы, предприятие в целом». Соответственно, данные бенефициары и будут являться субъектами, в чьих интересах мы управляем риском. Для каждого из них будут актуальны свои методы управления риском.

Если зададим вопрос: «Как управлять информационным риском?», то можно ответить так: «Мы можем уклониться от риска, можем его локализовать, распределить, компенсировать, поглотить».

Если зададим вопрос: «Кто и когда подвержен риску определённого типа?», то можно ответить: «Кредитор подвержен риску во время инвестиционной и частично эксплуатационной фаз, так как в течение данного периода для него существует риск невозврата кредита». В свою очередь, предприятие подвержено информационному риску в течение всех фаз реализации инвестиционного проекта, так как все риски проекта касаются благосостояния предприятия.

10 Бенефициар (от фр. benefice – прибыль, польза) – физическое или юридическое лицо, которое является владельцем всех или основной части акций компании, и получает все доходы от деятельности компании.

Таким образом, схема Квинтиллиана позволяет разделить проблему на части, выявить точку зрения, с которой мы смотрим на проблему или субъекта, интересы которого отстаиваем. В дальнейшем это позволит решить задачу гораздо легче [9].

Риск-менеджмент в банковской сфере обеспечивает эффективный подход к управлению безопасностью. Существующие подходы к управлению РНИБ сопряжены с определёнными сложностями, такими как сбор достоверной и очень подробной статистической информации в сфере информационной безопасности компании. Если взаимосвязи могут быть чётко идентифицированы и проанализированы, мы сможем разработать расширенные стратегии управления рисками и принимать более эффективные решения о планировании рисков.

Процесс управления РНИБ зарубежные авторы делят на три этапа [17]:

1. Оценка риска;
2. Минимизация риска;
3. Оценка эффективности.

В этих процессах нет универсального соответствия, но большинство подходов содержат распространённые элементы оценки и смягчения рисков.

Управление РНИБ и безопасностью – очень важные проблемы в банковской системе. Банковская система, включающая большое количество субъектов, подвержена различным опасностям и неопределённостям и представляет собой очень сложную структуру. В такой атмосфере очень сложно инициировать систему оценки и моделирования основных опасностей [18].

В нашей стране общая структура системы управления банковскими рисками включает четыре этапа:

1. Выявление (идентификация) риска;
2. Оценка и определение величины риска;
3. Мониторинг (контроль) изменения риска;
4. Осуществление минимизации риска.

Выявление того или иного РНИБ должно быть прописано во внутренних банковских документах [8].

В зависимости от допустимого предела риски делятся на допустимые, критические и катастрофические. Допустимый риск представляет собой средний уровень риска по отношению к другим хозяйственным субъектам и видам деятельности. Если $R_{ср}$ – средний уровень риска, а $R_{д}$ – его допустимый уровень, то имеет место неравенство $R_{д} < R_{ср}$.

Критический риск – это риск, уровень которого превышает средний уровень, но в пределах максимально допустимых значений риска R_{max}, принятых в определённой экономической системе для конкретных видов деятельности. То есть $R_{ср} < R_{кр} < R_{max}$.

Катастрофический риск превышает максимальный уровень риска R_{max}. Для этого риска свойственно соотношение $R_{кт} > R_{max}$ [7].

Соблюдением должного уровня банковской деятельности, а также контролем за РНИБ и управлением банковскими рисками должны заниматься:

- совет директоров банка;
- правление банка;
- президент банка;
- вице-президент банка;
- структурные подразделения банка (соответственно внутренним документам;
- служба внутреннего контроля.

Компетенции перечисленных органов управления определены уставом банка, его внутренними нормативными документами, а также положениями о подразделениях и должностными инструкциями для сотрудников кредитной организации.

Основной принцип системы управления РНИБ заключается в установлении процедур, обеспечивающих оценку риска, контроль и управление риском на том уровне, который соответствует масштабам банковской деятельности компании [8].

Рассмотрим проверку того, насколько хорошо банк выполняет положения внутренних нормативных актов, приведя перечень конкретных вопросов, на которые должен ответить аналитик-эксперт, чтобы получить информацию о качестве управления РНИБ в коммерческом банке:

- есть ли в банке подразделение (сотрудник), ответственное за оценку РНИБ?
- является ли данное подразделение (сотрудник) независимым от подразделений, осуществляющих банковские операции, сделки?
- разработаны ли в банке внутренние нормативные акты (положения, методики) по управлению РНИБ?
- утверждены ли акты по управлению РНИБ?
- разработаны ли в банке принципы управления РНИБ?
- определён ли во внутренних нормативных актах банка порядок проведения оценки РНИБ?
- осуществляется ли в банке страхование информационных технологий, информации и её носителей?
- способны ли меры, принятые банком, обеспечить сохранность и возможность восстановления информационных систем?

- способны ли меры, принимаемые банком, обеспечить физическую сохранность помещений?

- проводится ли в банке оценка РНИБ?

- ведётся ли в банке аналитическая база данных о понесённых убытках вследствие наступления РНИБ в разрезе направлений деятельности и ситуаций возникновения риска, позволяющая выявить наиболее уязвимые с точки зрения РНИБ области?

- составляется ли в банке внутренняя отчётность структурных подразделений для сбора сведений об убытках, нанесённых реализацией РНИБ?

- создана ли в банке система индикаторов уровня РНИБ, используемых при его мониторинге?

- прогнозируется ли в банке наиболее вероятная величина операционных убытков, понесённых компанией вследствие наступления РНИБ?

- составляется ли в банке управленческая отчётность о результатах мониторинга РНИБ?

- предусмотрен ли в банке порядок проведения самооценки управления РНИБ?

Результатом на выходе может стать некий агрегированный показатель, который складывается из отдельных составляющих. Каждому вопросу присваивается определённый балл по пятибалльной шкале, где 1 балл – «да» и 5 баллов – «нет».

Кроме того, каждый вопрос имеет свой вес, который аналитик определяет самостоятельно экспертным путём, предварительно согласовав свои действия с руководством банка. Агрегированный показатель качества системы управления РНИБ в банке рассчитывается по формуле

$$AGR = \sum(\text{Балл} \times \text{Вес}) / \sum \text{Весов} \qquad (2)$$

Чем ниже агрегированное значение показателя, тем выше уровень качества системы управления РНИБ в коммерческом банке и, наоборот, чем выше значение агрегированного показателя, тем данный уровень будет ниже [8]. Перечень приведённых вопросов не является последней инстанцией. Каждая кредитно-финансовая организация вправе разработать собственный образец анкеты.

Выводы

- соблюдение требований по защите информации организации имеет решающее значение для минимизации инцидентов информационной безопасности [19-23], поскольку мошенники постоянно используют различные методы и приёмы для компьютерных вторжений. К этим методам можно отнести как создание вредоносных программ и хищение закрытой информации со своего места работы, так и использование человеческого фактора для получения конфиденциальных данных;

- доверять собеседнику можно только в том случае, если абонент – активная сторона. Если абоненту позвонили по телефону, представились сотрудником банка и попросили назвать какой-нибудь номер или пароль, то он – пассивная сторона. Поэтому ничего, что хотят от абонента делать нельзя.

Если абоненту позвонили по телефону, предложили перезвонить по какому-то другому телефону и абонент звонит по этому телефону, то он опять пассивная сторона. В общем, если представились сотрудниками банка, перезвонить следует обязательно, но только по официальному номеру телефона, который есть на банковской карте или официальном сайте;

- информационная безопасность – это непрерывный процесс управления РНИБ. Можно сказать, что управление рисками – это в основном процесс принятия решений. Этап оценки риска – это набор информации, которая подлежит обработке. Стадия снижения риска – это фактическое принятие решений и внедрение результирующего подхода. Оценка эффективности – это постоянная обратная связь в процессе принятия решений;

- отечественный банковско-финансовый бизнес не столь развит, как западный, что является причиной невозможности применения зарубежных методов, рецептов и способов в условиях нашей страны. Система подготовки специалистов ОКФС в области ДБО отстаёт от мировых стандартов. Методическое и технологическое обеспечение регулирующих и надзорных подразделений для более эффективного выполнения функций в системах ДБО не отвечает современным требованиям. Накопленный опыт правоохранительных и законодательных органов по борьбе, раскрытию и предупреждению компьютерных преступлений оставляет желать лучшего. Поведение клиентов (доверие к результатам НТП – продуктам ДБО, финансовая и цифровая грамотность) слабо адаптированы к эволюции в цифровом мире.

***Рецензент**: Ревенков Павел Владимирович, доктор экономических наук, профессор кафедры «Информационная безопасность», Финансовый университет при Правительстве РФ, Москва, Российская Федерация. E-mail: pavel.revenkov@mail.ru*

Литература:

1. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014. 848 с.
2. B.I. Skorodumov, O.B. Skorodumova, L.F. Matronina. Research of Human Factors in Information Security // Modern Applied Science. Vol. 9, No. 5, 2015, pp. 287–294.
3. Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3-7. DOI: 10.21681/2311-3456-2016-5-3-7.
4. Поспелов А.Л., Ревенков П.В. Что сдерживает использование дистанционных каналов обслуживания? // Расчеты и операционная работа в коммерческом банке. 2015. № 1 (125). С. 70–75.
5. Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. Т. 13, № 9 (354). С. 1747–1760. DOI: 10.24891/ni.13.9.1747.
6. C. Skinner. Digital bank: Strategies to Launch or Become a Digital Bank. Singapore, Marshall Cavendish International (Asia), 2014, 300 p.
7. K. Subrahmanyam, M. Haritha, V. Tejaswini, Ch. Balaram, C. Dheeraj. Information Security and Risk Management for Banking System. International Journal of Computer Trends and Technology (IJCTT), 2014, Vol. 10, No. 3, pp. 171–176.
8. S. Bauer, E.W.N. Bernroider, K. Chudzikowski. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks // Computers & Security, Volume 68, July 2017, Pages 145–159.
9. Жарковская Е.П. Финансовый анализ деятельности коммерческого банка: учебник. М.: Издательство «Омега-Л», 2015. 378 с.
10. F. Mouton, L. Leenen, H.S. Venter. Social engineering attack examples, templates and scenarios. Computers & Security, 2016, vol. 59, pp. 186-209. DOI: https://doi.org/10.1016/j.cose.2016.03.004.
11. K. Krombholz, H. Hobel, M. Huber, E. Weippl. Advanced social engineering attacks. Journal of Information Security and Applications, 2015, vol. 22, pp. 113-122. DOI: https://doi.org/10.1016/j.jisa.2014.09.005.
12. M. Edwards, R. Larson, B. Green, A. Rashid, A. Baron. Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security, 2017, vol. 69, pp. 18-34. DOI: https://doi.org/10.1016/j.cose.2016.12.013.
13. S. Rathore, P.K. Sharma, V. Loia, Y.-S. Jeong, J.H. Park. Social network security: Issues, challenges, threats, and solutions. Information Sciences, Volume 421, December 2017, Pp. 43-69.DOI: https://doi.org/10.1016/j.ins.2017.08.063.
14. Бердюгин А.А. Обеспечение информационной безопасности дистанционного банковского обслуживания // Безопасные информационные технологии (БИТ-2016): Сборник трудов Седьмой Всероссийской научно-технической конференции под редакцией В.А. Матвеева. 2016. С. 58-61.
15. Travis J. Wiltshire, Samantha F. Warta, Daniel Barber, Stephen M. Fiore. Enabling robotic social intelligence by engineering human social-cognitive mechanisms. Cognitive Systems Research, Volume 43, June 2017, pp. 190-207. DOI: https://doi.org/10.1016/j.cogsys.2016.09.005.
16. Исмагилов Р.Х. Риск-менеджмент : конспект лекций. Ростов н/Д.: Феникс, 2015. 198 с.
17. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
18. Волков А.А. Управление рисками в коммерческом банке: практическое руководство. М.: Издательство «Омега-Л», 2015. 156 с.
19. C. Hadnagy, P. Wilson. Social Engineering: The Art of Human Hacking. Indianapolis, Wiley Publishing, Inc., 2011, 416 p.
20. David Tayouri. The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. Procedia Manufacturing. Volume 3, 2015, Pages 1096-1100. DOI: 10.1016/j.promfg.2015.07.181.
21. H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon. Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & Security, Volume 65, March 2017, Pages 14-28. DOI: 10.1016/j.cose.2016.09.009.
22. Joseph M. Hatfield. Social engineering in cybersecurity: The evolution of a concept. Computers & Security, Volume 73, March 2018, Pages 102-113. 10.1016/j.cose.2017.10.008.
23. N. S. Safa, R. von Solms, L. Futcher. Human aspects of information security in organisations. Computer Fraud & Security, 2016, vol. 2016, no. 2, pp. 15-18. DOI: 10.1016/S1361-3723(16)30017-3.

RISK MANAGEMENT OF INFORMATION SECURITY VIOLATION IN CONDITIONS OF ELECTRONIC BANKING[11]

***Berdyugin A.*[12]**

Abstract: *Banking business is developing in conditions that are uncertain. Financial organizations must build an integrated management system for all identified banking risks. The article deals with development and formalization of risk management subsystem of information security violation within overall risk manage–*

11 The article follows results of researches financed as part of the State Job of the Financial University under the Government of the Russian Federation in 2017.

12 Alexander Berdyugin, post-graduate student of Department «Information Security», Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: a40546b@gmail.com

ment system of credit and financial institution. The definition of information society is given. Calculations are given about statistics of Russian Statistics Committee and the Central Bank of Russia. It is dealt with motives, that driving by the violator of information security of commercial bank. Dynamic analysis of the number of devices intended for operations with and without the use of payment cards located in Russia is carried out.

It is examined types of threats for information protection system of commercial bank, including insider incidents, external cyberattacks and social engineering techniques. Paper draws our attention to the implementation of Business Process Reengineering in banking information security. Taking into account modern conditions of risk occurrence, scheme of the ancient Roman scientist Quintillian, that is intended for describe any problem is analyzed. Enumeration of issues providing information about the quality of information security risk management in a commercial bank is given. Appropriate conclusions are drawn about optimization the quality of risk management of information protection in banks.

Keywords: *risk management, financial organization, information security, remote banking services, computer incidents.*

References:

1. Rogovskij E.A. Kiber-Vashington: global'nye ambicii. M.: Mezhdunarodnye otnosheniya, 2014. 848 s.
2. B.I. Skorodumov, O.B. Skorodumova, L.F. Matronina. Research of Human Factors in Information Security, Modern Applied Science. Vol. 9, No. 5, 2015, pp. 287–294.
3. SHeremet I.A. Napravleniya podgotovki specialistov po protivodejstviyu kiberugrozam v kreditno-finansovoj sfere, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2016, No 5 (18). S. 3-7. DOI: 10.21681/2311-3456-2016-5-3-7.
4. Pospelov A.L., Revenkov P.V. CHto sderzhivaet ispol'zovanie distancionnyh kanalov obsluzhivaniya?, Raschety i operacionnaya rabota v kommercheskom banke. 2015, No 1 (125). S. 70–75.
5. Revenkov P.V., Berdyugin A.A. Social'naya inzheneriya kak istochnik riskov v usloviyah distancionnogo bankovskogo obsluzhivaniya, Nacional'nye interesy: prioritety i bezopasnost'. T. 13, No 9 (354). S. 1747–1760. DOI: 10.24891/ni.13.9.1747.
6. C. Skinner. Digital bank: Strategies to Launch or Become a Digital Bank. Singapore, Marshall Cavendish International (Asia), 2014, 300 p.
7. K. Subrahmanyam, M. Haritha, V. Tejaswini, Ch. Balaram, C. Dheeraj. Information Security and Risk Management for Banking System. International Journal of Computer Trends and Technology (IJCTT), 2014, Vol. 10, No. 3, pp. 171–176.
8. S. Bauer, E.W.N. Bernroider, K. Chudzikowski. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, Computers & Security, Volume 68, July 2017, Pages 145–159.
9. ZHarkovskaya E.P. Finansovyj analiz deyatel'nosti kommercheskogo banka: uchebnik. M.: Izdatel'stvo «Omega-L», 2015. 378 s.
10. F. Mouton, L. Leenen, H.S. Venter. Social engineering attack examples, templates and scenarios. Computers & Security, 2016, vol. 59, pp. 186-209. DOI: https://doi.org/10.1016/j.cose.2016.03.004.
11. K. Krombholz, H. Hobel, M. Huber, E. Weippl. Advanced social engineering attacks. Journal of Information Security and Applications, 2015, vol. 22, pp. 113-122. DOI: https://doi.org/10.1016/j.jisa.2014.09.005.
12. M. Edwards, R. Larson, B. Green, A. Rashid, A. Baron. Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security, 2017, vol. 69, pp. 18-34. DOI: https://doi.org/10.1016/j.cose.2016.12.013.
13. S. Rathore, P.K. Sharma, V. Loia, Y.-S. Jeong, J.H. Park. Social network security: Issues, challenges, threats, and solutions. Information Sciences, Volume 421, December 2017, Pp. 43-69.DOI: https://doi.org/10.1016/j.ins.2017.08.063.
14. Berdyugin A.A. Obespecheniye informatsionnoy bezopasnosti distantsionnogo bankovskogo obsluzhivaniya // Bezopasnyye informatsionnyye tekhnologii (BIT-2016): Sbornik trudov Sed'moy Vserossiyskoy nauchno-tekhnicheskoy konferentsii pod redaktsiyey V.A. Matveyeva. 2016. S. 58-61.
15. Travis J. Wiltshire, Samantha F. Warta, Daniel Barber, Stephen M. Fiore. Enabling robotic social intelligence by engineering human social-cognitive mechanisms. Cognitive Systems Research, Volume 43, June 2017, pp. 190-207. DOI: https://doi.org/10.1016/j.cogsys.2016.09.005.
16. Ismagilov R.H. Risk-menedzhment : konspekt lekcij. Rostov n/D.: Feniks, 2015. 198 s.
17. Barabanov A.V., Dorofeev A.V., Markov A.S., Cirlov V.L. Sem' bezopasnyh informacionnyh tekhnologij/Pod. red. A.S.Markova. M.: DMK Press, 2017. 224 s.
18. Volkov A.A. Upravlenie riskami v kommercheskom banke: prakticheskoe rukovodstvo. M.: Izdatel'stvo «Omega-L», 2015. 156 s.
19. C. Hadnagy, P. Wilson. Social Engineering: The Art of Human Hacking. Indianapolis, Wiley Publishing, Inc., 2011, 416 p.
20. David Tayouri. The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. Procedia Manufacturing. Volume 3, 2015, Pages 1096-1100. DOI: 10.1016/j.promfg.2015.07.181.
21. H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon. Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & Security, Volume 65, March 2017, Pages 14-28. DOI: 10.1016/j.cose.2016.09.009.
22. Joseph M. Hatfield. Social engineering in cybersecurity: The evolution of a concept. Computers & Security, Volume 73, March 2018, Pages 102-113. 10.1016/j.cose.2017.10.008.
23. N. S. Safa, R. von Solms, L. Futcher. Human aspects of information security in organisations. Computer Fraud & Security, 2016, vol. 2016, no. 2, pp. 15-18. DOI: 10.1016/S1361-3723(16)30017-3.