МИНИСТЕРСТВО НАУКИ и высшего ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Экономический факультет**

**Кафедра мировой экономики и менеджмента**

Допустить к защите

Заведующий кафедрой

д-р экон. наук, профессор

\_\_\_\_\_\_\_\_\_\_\_\_И.В. Шевченко

(подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г.

Руководитель ООП

д-р экон. наук, профессор

\_\_\_\_\_\_\_\_\_\_\_\_И.В. Шевченко

(подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**(МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)**

**КИБЕРБЕЗОПАСНОСТЬ КАК ФАКТОР ПОВЫШЕНИЯ УСТОЙЧИВОСТИ РАЗВИТИЯ РОССИЙСКИХ КОММЕРЧЕСКИХ БАНКОВ**

Работу выполнила\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_М. В. Мартиросян

(подпись, дата)

Направление подготовки 38.04.01 Экономика

Направленность (профиль) Финансовая экономика

Научный руководитель

д-р экон. наук, проф.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С. Н. Третьякова

(подпись)

Нормоконтролер

преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. Б. Катрюхина

(подпись)

Краснодар

2022

**СОДЕРЖАНИЕ**

Введение 3

1. Теоретические и методические основы оценки устойчивости коммерческих банков 8
   1. Экономическая сущность обеспечения устойчивости коммерческих банков 8
   2. Кибербезопасность как ключевой фактор обеспечения устойчивости коммерческих банков 15
   3. Современные подходы к обеспечению кибербезопасности коммерческих банков 23
2. Исследование устойчивости развития российских коммерческих банков на современном этапе 32
   1. Оценка показателей устойчивости развития российской банковской системы 32
   2. Анализ существующих моделей оценки рисков кибербезопасности, обеспечивающих устойчивость российских коммерческих банков 39
   3. Выявление проблем и перспектив развития устойчивости российских коммерческих банков на примере ПАО «Сбербанк России» 45
3. Разработка инструментария управления рисками кибербезопасности российских коммерческих банков 54
   1. Разработка методического подхода к анализу и оценке рисков кибербезопасности 54
   2. Рекомендации по совершенствованию инструментов страхования киберрисков на примере ПАО «Сбербанк» 61

Заключение 69

Список использованных источников 74

**ВВЕДЕНИЕ**

*Актуальность исследования*. После глобальных изменений конъюнктуры рынка, вызванных событиями 2020 и 2022 гг., возросла конкуренция на рынке банковских услуг, а для российских коммерческих банков стала актуальной задача управления рисками и устойчивостью, от эффективного решения которой напрямую зависит рентабельность самих банков. Обеспечение устойчивости коммерческих банков имеет ключевое значение как на стадии кризиса, так и на стадии посткризисного экономического подъема, поскольку банковский сектор является элементом критической инфраструктуры, от которого зависит экономический рост страны.

Кроме того, цифровая трансформация этой отрасли наряду с ростом пользователей мобильных приложений, интернет-банкингом и другими онлайн-сервисами сделала её уязвимой для будущих кибератак. Хотя цифровые банковские решения обеспечивают легкий доступ к финансовым услугам для клиентов, они также создают бреши в кибербезопасности, которыми могут воспользоваться киберпреступники. Киберпреступления растут в периоды экономической нестабильности, становятся сложнее и мощнее, что порождает новые операционные и репутационные риски. Реализация киберугроз напрямую сказывается на финансовом результате банка, поскольку может приводить к значительным расходам на восстановление деятельности и устранение последствий кибератак.

По мере того, как все большее количество банков внедряют инновационные решения для развития цифрового банкинга, наличие эффективной системы кибербезопасности становится важнее, чем когда-либо прежде. Данная проблема также обостряется сложностью в анализе и оценке кибербезопасности, ведь ввиду своей новизны она является слабо изученной.

*Степень изученности проблемы.* Вопросы исследования теоретико-методологических аспектов и принципов устойчивости коммерческих банков и особенностей развития кибербезопасности нашли свое отражение в работах российских экономистов, таких как: Алпеев А. С., Андреева Л. Ю., Вигриянова Ю. С., Гавриченко Н. В., Дерюгин Р. А., Ильясов С. М., Кумышева М. К., Маслаченков Ю. С., Белых Л. П. и др.

*Целью данного исследования* является разработка теоретико-методологических положений и практических рекомендаций, направленных на повышение устойчивости российских коммерческих банков посредством развития кибербезопасности.

Достижение поставленной цели осуществимо с выполнением *следующих задач:*

1. раскрыть экономическую сущность обеспечения устойчивости коммерческих банков;
2. определить кибербезопасность как ключевой фактор обеспечения устойчивости коммерческих банков;
3. изучить современные подходы к обеспечению кибербезопасности коммерческих банков;
4. оценить показатели устойчивости развития российской банковской системы;
5. проанализировать существующие модели оценки рисков кибербезопасности, обеспечивающие устойчивость российских коммерческих банков;
6. выявить проблемы и перспективы развития устойчивости российских коммерческих банков на примере ПАО «Сбербанк России»;
7. разработать методический подход к анализу и оценке рисков кибербезопасности;
8. составить рекомендации по совершенствованию инструментов страхования киберрисков на примере ПАО «Сбербанк».

*Объектом исследования* выступает устойчивость российских коммерческих банков, активно принимающих участие в развитии своей кибербезопасности. *Предметом исследования* являются экономические отношения, возникающие в процессе обеспечения устойчивости российских коммерческих банков.

*Гипотеза исследования* базируется на предположении автора, что применение финансовых инструментов и следование тенденциям в банковском секторе в области кибербезопасности является эффективным средством развития устойчивости и минимизирует риски российских коммерческих банков.

В ходе написания диссертационной работы были использованы такие *методы* научного познания, как анализ, синтез, сравнение и формализация.

*Теоретической и методической основой исследования* послужили труды зарубежных и отечественных специалистов в области банковской устойчивости, риск-менеджмента и кибербезопасности. Эмпирическую основу исследования составили данные аналитических организаций, статистические данные, а также информация сети Интернет, затрагивающие различные аспекты исследуемой проблематики. Исследования, опубликованные на сайте Центрального банка Российской Федерации, являются основным источником, используемым в данной работе.

*Теоретическая значимость исследования* заключается в определении роли кибербезопасности как фактора повышения устойчивости развития российских коммерческих банков.

*Практическая значимость исследования* заключается в возможности применения описанных в данной работе предложений и рекомендаций в процессе разработки системы кибербезопасности российских коммерческих банков.

*Научная новизна* магистерской работы заключается в разработке методических и практических рекомендаций, которые позволяют комплексно подойти к совершенствованию кибербезопасности российских коммерческих банков, что повысит их устойчивость. А именно:

* дополнена классификация Ю. С. Маслаченко и А. Ю. Петрова устойчивости коммерческого банка новым видом «информационная устойчивость», под которым подразумевается способность коммерческого банка защищать свое информационное пространство. Это дополнение позволит сделать подход к дальнейшим исследованиям устойчивости банков более комплексным и полноценным;
* дополнен термин обеспечения кибербезопасности, который предлагается трактовать следующим образом. Обеспечение кибербезопасности – это комплекс действий стратегического характера, направленный на защиту критически важных систем и их пользователей от угроз, совершаемых в киберпространстве, с целью предотвратить экономический, технический и информационный ущерб. В предложенном нами определении акцентируется внимание на следующих аспектах: 1) кибербезопасность защищает не только систему, но и её пользователей; 2) защита активов происходит в киберпространстве; 3) киберугроза ставит под риск не только информационную безопасность, но и финансовую. Предложенный нами термин позволяет глубже понять проблематику и сделать способы управления кибербезопасностью эффективнее;
* разработан методический подход к анализу и оценке рисков кибербезопасности, который включает следующие направления: 1) направления анализа киберугроз; 2) формирование сценариев экстремальных ситуаций (вызванных реализацией киберугроз); 3) направления оценки рисков нарушения кибербезопасности. Предложенный методический подход позволит коммерческим банка разрабатывать собственные экономико-математические модели анализа и оценки киберрисков, соответствующие потребностям отдельного банка, что сделает управление киберрисками эффективнее;
* предложены и апробированы на примере ПАО «Сбербанк» рекомендации по совершенствованию инструментария страхования киберрисков. Сбербанку на основе анализа рекомендовано комплексное страхование рисков кибербезопасности в российской страховой компании АО «Согаз» или АО «АльфаСтрахование» с возможностью перестрахования рисков в ведущих зарубежных страховых компаниях, что позволит минимизировать негативные последствия от кибератак и компенсировать убытки.

*Апробация результатов исследования.* Ключевые положения магистерского исследования изложены в двух статьях, которые были опубликованы в рецензируемом научном журнале по экономической тематике, включенных в ядро РИНЦ.

Выпускная квалификационная работа состоит из введения, основной части, заключения и списка использованных источников. Основная часть состоит их трех глав: первая включает в себя теоретический обзор устойчивости коммерческих банков, который раскрывает тему ВКР на научном уровне. Вторая глава представляет собой аналитическую часть, где оценивается текущее состояние объекта исследования на макроуровне. Третья глава – проектная часть работы, где даются рекомендации на основе проведенного анализа, и где подтверждается экономическая целесообразность развития системы кибербезопасности на основе применения финансовых инструментов.

**1 Теоретические и методические основы оценки устойчивости коммерческих банков**

## Экономическая сущность обеспечения устойчивости коммерческих банков

Банковские кризисы, которые произошли как в странах с переходной экономикой, так и в развивающихся странах за последние 20 лет, укрепили убежденность в важности стабильной и хорошо регулируемой банковской системы. Поэтому всё большее значение для России в настоящее время приобретают вопросы поддержания устойчивости банковской системы в целом и её элементов – банков.

Сам термин «устойчивость» имеет множество определений и интерпретаций. Наиболее часто используемое взято из словаря русского языка и определяется как «способный сохранить состояние равновесия при внешних воздействиях» [33].

После изучения отечественного и зарубежного опыта можно утверждать, что как такового определения устойчивости коммерческого банка нигде не представлено. Как правило, используется термин «финансовая устойчивость». То есть чаще всего в работах экономистов между терминами «устойчивость» и «финансовая устойчивость» нет разграничений – рассмотрение устойчивости кредитной организации сводится к его финансовой устойчивости.

В консультативном документе Базельского комитета по банковскому надзору, посвященному вопросам повышения устойчивости банковского сектора, используется термин «устойчивость банковского сектора». Под устойчивостью в нём понимается «способность банковского сектора выдерживать потрясения, возникающие в результате финансового и экономического стресса, независимо от его источников» [5].

Более широкое определение устойчивости коммерческого банка с позиции «общеэкономического содержания» дают Ю. С. Маслаченков и А. Ю. Петров и оно включает несколько типов такой устойчивости (табл. 1.1).

Таблица 1.1 – Типы устойчивости коммерческих банков [29, 41]

|  |  |
| --- | --- |
| Тип устойчивости | Пояснение |
| Финансовая | объем и структура собственных средств, уровень доходов и прибыли, норма прибыли на собственный капитал, достаточность ликвидности |
| Организационно-структурная | организационно-технологическая дифференциация отдельных видов деятельности на основе функционально-технологической документации |
| Функциональная | 1) специализация банка на определенном перечне услуг (устойчивость заключается в более эффективном управлении ограниченным ассортиментом продуктов)  2) универсализация банка (устойчивость заключается в возможности удовлетворить весь набор потребностей клиентов в банковских продуктах в одном банке) |
| Капитальная | определяется размером собственного капитала банка |
| Коммерческая или рыночная | мера встроенности банка в инфраструктуру рыночных отношений (степень и прочность связей с государством, участие в межбанковских отношениях, длительность и качество отношений с кредиторами, клиентами и вкладчиками, социальная значимость банка) |

О. И. Лаврушин в учебном пособии «Деньги, кредит, банки» определяет устойчивость банка как «его динамичное состояние, которое обеспечивает необходимую степень защиты от неблагоприятного воздействия внешних и внутренних факторов». Подобно Ю. С. Маслаченко он классифицировал устойчивость по структуре как финансовую, организационную, кадровую, операционную и коммерческую устойчивость [28].

Рассмотрев различные авторские трактовки термина «устойчивость коммерческого банка», можно сделать ряд значимых выводом. Во-первых, многие авторы считают, что устойчивость банка определяется финансовыми результатами его деятельности. То есть исключительное внимание уделяется финансовой устойчивости, как главному критерию обеспечения непрерывной деятельности коммерческого банка. Безусловно, данный вид устойчивости значим для банка как для коммерческой организации, ведь её потеряла ведет к ослаблению других видов устойчивости. Однако, финансовая устойчивость – не единственное условие устойчивости банка. Во-вторых, классификации устойчивости коммерческих банков у различных авторов не содержат на наш взгляд одной из наиболее актуальных её видов – информационной устойчивости, что позволяет нам сделать вывод о том, что имеющиеся классификации в учебных пособиях устарели.

Правильное определение термина «устойчивость коммерческого банка» имеет важное значение на макроэкономическом уровне. Это связано с тем, что коммерческие банки в большей степени, чем другие экономические институты имеют социальную природу. Банк – это базовый кредитный институт, который выполняет посредническую функцию в проведении расчетов между экономическими субъектами (населения, финансовых учреждений, предприятий различных отраслей и организационно-правовых форм собственности). Кроме того, законодательно закреплена обязанность банков обеспечивать сохранность денежных средств населения. Это придает банкам статус не просто коммерческой организации, но гаранта социальной стабильности общества. В связи с этим негативный эффект от потери устойчивости у коммерческих банков для общества будет больше, чем у других экономических субъектов [30].

Вместе с тем всё более приоритетным для коммерческих банков, общества и экономики направлением становится цифровизация, которая также оказывает существенное воздействие на устойчивость их функционирования. Конкурентное, социальное и институциональное давление подталкивает коммерческие банки к участию в цифровой трансформации.

С развитием инновационных технологий меняются и бизнес-процессы. Появляются инновационные решения, которые позволяют оптимизировать многие финансовые услуги: сделать их проще, доступнее и дешевле. Цифровая трансформация способствует привлечению новых клиентов и генерации прибыли. Из-за глобализации и жесткой конкуренции крупные банки со всего мира начали переходить на новую бизнес-модель – модель цифрового банкинга, которая позволяет клиентам выполнять операции через удаленные каналы доступа [50].

Тем не менее, не стоит недооценивать проблемы, с которыми сталкиваются многие банки при переходе на инновационные финансовые технологии. Решение интернет-банков вести большую часть своего бизнеса в Интернете, помимо демонстрации своих сильных сторон, порождает потенциальные трудности.

Угрозы нефинансовых рисков в дистанционных банковских услугах стоят гораздо острее, чем в традиционных. Источниками угроз являются программное обеспечение и человеческий фактор. Более того, быстрое развитие цифровизации фактически требует актуализации законодательства, регулирующего онлайн-транзакции, поскольку в случае финансовых потерь в ущерб клиентам или в других конкретных ситуациях не существует компенсационных мер. Таким образом, в настоящее время одной из важнейших задач банковского сектора становится обеспечение её информационной устойчивости.

Принимая во внимание вышеизложенное, считаем необходимым актуализировать существующую классификацию устойчивости коммерческого банка по структуре и представить её следующим образом (таб. 1.2).

Информационная устойчивость является важным, но относительно новым явлением, хотя коммерческие банки уже давно находятся в авангарде применения финансовых технологий.

Таблица 1.2 – Классификация устойчивости по структуре (составлено автором)

|  |  |
| --- | --- |
| Тип устойчивости | Пояснение |
| Финансовая | устойчивость финансовой системы к потрясениям, ее бесперебойная и эффективная работа |
| Организационно-структурная | менеджмент банка не противоречит целям и задачам её деятельности и определенному ассортименту банковских продуктов и услуг, посредством реализации которых банк обеспечивает достижение своей стратегии |
| Функциональная | 1) специализация банка на определенном перечне услуг,  2) универсализация банка |
| Капитальная | определяется размером собственного капитала банка |
| Коммерческая или рыночная | мера встроенности банка в инфраструктуру рыночных отношений |
| Информационная | способность коммерческого банка защищать свое информационное пространство |

Несмотря на различные преимущества, связанные с внедрением информационных технологий, очевидны и угрозы, возникающие в связи с этими новыми решениями. Поскольку коммерческие банки осуществляют бизнес-операции в условиях цифровизации и интернет-банкинга, они более уязвимы к кибератакам, чем другие финансовые учреждения. Сложность также заключается в том, что, когда киберпреступление происходит в рамках финтеха, его трудно идентифицировать из-за отсутствия контролирующего органа. И трудно оценить экономический ущерб, поскольку кибератаки по-разному влияют на деятельность финансовых учреждений.

Вместе с тем, первостепенное значение в обеспечении устойчивости развития коммерческих банков имеют операционные риски. Цель коммерческих банков, которая заключается в получении прибыли, всегда ограничивается размером убытков, которые они могут принять. Ключевой риск, влияющий на устойчивость развития коммерческих банком, заключается в том, что убытки от деятельности окажутся выше запланированной прибыли [50]. Следовательно, влияние операционных рисков на прибыль и убытки банка является основным показателем эффективности его деятельности. Величину, требуемую для покрытия убытков коммерческого банка от операционной деятельности, определяет его капитал.

Таким образом, в целях обеспечения устойчивости развития для коммерческих банков является актуальной задача менеджмента рисков, в том числе рисков кибербезопасности. Совершенствование менеджмента рисков влияет как на финансовое состоянии банка, так и устойчивость его развития в целом, поскольку приведет к уменьшению резерва капитала на убытки и увеличению прибыли. В условиях цифровизации и соблюдения требований мегарегулятора полноценный менеджмент операционных рисков, в которым относятся и риски кибербезопасности, является ключевым условием обеспечения устойчивости коммерческих банков.

В 2016 году Управление финансовых исследований Министерства финансов США написало в своем отчете о финансовой стабильности Конгрессу, что уязвимость «инцидентов кибербезопасности, затрагивающих финансовые компании» создает определенные риски для заражения, а также для финансирования и ликвидности [73]. В этом отчете и связанном с ним исследовательском документе выделяется три «канала», по которым эти риски могут передаваться, что может привести к системным кризисам:

1. отсутствие (финансовой) взаимозаменяемости: финансовая система зависит от нескольких ключевых центров, как правило, определенных фирм или коммунальных предприятий (например, электронных торговых систем, бирж или клиринговых палат), которые выполняют жизненно важную функцию для всей отрасли. Примеры этих функций включают хранение ценных бумаг, управление обеспечением, согласование и подтверждение сделок, все из которых являются технологически емкими автоматизированными процессами. Короче говоря, «индустрия финансовых услуг полагается на надежную инфраструктуру информационных и коммуникационных технологий (ИКТ) для выполнения транзакций или перемещения платежей». Было бы мало простых обходных путей замены, если бы инцидент затронул эти учреждения или системы;
2. потеря доверия: в документе отмечается, что атаки обычно поражают потребительские сети, не оказывая системного воздействия, но также и то, что более масштабная кража может вызвать более масштабную потерю доверия. К ряду атак относят: взломы банкоматов, уничтожение одного или нескольких особо надежных учреждений, сбои, вызванные хакерами, выпуск компрометирующих электронных писем от банкиров или регулирующих органов или захват учетных записей. Каким бы ни был спусковой крючок, достаточно серьезная потеря уверенности может вызвать «набег на банки»;
3. целостность данных. Системные воздействия могут возникать в результате кибервторжений, которые напрямую изменяют или иным образом влияют на качество рыночных или потребительских данных, что приводит к приостановке работы системы до тех пор, пока не будут восстановлены все оставшиеся неповрежденные резервные копии. Как выяснили многие учреждения из недавних атак программ-вымогателей, таких как WannaCry, восстановление может занять больше времени, чем ожидалось, и привести к потере доверия или другим системным последствиям [72].

Эти «каналы» – буквально пути, по которым киберинцидент может превратиться в финансовый кризис. Мы считаем, что к трем выделенным каналам следует добавить хотя бы один:

* отсутствие взаимозаменяемости (ИКТ): документ подчеркивает, что финансовый сектор зависит от нескольких ключевых центров, но, конечно же, это относится и к ИКТ. Например, большой (и растущий) процент мировых вычислений и хранилищ приходится всего на нескольких поставщиков облачных услуг; корпоративные ИТ-предприятия, как правило, очень похожи и используют одни и те же операционные системы и приложения; все компании зависят от одних и тех же базовых интернет-протоколов, таких как TCP/IP или DNS, а локальные бедствия часто обнаруживают неожиданные физические зависимости, нарушая работу целых регионов или отраслей.

Несмотря на то, что традиционные финансовые и макрополитические потрясения способны причинить широкомасштабный ущерб, они, как правило, возникают в результате самосохранения, а не злого умысла. Трейдер, пытающийся загнать рынок в угол, не стремится разрушить всю систему. Точно так же политики могут ошибаться или недооценивать влияние своей политики, но не действуют с целью создания финансовых потрясений. Кибератаки, напротив, могут быть нацелены и рассчитаны на то, чтобы вывести из строя, разрушить, развратить или поставить под угрозу функционирование рынка, преднамеренно инициировать финансовую нестабильность.

Исходя из вышеизложенного, можно сделать вывод о том, что устойчивость банковской системы является сложноструктурированной категорией, отражающей свойства системы и условия ее функционирования. Вместе с тем, в настоящее время как следствие цифровизации экономики на передний план выходит информационная устойчивость. В целях развития информационной устойчивости для кредитных организаций становится крайне важным обеспечение кибербезопасности и эффективное управление киберрисками, которое поможет снизить количество и вероятность угроз со стороны кибермошенников и свести к минимуму величину потерь от данных угроз. Об этом пойдет речь в следующем параграфе.

## Кибербезопасность как ключевой фактор обеспечения устойчивости коммерческих банков

В последние несколько лет значение финансовых технологий в деятельности коммерческих банков значительно расширилось. Основанием для этого является повышение качества обслуживания клиентов, гибкости, новаторского мышления и развитие цифровой инфраструктуры. Несмотря на противоречие, этот альянс повышает уязвимость коммерческих банков к рискам кибербезопасности из-за развития таких угроз, как атаки вредоносного ПО, утечка и проблемы с целостностью данных. Банковский сектор наиболее уязвим к рискам кибербезопасности, чем любой другой финансовый институт.

Термин кибербезопасность постоянно используется политиками, ИТ-специалистами, предпринимателями и операторами национальной безопасности. Спектр настолько широк, что кажется почти невозможным, чтобы так много людей согласились с одним определением. С момента появления термина многие ученые предпринимали попытки интерпретации и определения кибербезопасности. В таблице в 1.3 представлены некоторые из определений российских и зарубежных авторов и организаций.

Таблица 1.3 – Дефиниции термина кибербезопасность (составлено автором)

|  |  |
| --- | --- |
| Автор / источник | Определение кибербезопасности |
| А.С. Алпеев | * раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности [2]; |
| Концепция стратегии кибербезопасности Российской Федерации | * совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями [24]; |
| Jake Frankenfield | * меры, принимаемые для защиты подключенных к Интернету устройств, сетей и данных от несанкционированного доступа и использования в преступных целях; |

Продолжение таблицы 1.3

|  |  |
| --- | --- |
| Автор / источник | Определение кибербезопасности |
| Лаборатория Касперского | * практика защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак; |
| Public Safety Canada | * совокупность технологий, процессов, практик и мер реагирования и смягчения последствий, предназначенных для защиты сетей, компьютеров, программ и данных от атак, повреждений или несанкционированного доступа с целью обеспечения конфиденциальности, целостности и доступности; |
| Издательство Оксфордского университета, 2014 г. | * состояние защиты от преступного или несанкционированного использования электронных данных или меры, принятые для достижения этого; |
| Майкрософт | * набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от цифровых атак. |

Определения, представленные в таблице 1.3, не раскрывают термин кибербезопасность в полной мере по ряду причин. Во-первых, кибербезопасность как концепция охватывает пространство, которое больше, чем просто защита компьютеров от вирусов или хакерских атак. Она охватывает в том числе безопасность отдельного человека и общества в целом, что на наш взгляд важно подчеркнуть, т. к. прослеживается явная тенденция определять кибербезопасность как связанную с безопасностью систем, а не отдельных лиц.

Во-вторых, рабочее определение кибербезопасности на наш взгляд должно включать не только определение того, что именно защищает, но и от чего защищается референтный объект. В случае кибербезопасности существует несколько типов угроз, но их всех объединяет то, что они влекут за собой какое-то цифровое нарушение/атаку. Таким образом, кибербезопасность это не просто защита от угроз безопасности. Важно понимать, что она связана исключительно с цифровыми технологиями, то есть происходит в киберпространстве.

В-третьих, несмотря на то, что угроза происходит в киберпространстве, она ставит под риск и физическую безопасность, т. к. наносит физический ущерб. Наблюдается «кинетическое пересечение», когда угроза из киберпространства переходит в угрозу в нецифровом пространстве.

Таким образом, концепция кибербезопасности требует многогранного теоретического подхода. Опираясь на представленные в таблице 1.3 определения и собственные соображения, аргументированные выше, мы предлагаем следующее определение обеспечению кибербезопасности:

*Обеспечение кибербезопасности* – это комплекс действий стратегического характера, направленный на защиту критически важных систем и их пользователей от угроз, совершаемых в киберпространстве, с целью предотвратить экономический, технический и информационный ущерб.

Потенциально возможные угрозы превращаются в реальную кибератаку в случаях, когда соответствующие уязвимости использует в своих целях некоторый субъект, которым может быть как физическое лицо, так и программа [18]. Под кибератакой понимается предумышленно организованная попытка проникновения в информационную инфраструктуру, направленная на нанесение экономического, технического или информационного ущерба [2].

Кибербезопасность имеет важное значение для вооруженных сил страны, финансового сектора, крупных корпораций, малого бизнеса и других организаций и частных лиц, поскольку данные в настоящее время являются краеугольным камнем любой организации. Если эти данные будут использованы, то существует много рисков. Чтобы обеспечить защиту данных клиентов при использовании новых технологий, необходимо внедрять интеллектуальные решения для комплексного обеспечения безопасности. Именно развитие информационных технологий является главной причиной эволюции киберрисков.

Финансовый сектор столкнулся с наибольшим количеством кибератак среди всех других отраслей за последние три года, согласно отчету Cybercrime Magazine [72]. Один финансовый сектор был ответственен почти за пятую часть всех кибератак в этот период. В отчете о стоимости киберпреступности за 2019 год говорится, что средняя стоимость киберпреступности в расчете на одну компанию в сфере финансовых услуг составила колоссальные 18,5 млн долларов, что намного выше, чем в любой другой отрасли.

Банковский сектор особенно уязвим из-за ценности хранимых в нем данных. Хакеры продают украденные финансовые данные и банковские учетные данные лицам, предлагающим высокую цену, или используют их для кражи миллионов долларов. Потенциальная поверхность атаки для банков только увеличилась в размерах из-за их большего цифрового присутствия. Банковское дело и кибербезопасность должны идти рука об руку для обеспечения защиты и безопасности данных.

Очевидной причиной важности кибербезопасности в транзакциях банковского сектора является защита активов клиентов. Коммерческие банки хранят очень важные и ценные данные в электронном виде, от информации о кредитных картах и ​​депозитах до имущества, завещаний, титулов и других конфиденциальных данных, и регулярно обрабатывают триллионы рублей. По мере того, как все больше людей переходят на безналичные расчеты, осуществляют операции через онлайн-кассы и мобильные приложения, персональные данные могут быть перенаправлены в другие места и использованы для мошеннических действий. Хотя потребители, вероятно, в случае реализации кибермошенничества смогут вернуть свои деньги в соответствии с федеральным законом, но некоторые эксперты полагают, что эскалация атак может в итоге поставить под угрозу платежеспособность любого крупного банка. Поэтому неудивительно, что на отрасль распространяются нормативные требования, направленные на повышение киберустойчивости и защиту данных и денег потребителей [4].

Итак, разберем детально основные риски кибербезопасности, которые ставят под угрозу устойчивость коммерческих банков:

1. внутренние уязвимости;

Одна из слабых сторон кибербезопасности финансового сектора – это сотрудники. Согласно индексу IBM X-Force Intelligence за 2019 год, почти две трети (29%) проанализированных атак были совершены инсайдерами, попадавшимися на фишинговые электронные письма. В ходе этих атак хакеры нацелены на учетные записи электронной почты старших сотрудников, таких как генеральные директора, и обманным путем вынуждают компанию делиться конфиденциальной информацией.

1. нехватка предложений на рынке труда;

Кибербезопасность организаций является относительно молодой сферой деятельности и довольно многогранной. И поскольку актуальность кибербезопасности только растет, вакансий на рынке труда становится больше, чем предложений.

1. большое количество пользователей;

Проблема нехватки кадров усугубляется тем, что большое и сложное население имеет доступ к банковским и финансовым сетям. От пользователей со стороны персонала до клиентов, банкам приходится иметь дело с множеством точек соприкосновения и не иметь полного контроля над тем, как взаимодействуют эти пользователи. Эти увеличенные точки соприкосновения дают киберпреступникам больше возможностей для атак. Например, персональные устройства пользователей могут стать легкой добычей для хакеров, стремящихся взломать финансовые сети, особенно если пользователи отказываются от таких функций безопасности, как пароли.

1. риски цепочки поставок;

Часто финансовые учреждения имеют сложную систему безопасности и могут полагаться на сторонних поставщиков, таких как поставщики облачных услуг. Даже если собственные системы безопасности банка очень устойчивы к кибератакам, сторонние поставщики услуг могут представлять собой слабое звено в цепочке кибербезопасности. Киберпреступники все чаще нацеливаются на поставщиков программного обеспечения, а затем доставляют вредоносный код клиентам в цепочке поставок посредством загрузки продуктов или обновлений, которые кажутся безопасными.

1. непредсказуемость возникновения кибератаки [8];

Киберриски сопровождаются трудностями в анализе и оценке из-за крайней анонимности киберпреступников, поэтому кибератаку трудно прогнозировать. Киберпреступники пользуются этим преимуществом, которое достигается применением различных механизмов шифрования.

1. трансграничность;

Киберриски не ограниченны в пространстве [11]. Таким образом, киберпреступники и коммерческие банки могут находиться на расстоянии тысяч километров и это не помешает реализации кибератаки.

1. несовершенство законодательства;

Нормативно-правовое регулирование в области кибербезопасности развито слабо. Становление законодательства по кибербезопасности значительно отстает от развития цифровых технологий, в том числе новых форм киберпреступности. Кроме того, имеется неоднозначность в определении элементов состава киберпреступления, поскольку при точном их описании это приведет к снижению гибкости применения закона, а тем более снижению возможности быстрого реагирования на новые виды кибератак.

1. сокрытие произошедших кибератаках;

Организации стремятся не оглашать информацию о том, что они стали жертвой кибермошенников и какой получили от этого убыток, чтоб сохранить свою деловую репутацию [32]. Это делает процесс обнаружения и предотвращения киберпреступлений ещё более затруднительным.

1. убыточность.

В случаях, когда кибератаку не удалось предотвратить, банкам приходится затрачивать огромные суммы на устранение последствий: восстановление данных, расследование инцидента, убытки от перерывов в работе и т. п.

Получается, что киберриски всегда сопряжены с какими-либо неблагоприятными последствиями. Они могут приводить не только к потере прибыли, но и капитала коммерческого банка, что в свою очередь влияет на устойчивость последнего и может привести к банкротству.

Конечно, существует множество причин для такого восприятия риска. Например, угрозы кибербезопасности представляют как операционные, так и репутационные риски. Кибератака может нанести ущерб или полностью подорвать способность финансового учреждения вести бизнес (операционный риск). Более того, клиенты могут потерять доверие и перевести свой бизнес в другое место из-за кибератаки (репутационный риск) [50].

Кибератаки могут повлиять на все сферы жизни, о чем свидетельствуют глобальные атаки программ-вымогателей WannaCrypt в мае 2017 года, которые затронули более 200 000 компьютеров как минимум в 150 странах, в том числе в больницах, коммунальных службах, железных дорогах, телекоммуникационных и автомобильных компаниях; а также более поздняя программа-вымогатель Petya от июня 2017 года, которая поразила компьютеры в 64 странах. Хотя воздействие недавних атак программ-вымогателей на финансовые учреждения было ограниченным, сектор финансовых услуг традиционно был самой большой мишенью из-за привлекательности получения финансовой выгоды и доступа к конфиденциальным финансовым данным [21].

Отдельные финансовые учреждения вкладывают значительные средства в функции контроля для противодействия этим угрозам, повышения осведомленности о рисках и защиты критически важных активов и данных. Власти, в свою очередь, разработали стратегические инициативы, руководящие документы и нормативные подходы для борьбы с киберпреступностью и повышения устойчивости финансовой системы в целом. В мире также разрабатываются различные инициативы, которые способствуют сбору разведданных и обмену информацией между заинтересованными сторонами из государственного и частного секторов (что вместе с данными является необходимым условием для киберстрахования). Но из-за глобального характера, важности и взаимосвязанности финансовой системы, а также резкого роста числа кибератак все большее внимание уделяется тому, какое влияние такие атаки могут оказать не только на отдельные учреждения, но и на стабильность всего финансового сектора.

Таким образом, обеспечение кибербезопасности – это комплекс действий, направленных не только на защиту активов организации, но на защиту активов пользователей от угроз, совершаемых в киберпространстве с целью предотвращения убытков. Финансовые институты являются главными целями для киберпреступников, поскольку имеют широкой цифровое присутствие и являются сосредоточением огромного количества активов и ценных данных. Риски кибербезопасности охватывают как операционные, так и репутационные риски и в случае реализации кибератаки могут нанести колоссальный ущерб коммерческому банку. На устранение последствий кибератак банки затрачивают собственный капитал, а значит такая угроза напрямую воздействует на устойчивость коммерческих банков. Поскольку проблема обеспечения кибербезопасности становится всё более актуальной, банкам необходимо совершенствовать системы управления данным видом риска, чтоб обеспечить стабильное финансовое состояние и устойчивость развития.

**1.3 Современные подходы к обеспечению кибербезопасности коммерческих банков**

ОЭСР (организация экономического сотрудничества и развития), Совет Европы, ЕС, ООН и Интерпол имеют существенное значение в сплочении международных усилий и построении международного сотрудничества в борьбе с преступлениями в цифровой среде [9].

ОЭСР первой взялась за масштабное исследование проблемы киберпреступности и уголовно-правовых мер по борьбе с ней на глобальном уровне. В период 1983–1985 гг. организация исследовала возможности упорядочивания нормативов, предусматривающих уголовную ответственность за преступления в цифровом пространстве [60]. Ключевые результаты данного исследования отражены в докладе «Преступления, связанные с компьютером: анализ правовой политики».

Более прикладной вклад был внесен Генеральной Ассамблеей ООН. В 1990 году 14 декабря была принята резолюция [44], призывающая страны – члены ООН усилить меры по борьбе с киберпреступностью, усовершенствовать национальное законодательство, содействовать развитию международных стандартов предотвращения, судебного преследования и наказания в области преступности в киберпространстве.

Первая международная конференция по преступлениям в киберпространстве была проведена в 1995 году Интерполом. Она подтвердила обеспокоенность международного сообщества распространением киберпреступности. В последующем конференции проводились Интерполом в 1995, 1996, 1998 и 2000 гг.

Ещё одна международная конференция была проведена «Большой восьмеркой» в мае 2000 г. Главной темой конференции было объединение усилий по борьбе с киберпреступностью. По итогам встречи было опубликовано коммюнике, декларирующее, что государства будут принимать усилия для разработки совместного подхода к киберпреступлениям, которые в действительности угрожают устойчивости глобального информационного сообщества [23].

25 мая 2001 в Будапеште после нескольких лет попыток (27 проектов за 4 года) Советом Европы была принята Конвенция о киберпреступности [19]. Ценность этого документа заключается в том, что он регулирует правоотношения в сфере глобальной компьютерной сети. На данный момент это единственный документ такого уровня.

Тем не менее, невзирая на усилия, предпринимаемые на международном уровне, все они прежде всего должны приводить к действия по реформированию уголовного законодательства на национальном уровне. То есть национальные и международные старания должны дополнять друг друга. Это необходимо для обеспечивая глобального внимания к проблемам киберпреступности, стандартизации национальных законодательств и формирования перечня действий по борьбе с преступлениями в киберпространстве. В данном ключе отдельное внимание вызывают проекты законов SOPA и PIPA в Соединенных Штатах Америки [21].

В России уголовно-правовая борьба с преступлениями в сфере компьютерной информации основывается на главе 28 УК РФ, в которой киберпреступления выделены как отдельный институт [61]. В 2016 году 6 декабря была утверждена Доктрина информационной безопасности РФ, содержащая систему официальных взглядов на обеспечение национальной безопасности России в цифровом пространстве [13].

В 2017 году Российская Федерация предложила проект Конвенции ООН о взаимодействии в сфере предотвращения киберпреступности [10, 42]. Генассамблея приняла эту резолюцию, несмотря на сопротивление со стороны США.

В 2018 году на Международном конгрессе по кибербезопасности В. В. Путин озвучил список мер по защите страны от киберпреступности [22]. Озвученные меры включают пять основных шагов:

* разработка комплексных решений, которые включают создание необходимых правовых условий, способствующих эффективной работе спецслужб по реагированию на кибепреступления;
* создание системы автоматизированного обмена информацией между различными структурами о киберугрозах;
* базирование используемого в России программного обеспечения (ПО) и инфраструктуры на сертифицированных российских решениях;
* повышение квалификации российских специалистов по информационной безопасности;
* совершенствование механизма обмена данными о киберпреступлениях с другими странами.

В апреле 2021 года В. В. Путин утвердил основы государственной политики в области международной кибербезопасности. Документ отражает стратегическое планирование международной кибербезопасности, определяет основные угрозы международной информационной безопасности, цели и задачи российской политики в сфере международной кибербезопасности и основные направления её реализации [44].

Основными органами в России, занимающимися вопросами кибербезопасности являются ФСБ, МВД, Служба внешней разведки, Минюст, Министерство обороны, Росгвардия и ФСО [27].

Что касается практический шагов, в 2022 г. в России уже в пятнадцатый раз провели Неделю безопасного Рунета (в 2022 г. она прошла с 2 по 8 февраля). Координатором мероприятия выступает Центр безопасного Интернета при поддержке Лаборатории Касперского, РОЦИТ, РАЭК, Координационного центра доменов .ru и .рф и Ростелеком-Солар [16]. Данные мероприятия посвящены различным аспектам кибербезопасности и рассчитаны на все основные категории пользователей российских платформ от детей до пожилых людей.

Кроме того, ежегодно начиная с 2010 года проводится Международный форум AntiFraud Russia. Форум представляет собой одно из главных событий в сфере борьбы с кибермошенничеством в банковской и телекоммуникационной отраслях, а также в сфере электронной коммерции [15].

ПАО «Сбербанк» является одним из самых деятельных участников в борьбе с киберпреступностью в банковском секторе России. Сбер предлагает новые продукты, открывает центры по кибербезопасности, проводит форумы и конференции. Одним из важнейших его проектов является Международный конгресс по кибербезопасности, который проводится с 2018 года.

В предыдущем параграфе были рассмотрены основные проблемы обеспечения кибербезопасности, ставящие под риск устойчивость коммерческих банков. В таблице 1.4 рассмотрим возможные пути решения рассматриваемых проблем.

Таблица 1.4 – Основные проблемы, порождающие развитие киберпреступности, и пути их решения (составлено автором)

|  |  |
| --- | --- |
| Проблема | Пути решения |
| Внутренние уязвимости | Внедрение культуры обучения, системы мотивации и программные решения |
| Нехватка кадров | Внедрение автоматизированных решений и аутсорсинга |
| Большое количество пользователей | Многофакторная аутентификация, проверка подлинности; повышение IT-грамотности пользователей онлайн ресурсов |
| Риски цепочки поставок | Тщательная проверка и сегментация |
| Непредсказуемость возникновения кибератаки | Инвестиции в исследования в сфере кибербезопасности, выделение грантов, внедрение системы мотивации для IT-специалистов |
| Трансграничность | Партнерство международных организаций с целью предотвращения кибератак, проведение форумов и конференций |
| Несовершенство законодательства | Определение наказаний в зависимости от видов киберпреступлений; внедрение соответствующих нормативно-правовых актов; ужесточение наказания за кибератаки |
| Сокрытие произошедших кибератак | Ужесточение санкций за нераскрытие сведений о произошедших кибератаках, поддержка пострадавших организаций в СМИ для нивелирования репутационных рисков |

Продолжение таблицы 1.4

|  |  |
| --- | --- |
| Проблема | Пути решения |
| Убыточность | Резервирование капитала на покрытие убытков от устранения последствий пережитых киберпреступлений |

Таким образом, крайне необходимо партнерство с другими государствами и выработка международных стандартов противодействия. России в таком случае необходимо продолжать стремиться расширять международное сотрудничество, в том числе выдвигать предложения и поддерживать инициативы других, несмотря на не стабильную политическую конъюнктуру.

Кибербезопасность должна стать предметом заботы не только ИТ-отдела. Персонал, имеющий доступ к сети на всех уровнях (от административного до управленческого) должен быть обучен и компетентен в основах кибербезопасности. Банки должны четко определить, как сотрудники должны взаимодействовать с сетью. Внедрение политики в отношении местоположения и устройств, с которых сотрудники могут входить в систему, а также разрешенного им типа доступа поможет свести киберугрозу к минимуму. Но внутренние уязвимости – это не только сотрудники, но и несвоевременное обновление ПО или плохая конфигурация серверов. В таком случае программные решения, как например антифишинговое ПО для просмотра веб-страниц, могут помочь предотвратить попадание фишинговых электронных писем в почтовые ящики сотрудников [11].

Организации в банковской и финансовой сфере могут использовать автоматизированные решения для борьбы с нехваткой сотрудников в ИТ-секторе. Благодаря быстрому развитию машинного обучения и искусственного интеллекта на рынке появляется все больше инструментов, которые могут автоматизировать кибербезопасность. В настоящее время они доведены до такой степени, что их можно серьезно рассматривать в качестве альтернативы некоторым ИТ-ролям. Кроме того, пробел в знаниях, вызванный нехваткой талантов, можно заполнить за счет аутсорсинга с подрядчиками и поставщиками систем безопасности. Эти третьи стороны могут помочь настроить устройства безопасности и постоянно тестировать технологии, чтобы помочь выполнить обязательства по соблюдению нормативных требований.

Система является безопасной только в том случае, если ее используют осторожно все пользователи сети, поэтому важно найти решение, которое интегрируется с текущими системами и приложениями и является простым в использовании. Так, чтоб обеспечивать безопасность мобильных приложений пользователей, можно внедрить многофакторную аутентификацию. Она поможет обеспечить единообразие взаимодействия с пользователем, предусмотрев дополнительные шаги для доступа.

Для управления рисками в цепочке поставок, при привлечении любого стороннего поставщика крайне важно учитывать последствия для кибербезопасности. Важно владеть полной информацией о том какие данные будут переданы, где они будут храниться, как организация их защищает и кто будет нести ответственность в случае нарушения. Некоторые практические способы обеспечения безопасности данных и сети включают реализацию многофакторной аутентификации между поставщиками.

Также коммерческим банкам рекомендуется разрабатывать экономико-математические модели прогнозирования направлений кибератак и оценки потенциальных рисков. Каждому банку в отдельности необходимо разрабатывать собственные системы защиты данных, оптимизируя процессы обмена информацией внутри организации. Крупными разработчиками банковских систем защиты с богатым опытом в данной области являются Data Protection Systems, Group IB, Cisco и Лаборатория Касперского.

Все перечисленные мероприятия безусловно помогу свести риск возникновения кибератаки к минимуму, но не избавят от него полностью ввиду сложности прогнозирования и анализа этих рисков. В случае, если хакерскую атаку не удалось отклонить, это наносит ущерб прибыли коммерческого банка, поскольку в отдельных случаях необходимы большие затраты на устранение последствий. В сумму таких затрат входят расходы на IT-расследование, восстановление данных и восстановление репутации, убытки от простоя, услуги юристов и др.

В этом случае эффективным финансовым инструментом будет страхование киберрисков. Вместе с тем, киберстрахование недостаточно развито на российском рынке страховых услуг. Такой продукт предлагает несколько компаний, невзирая на то, что в рамках государственной программы «Цифровая экономика» было рассмотрено предложение о том, чтобы сделать киберстрахование обязательным для критической инфраструктуры, к которым относятся и банки.

Страховые решения и их применение играет важную роль в стратегии управления киберрисками. Страхование, в его простейшем определении, представляет собой передачу рисков. Страховые полисы очевидно не должны заменять эффективные стратегии управления. Однако после принятия всех разумных мер для снижения конкретного риска необходимо приобрести страховые полисы, чтобы обеспечить полную защиту организации. Многие брокеры и андеррайтеры, работающие по всему миру, особенно на Западе, специализируются на обеспечении киберрисков. Киберстрахование может покрывать убытки, возникающие в результате прямых последствий киберпреступлений, а также любые убытки, причиненные третьим лицам (клиентам) [20].

Однако, стандартного полиса в области страхования от киберрисков не существует, и страховые компании выдают пакетные полисы, которые могут охватывать ряд гарантий в зависимости от качества и потребностей застрахованного. Необходимо провести комплексный анализ рисков и определить правильные дополнительные гарантии и ограничения. Уровень оперативных и технологических мер кибербезопасности, принятых страхователем, является важным фактором при определении содержания и стоимости страховки. И можно с уверенностью сказать, что желательно, чтобы страховые специалисты имели хотя бы ноу-хау о технологиях кибербезопасности, поскольку данных о документально подтвержденных убытках в этой области недостаточно.

Резюмируя вышесказанное, можно подытожить, что важнейшим направлением развития кибербезопасности является международное сотрудничество, поскольку эффективно совладать с угрозой такого масштаба в одиночку не представляется возможным. Для результативности международного сотрудничества разработка стандартов на глобальном уровне должна сопровождаться развитием национального законодательства, проведением форумов и конференций, созданием условий для проведения исследований в сфере обеспечения кибербезопасности, подготовкой квалифицированных кадров и т. д. На уровне отдельной организации компании должны ответственно подходить к развитию своей системы кибербезопасности, а именно совершенствовать ПО, разрабатывать собственные модели оценки рисков кибербезопасности, страховать киберриски, повышать квалификацию всех сотрудников, способных стать жертвами киберпреступлений и т. д. На сегодняшний день кибербезопасность в российском банковском секторе развита недостаточно. Коммерческим банкам необходимо разрабатывать подход к оценке рисков, законодательную базу и методы управления киберрисками. Ведь то, как растёт количество киберпреступлений и какие приносит потери, он становится одной из главных угроз для банковского сектора, которая влияет на обеспечение его устойчивости.

**2 Исследование устойчивости развития российских коммерческих банков на современном этапе**

**2.1 Оценка показателей устойчивости развития российской банковской системы**

Банковская система России представляет собой совокупность взаимосвязанных между собой кредитных организаций, регулируемых Центральным Банком и функционирующих в рамках единого банковского законодательства. На 01.08.2022 в Российской Федерации действует 363 кредитные организации, из них 329 – банки. Филиалов и внутренних структурных подразделений кредитных организаций насчитывается 25 861 [1].

В целях оценки устойчивости российского банковского сектора будем анализировать следующие макроэкономические показатели: активы, капитал, прибыль, вклады населения, средства на счетах в банках, а также отношения перечисленных показателей к объему ВВП, рентабельность и т. д. Кроме того, важно оценить показатели, определенные Банков России в рамках пруденциального надзора. Эти показателями являются обязательными нормативами деятельности коммерческого банка, установленными в соответствии с Федеральным законом "О Центральном банке Российской Федерации (Банке России)" [62]. В таблице 2.1 сгруппированы ключевые макроэкономические показатели, характеризующие деятельность российского банковского сектора за период 2017–2021 гг.

В таблице по всем макроэкономическим показателям наблюдается положительная динамика. Отношение активов к объёму ВВП за данный период увеличилось на 7,1%, что обусловлено превышением темпов роста активов банковского сектора над экономическим ростом страны. Небольшие снижения данного показателя были в 2018–2019 гг. и в 2021 г., что вызвано социально-экономическими процессами в России и мире.

Таблица 2.1 Основные макроэкономические показатели деятельности российского банковского сектора [1]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Показатель | 01.01.18 | 01.01.2019 | 01.01.2020 | 01.01.2021 | 01.01.2022 | Темп  роста, % | Абсолютное отклонение |
| 1. Активы банковского сектора, млрд руб. | 77 961 | 86 232 | 88 796 | 103 842 | 120 310 | 154,3 | 42 349 |
| в % к ВВП | 84,9 | 83,0 | 81,0 | 96,8 | 92,0 | - | 7,1 |
| 1. Собственный капитал, млрд руб. | 9 397 | 10 269 | 10 981 | 11 413 | 12 605 | 127,5 | 3 208 |
| в % к ВВП | 10,2 | 9,9 | 10,1 | 10,7 | 9,6 | - | -0,6 |
| в % к активам | 12,1 | 11,9 | 12,4 | 11,0 | 10,5 | - | -1,6 |
| 1. Корпоративные кредиты и кредиты физ. лицам, млрд руб. | 45 994 | 52 912 | 56 654 | 64 804 | 74 949 | 163 | 28 955 |
| в % к ВВП | 50,1 | 50,9 | 51,7 | 60,4 | 57,3 | - | 7,2 |
| в % к активам | 59,0 | 61,4 | 63,8 | 62,4 | 62,3 | - | 3,3 |
| 1. Вложения в ценные бумаги, млрд руб | 10 564 | 11 484 | 12 012 | 16 151 | 17 289 | 163,7 | 6 725 |
| в % к ВВП | 11,5 | 11,1 | 11,0 | 15,0 | 13,2 | - | 1,7 |
| в % к активам | 13,6 | 13,3 | 13,5 | 15,6 | 14,4 | - | 0,8 |
| 1. Вклады физ. лиц, млрд руб. | 25 987 | 28 459 | 30 412 | 32 834 | 34 695 | 133,5 | 8 708 |
| в % к ВВП | 28,3 | 27,4 | 27,7 | 30,6 | 26,5 | - | -1,8 |
| в % к пассивам | 33,3 | 33,0 | 34,2 | 31,6 | 28,8 | - | -4,5 |
| 1. Депозиты и средства корпоративных клиентов, млрд руб. | 24 843 | 28 005 | 28 146 | 34 067 | 39 885 | 160,5 | 15 042 |
| в % к ВВП | 27,0 | 27,0 | 25,8 | 31,8 | 30,5 | - | 3,5 |
| в % к пассивам | 31,9 | 32,5 | 31,7 | 32,8 | 33,2 | - | 1,3 |

Основными путями направления ресурсов банков являются коммерческие кредиты и кредиты, предоставленные физическим лицам. Их отношение к объему ВВП за анализируемый период выросло на 7,2%. Портфель ценных бумаг увеличился на 163,7%. Данный актив можно использовать в качестве обеспечения сделок рефинансирования Банка России, когда ликвидности недостаточно.

Ресурсы банков в 2017–2019 гг. по большей части формировались за счет средств, полученных от физических лиц, однако в 2020–2021 гг. перевешивать стали средства корпоративных клиентов (их значение по отношению к ВВП увеличилось на 3,5% за анализируемый период, а в структуре пассивов – рост на 1,3%). За счет депозитов и средств корпоративных клиентов пассивы банковского сектора увеличились на 15 042 млрд руб. за период 2018–2021 гг. и составили долю 33,2% на 01.01.2022. Это может свидетельствовать о росте доверия реального сектора экономики банковскому сектору, что положительно сказывается на финансовой устойчивости последнего.

В таблице 2.2 представлены макропруденциальные показатели деятельности банковского сектора.

Таблица 2.2 – Макропруденциальные показатели деятельности российского банковского сектора [1]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Показатель | 01.01.18 | 01.01.19 | 01.01.20 | 01.01.21 | 01.01.22 | Абсолютное  отклонение |
| Достаточность  капитала (Н1) | 12,1 | 12,2 | 12,2 | 12,5 | 12,3 | 0,2 |
| Норматив мгновенной ликвидности (Н2) | 118,5 | 128,7 | 136,7 | 84,3 | 104,6 | -13,9 |
| Норматив текущей  ликвидности (Н3) | 167,4 | 166,4 | 180,4 | 118,6 | 132,6 | -34,8 |
| Норматив долгосрочной ликвидности (Н4) | 55,4 | 57,5 | 53,6 | 58,1 | 60,6 | 5,2 |
| Рентабельность  активов | 1,0 | 1,5 | 2,0 | 1,7 | 2,1 | 1,1 |
| Рентабельность  капитала | 8,3 | 13,8 | 19,5 | 15,7 | 21,1 | 12,8 |

Норматив достаточности собственных средств является одним из важнейших показателей устойчивости банка и отражает его способность покрывать предполагаемые финансовые потери за счет собственного капитала, т. е. без ущерба клиентам. За анализируемый период данный показатель стабильно выше порогового значения и даже вырос на 0,2%, что говорит о том, что рост капитала был немного быстрее, чем рост активов банка. Это может выть связано с тем, что во время экономической нестабильности банки, желая обезопасить себя, увеличивают собственный капитал и ограничивают выдачу кредитных средств. Так, наибольший рост этого показателя наблюдается в «пандемийный» 2020 г.

Все показатели ликвидности также значительно превосходят пороговые значения, однако наблюдается отрицательная динамика за анализируемый период. Это значит, что ликвидных активов меньше, чем обязательств банка. Отрицательная динамика показателей Н2 и Н3 связана со снижением данных показателей в 2020 г., в период экономической нестабильности во всем мире.

Тем не менее, по данным таблицы все ключевые нормативы выполняются, что говорит об эффективном управлении банками своими активами и обязательствам. Однако отметим, что накапливаемые кредитными организациями риски реализуются в периоды снижения экономической стабильности, как например мы заметили по некоторым показателям за 2020 г.

В текущем же году, основной угрозой, которая может привести к потере устойчивости коммерческого банка, является конфиденциальность банковской информации. Данный подвид операционного риска достиг пика своего развития во время пандемии и продолжает распространение сейчас, когда мир охватил новый экономический кризис. По данным «Лаборатории Касперского», в четверку наиболее пострадавших стран от этих кибератак вошли Россия, Украина, Индия и Тайвань [69].

Согласно Positive Technologies 30% российских банков, опрошенных в ходе исследования «Сколько стоит безопасность» в 2017 г., оценивают потери от одного дня простоя из-за кибератаки в 50 млн рублей. Оценки остальных участников опроса распределились следующим образом: 7% опрошенных – 10–50 млн руб., 25% – 2-10 млн руб. и 38% – 0,5-2 млн рублей. Помимо потерь от простоя, банкам также необходимо нести затраты на восстановление корпоративной инфраструктуры. 12% из опрошенных банков оцениваю восстановление от кибератак в сумму от 10 до 50 млн руб., а треть банков (33%) готова потратить на восстановление от 2 до 10 млн рублей. Большее беспокойство у опрошенных банков вызывает угроза кражи базы данных. Так, больше половины из них (53%) оценили ожидаемые потери от кражи базы данных в сумму более 50 млн рублей [58].

Согласно ежегодному отчету ФинЦЕРТ, посвященному анализу и мониторингу операций, совершаемых без согласия клиентов финансовых организаций; основную долю всех операций без согласия клиентов составляют методы социальной инженерии (49,4% в 2021 г.). Общий объем и количество таких операций (без согласия клиента) выросли к 2021 г. на 33,8% и 38,8% соответственно по сравнению с 2020 г. (рис. 2.2) [36-38].

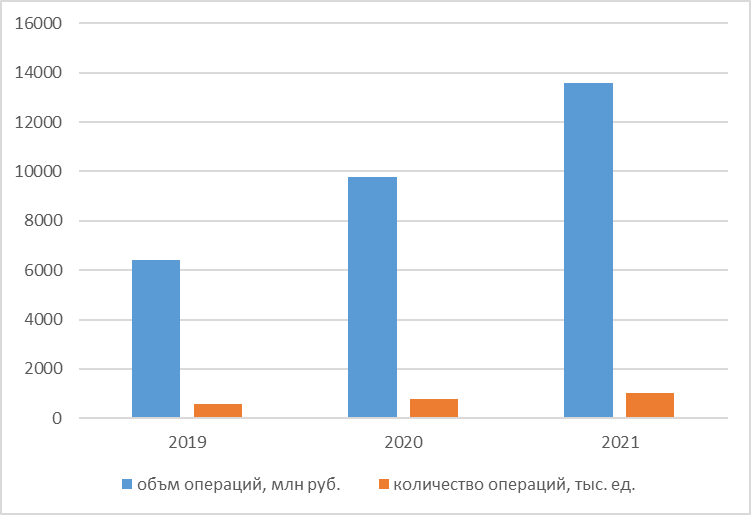


Рисунок 2.1 – Общий объем и количество операций без согласия клиентов [36-38]

По рисунку 2.1 можно заметить, что объем и количество таких операций постоянно увеличиваются. Причиной тому служит активное развития новых дистанционных платежных сервисов и рост объема денежных переводов с использованием электронных средств платежа.

Наиболее распространенными способами социальной инженерии стали:

1. CNP-транзакции (операции по банковским платежным картам без их физического присутствия) – в 2021 году клиенты банков сообщили о 742,3 тыс. таких транзакций (объем хищений составил 4 140,2 млн руб.);
2. через банкоматы, терминалы, импринтеры – 83,9 тыс. случаев (объем хищений 1 971,2 млн руб.);
3. в системе дистанционного банковского обслуживания – в 2021 г. становились мишенью мошенников более 204,6 тыс. раз (объем хищений 6 019,7 млн руб.);
4. телефонное мошенничество. В 2021 году Банком России было заблокировано 179 071 номер, используемых злоумышленниками для хищения средств у граждан.
5. использованием фишинговых сайтов. В 2021 году сайты чаще всего маскировались под сайты действующих коммерческих банков в целях получения персональных данных пользователей, данных для входа в онлайн-банк, а также информацию по банковским картам (рисунок 2.2) [38].

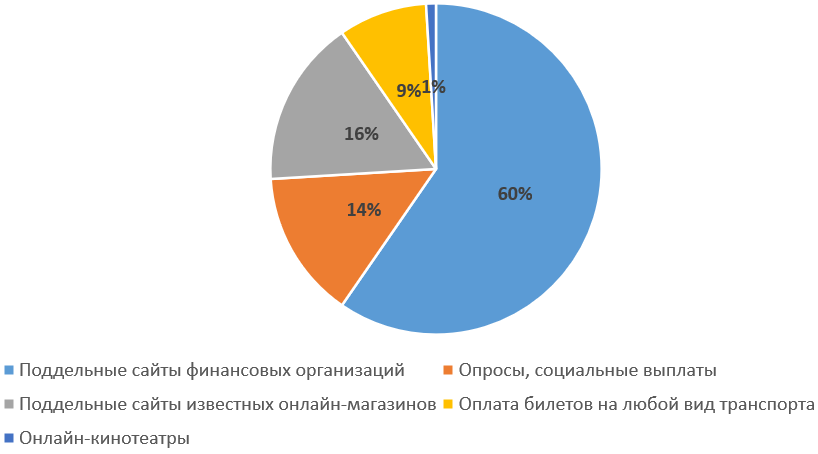


Рисунок 2.2 – Виды мошеннических сайтов [38]

Набор средств и методов атак, которыми оперируют злоумышленники, ситуативно меняются в зависимости от обстоятельств внешней среды [14]. Так, в 2020 г. возросло число кибератак на различные сервисы дистанционного обслуживания. Основной предпосылкой послужил переход коммерческих банков на удаленный режим работы (временное закрытие филиалов банков). Во-первым, клиенты банков стали чаще использовать банковские приложения для оплаты различных услуг. А во-вторых, под угрозой оказались ПО сотрудников банков, работающих удаленно с помощью личных ПК [35]. В 2020 г. (в сравнении с предыдущим годом) Банк России зафиксировал:

1. рост количества фишинговых рассылок;
2. появление новых видов вредоносного программного обеспечения (ВПО);
3. активизацию хакерских группировок.

В 2020 г. через АСОИ ФинЦЕРТ было получено 968 сообщений о фактах распространения ВПО, содержавших 1300 образцов ВПО. Сравнение структуры ВПО с данными 2019 года позволило выделить следующую тенденцию. Если в 2019 г. программы-шифровальщики (программы, которые шифруют файлы и требуют выкуп за их расшифровку) занимали лидирующую долю (50%), а на втором месте было шпионское (используется для отслеживания действий пользователя в целях получения доступа к конфиденциальной информации) ПО (21%), то в 2020 г. на первое место вышло шпионское ПО, доля которого выросла более чем в 2,5 раза. В дальнейшем наблюдается тенденция к практически полному уходу программ-шифровальщиков [35].

Число кибератак на российский банковский сектор достигло своего пика в первой половине 2022 г. С конца февраля текущего года российские коммерческие банки подвергались активным кибератакам. По словам главы департамента информационной безопасности Банка России Вадима Уварова их количество увеличилось в 20 раз по сравнению с аналогичным периодом предыдущего года [64].

При этом у преступников не появилось каких-либо принципиально новых инструментов, изменилось лишь количество попыток взлома. Причиной такого резкого скачка могли служить политически мотивированные действия хакеров, уход из страны вендоров, выпускающих системы защиты информации, и проблемы с привлечением к ответственности киберпреступников, находящихся за рубежом. Положительной стороной, которую можно разглядеть в данном случае, является рост спроса на защитные продукты российских разработчиков, чему способствует сокращение конкуренции.

Таким образом, за анализируемый период 2017–2021 гг. российский банковский сектор демонстрирует положительный рост почти по всем ключевым макроэкономическим и макропруденциальным показателям. Отрицательное абсолютное отклонение наблюдалось только по показателям текущей и мгновенной ликвидности, что было связано с нестабильной экономической конъюнктурой в стране. Одной из угроз, которая получила распространение как раз в период экономической нестабильности, является киберпреступность. Рост его количества и объема прямо влияет на устойчивость развития банков, поскольку огромные расходы на расследование и устранение последствий кибератак уменьшают величину собственного капитала. Основным методом хищения средств у клиентов коммерческих банков является социальная инженерия. Следовательно, чтоб избежать больших потерь и репутационных рисков, банкам следует развивать свою систему кибербезопасности.

**2.2 Анализ существующих моделей оценки рисков кибербезопасности, обеспечивающих устойчивость российских коммерческих банков**

Единой универсальной методики анализа устойчивости банка не существует (не только в России, но и за рубежом), поскольку банки различаются по функциональному признаку, набору выполняемых операций и услуг, составу клиентов, территориальному признаку, проводимой политике на финансовых рынках и т. д.

Финансовым организациям, в частности – банкам, необходимо поддерживать уровень кибербезопасности на должном уровне, дабы обезопасить себя от нежелательных потерь. Однако, это требует значительных усилий и затрат, поэтому не все кредитные организации занимаются этим, в особенности мелкие банки. Одним из основных направлений совершенствования кибербезопасности в банковском секторе является разработка экономико-математических моделей прогнозирования кибератак и оценки рисков. Моделирование рисков кибербезопасности – это задача создания множества сценариев риска, оценки серьезности каждого из них и количественного определения потенциального результата в случае реализации любого сценария.

Моделирование киберрисков коммерческих банков развито слабо из-за новизны проблемы и сложности оценки рисков. Банки не готовы раскрывать информацию об имеющихся средствах защиты, произошедших кибератаках и размере причиненного ущерба.

Несмотря на существование различных моделей оценки киберрисков, специалисты российского финансового конгломерата ПАО Сбербанка разработали собственную методику, поскольку при попытке выбрать подходящий метод столкнулись со следующими трудностями [25]:

* все существующие методики трудно адаптируются к значительному объёму обрабатываемой информации и огромному количеству банковских процессов, особенно когда речь идет о таком крупной компании как Сбер;
* иррациональность применения методов, требующих оценки стоимости активов, поскольку ценность не каждого актива можно оценить количественно (например, какова ценность продукта «Сбербанк Онлайн»), а также потому, что ценность подобных активов меняется каждый день, и оценить эти изменения очень нелегко;
* не гибкость применения методов сценарного анализа, согласно которым вероятность реализации инцидента равна произведению вероятностей всех событий, которые в итоге привели к нему. Данные модели подходят не для каждого вида киберриска. Они эффективны, например, для анализа сбоев и нарушения доступности, но не подходят для оценки риска утечки данных;
* затруднительность применения балльных методов оценки киберрисков, ввиду необходимости их доработки, которая позволит объединить многочисленные факторы, влияющие на риск, в единый метод.

Модель оценки киберрисков Сбербанка постоянно обновляется и совершенствуется, чтобы быть актуальной и результативной в связи со стремительным развитием кибератак, которые с каждым днем становятся все сложнее и мощнее. Прообраз, на котором основывается нынешняя модель оценки киберрисков Сбера был представлен в конце 2017 г. менеджером по методологии кибербезопасности Сбера, Надеждой Симачевской [26].

Основные моменты, на которых основывались специалисты при создании инструмента оценки киберрисков:

1. объективное представление об уровне кибератаки;
2. легкость и удобство в процессе оценки;
3. привлечение к оценке рисков кибербезопасности специалистов разного профиля;
4. универсализация методики оценки для возможности сравнения результатов и ранжирования их по степени важности.

При разработке методика базировалась на классической формуле риска (1), это вероятность наступления инцидента, умноженная на величину возможного ущерба [7]:

𝑅 = 𝑈 ∗ 𝑝 (1)

где

*U* – величина возможного ущерба,

*p* – вероятность наступления рискового события.

Был выделен перечень факторов риска, оказывающих влияние на оба показателя, который представлен в таблице 2.3.

Таблица 2.3 – Система риск-факторов [26]

|  |  |  |
| --- | --- | --- |
| Ущерб (U) | \* | Вероятность (p) |
| Критичность информационного актива | Актуальные угрозы |
| Обрабатываемые данные | Уязвимости, через которые могут  реализовываться угрозы |
| Нарушения функционирования процессов |
| Недовольство клиентов и партнеров | Потенциал нарушителя |
| Репутационные потери | Эффективность защитных мер |
| Санкции регуляторов |

Оценка риска кибербезопасности проводится в 3 этапа.

*Первый этап*. Определение перечня риск-факторов для оцениваемого вида киберриска. Для каждого вида риска эксперты выделяют перечень актуальных угроз, уязвимостей и мер защиты.

*Второй этап.* Экспертная оценка риск-факторов. Независимо друг от друга эксперты оценивают каждый риск-фактор по четырехуровневой шкале (рисунок 2.3 и 2.4). Уровень риска определяется произведением оценок ущерба и вероятности, установленных экспертом.

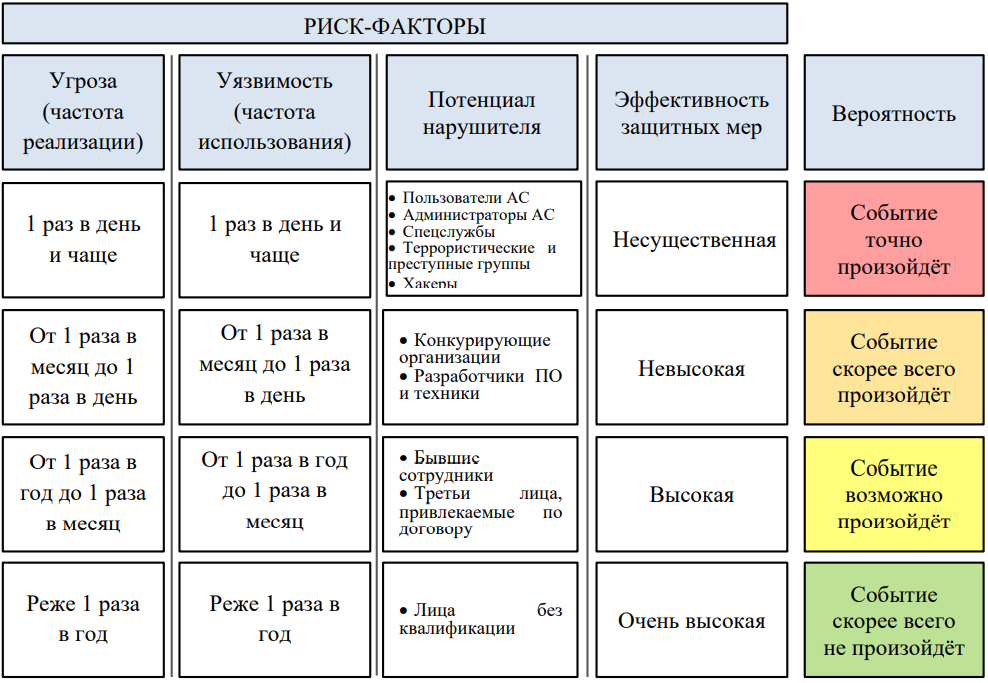


Рисунок 2.3 – Критерии оценки риск-факторов показателей вероятности [26]

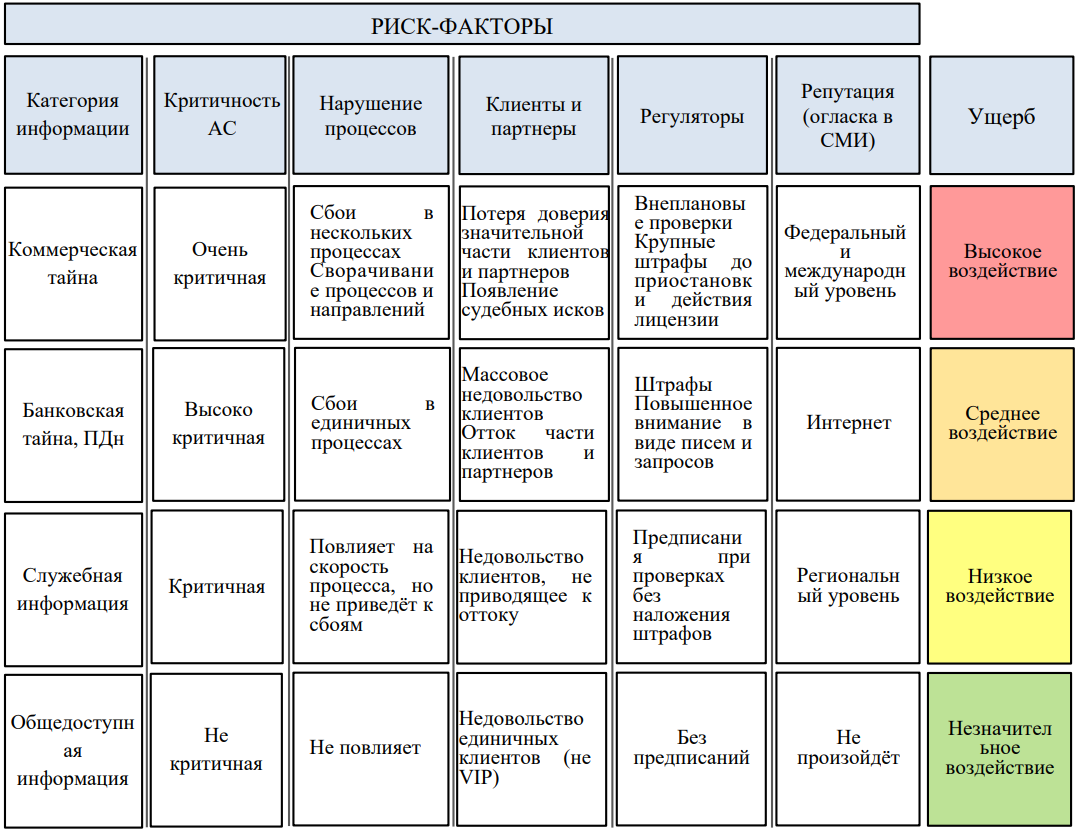


Рисунок 2.4 – Критерии оценки риск-факторов показателей ущерба [26]

Также на этом этапе определяется вес каждого из риск-факторов с целью снизить воздействие на итоговый показатель киберриска некритичных для него факторов. Например, для риска утечки информации некритичной является оценка ущерба от нарушения процессов, а параметр «категория информации» является определяющим, и его вес необходимо повысить. Веса факторов оцениваются по шкале от 1 до 9.

*Третий этап.* Вычисление рейтинга киберриска. На этом этапе заметно значительное отличие методики Сбера от остальных. Преимущество состоит в возможности объединить большое количество полученных мнений и весов в одном значении рейтинга риска (R) в отличие от, предположим, классического метода, при котором уровень риска находится на пересечении соответствующей строки вероятности и столбца ущерба, не имея возможности оперировать большим количеством мнений экспертов.

Для расчета итогового рейтинга риска (*R*) методика Сбера использует матричный метод вычислений, объединяющий все качественно оцененные факторы в одно количественное значение. Это не только позволяет учесть многообразие мнений экспертов, но и разницу в весах, что повышает объективность оценки. Рейтинг риска (*R*), выраженный числом от 0 до 1, и соответствующий ему уровень риска, определяется по таблице 2.4.

Таблица 2.4 – Система определения соответствующего рейтингу (R) уровня риска [26]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Рейтинг риска | Низкий | Средний | Высокий | Критический |
| Значение R | R < 0,25 | 0,25 ≤ R < 0,5 | 0,5 ≤ R < 0,75 | 0,75 ≤ R |

Таким образом, модель оценки киберрисков Сбербанка способствует решению основных задач обеспечения кибербезопасности коммерческого банка:

* результат оценки – это спектр значений рейтинга риска, что даёт возможность сравнить результаты и ранжировать их по уровню важности;
* имеется возможность оценки динамики уровня риска при небольшом изменении тех или иных риск-факторов;
* методика применима при любых объемах оценки;
* алгоритм и критерии оценки понятны для всех сотрудников, от бизнесменов до работников отдела безопасности;
* процесс оценки экспертами не требует больших затрат времени и является простым и удобным в применении.

Риски являются частью каждого ИТ-проекта и бизнес-организации. Анализ риска должен проводиться на регулярной основе и обновляться для выявления новых потенциальных угроз. Стратегический анализ рисков помогает свести к минимуму вероятность будущих рисков и ущерб. Анализ рисков применяется к информационным технологиям, проектам, вопросам безопасности и любому другому событию, где риски могут быть проанализированы на количественной и качественной основе.

И всё же, для обеспечения банковской кибербезопасности определенной автоматизированной системы нет, как и нет заранее готового, стабильного решения. Это диктуется динамикой банковского сектора и связано с тем, что структура каждого коммерческого банка, функциональные связи между его подразделениями и отдельными сотрудниками уникальны, динамично разви-ваются и фактически никогда не повторяются. Только лишь прямое руковод-ство банка на основе экономических показателей и анализа киберрисков решает, насколько критично нарушение кибербезопасности для компонентов своей информационной системы. И на основе этого разрабатывает собствен-ный механизм управления киберрисками.

**2.3 Выявление проблем и перспектив развития устойчивости российских коммерческих банков на примере ПАО «Сбербанк»**

Коммерческий банк ПАО «Сбербанк» является одним из крупнейших банков России и ведущим международным финансовым институтом [34]. Мажоритарным акционером Сбербанка является Фонд национального благосостояния России, который владеет 50% уставного капитала плюс одна голосующая акция (остальные акции – в публичном обращении). В таблице 2.5 представлены основные характеристики банка.

Таблица 2.5 – Ключевые характеристики Сбербанка за декабрь 2021 г. [34]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Количество подразделений | Количество сотрудников | Активы,  млрд руб. | Чистая прибыль, млрд руб. | Капитал, млрд руб. |
| 13 600 | 288 000 | 38 812 | 1 147 | 5 071 |

В 2021 г. чистая прибыль Сбербанка впервые превысила 1 трлн рублей, увеличившись в 1,7 раза по сравнению с предыдущим годом, за счет увеличения кредитования и запуска новых кредитных продуктов. По объему активов Сбербанк является лидером российского банковского сектора – 2021 году они увеличились на 15% и достигли 38 трлн руб. Капитал в основном за счет роста чистой прибыли вырос на 1,62% до 5 трлн руб. Более того, банк занимает крупнеющую долю на рынке по вкладам и кредитам (36,7% в 2021 г.) [57].

Норматив достаточности собственных средств (Н1) Сбербанка за январь 2022 г. равен 14,17%, что превышает среднее значение норматива по сектору на 1,87%. Учитывая всё вышеизложенное, можно характеризовать Сбербанк как устойчивый и довольно надежный банк.

Сбербанк является одним из лидеров по внедрению инноваций и современных технологий. Так, чтоб сделать свои сервисы более совершенными, удобным и технологичным банк регулярно развивает возможности дистанционного управления счетами клиентов. Кроме того, в Сбербанке реализована система удаленных каналов обслуживания, в которую входят:

* веб-сайт «Сбербанк Онлайн»;
* мобильные приложения «Сбербанк Онлайн» для смартфонов (более 73,5 млн активных ежемесячных пользователей);
* SMS-сервис «Мобильный банк»;
* сеть устройств самообслуживания (более 61,4 тыс. банкоматов и терминалов в России) [34].

Среди всех российских банковских мобильных приложений самым популярным является приложение Сбербанка. Клиенты с его помощью контролируют состояние своих карт, вкладов, счетов; просматривают операции и получают выписки по счетам; открывают вклады; получают информацию об имеющихся кредитах и оформляю их; осуществляют переводы и различного рода платежи и т. д. Приложение имеет антивирусную систему и является относительно безопасным, однако внушительное количество пользователей делает его привлекательной мишенью для хакеров и киберприступников, которые способны обойти защиту или ввести пользователей в заблуждение и украсть их денежных средств.

В 2018 г. компания запланировала построить экосистему вокруг Сбербанка, включающую финансовые и нефинансовые услуги. Сейчас в неё входят такие компании как «СберМаркет», «СберМегаМаркет», «Самокат», «Okko», «СберЛогистика», «Еаптека», «Звук», «СберЗдоровье», «СберСпасибо», «СберСтрахование», «СберМобайл» и «СберДиск». Помимо этого, Сбербанк активно участвует в совместных предприятиях с такими компаниями как Яндекс.Маркет, Rambler.group, Mail.ru Group. Также банк имеет собственные разработки – «ДомКлик», «Поговорим», «СбербанкАСТ», «Сбер решения», «Bi.Zone» и др.

Из вышеизложенного можно заметить, что в основном все новые бизнес-проекты, в которые вкладывает средства Сбербанк, являются диджитал платформами и сервисами или виртуальными продуктами. Это связано с актуальностью возможности удаленного доступа к счетам и банковским операциям, использования искусственного интеллекта для биометрической аутентификации, развитие системы онлайн-банкинга и т. п. Однако такая тенденция сопровождается рядом рисков, ключевым из которых являются риски кибербезопасности. Известные случаи кибермошенничества на Сбербанк представлены в таблице 2.6 в хронологическом порядке.

Таблица 2.6 – Последствия известных случаев кибератак в ПАО «Сбербанк» за период 2016–2022 гг. [34, 57, 63]

|  |  |  |
| --- | --- | --- |
| Год | Кибератака | Последствия |
| 2016 | DdoS-атаки; массовые рассылки почтовых сообщений, содержащих загрузчики ВПО; фишинг; атаки, направленные на устройства самообслуживания | Предотвращен ущерб от мошенничества в каналах ДБО на сумму 16 млрд руб. Ущерб от мошенничества в «Сбербанк Онлайн» снижен более чем в 7 раз, в системе «Мобильный банк» - в 2 раза. |
| 2017 | DdoS-атаки; социальная инженерия; фишинг; атаки, направленные на устройства самообслуживания | Предотвращён ущерб на сумму 40 млрд руб. Ущерб от фишинговых атак свыше 5 млн руб. |

Продолжение таблицы 2.6

|  |  |  |
| --- | --- | --- |
| Год | Кибератака | Последствия |
| 2018 | DdoS-атаки; социальная инженерия; фишинг; атаки, направленные на устройства самообслуживания | Предотвращён ущерб на сумму 32 млрд руб. средств клиентов. Ущерб от ограблений банкоматов – свыше 10 млн. руб. Утечка данных сотрудников Сбербанка. |
| 2019 | DdoS-атаки; социальная инженерия; фишинг; атаки, направленные на устройства самообслуживания | 39,7 млрд. руб. – объём предотвращенного фрода во всех удаленных каналах обслуживания. 2,5 млн жалоб на телефонное мошенничество. Утечка данных клиентов Сбербанка |
| 2020 | Социальная инженерия; DdoS-атаки; взлом банкоматов; 16 тыс. фишинговых сайтов с символикой Сбербанка; атаки, направленные на устройства самооб-служивания | Предотвращена попытка хищения средств со счетов клиентов на общую сумму около 57 млрд рублей. |
| 2021 | Два громких дела о краже сотрудниками Сбербанка денег со счетов клиентов.  DdoS-атаки; социальная инженерия; фишинг; атаки, направленные на устройства самообслуживания | Информация о потерях банка в общем доступе не представлена. |
| 2022 | Крупнейшая в истории Сбербанка DdoS-атака, в которой участвовало не менее 104 000 хакеров и не менее 30 000 устройств. Более 25 000 кибератак на госресурсы и | DdoS-атака успешно ликвидирована.  Предотвращено более 470 хакерских атак. Информация о потерях банка не представлена. |

Продолжение таблицы 2.6

|  |  |  |
| --- | --- | --- |
| Год | Кибератака | Последствия |
|  | 1200 инцидентов на критической инфраструктуре. |  |

Данные, представленные в таблице 2.6 очевидно являются неполными, поскольку чаще всего информация о киберпреступлениях в банках считается конфиденциальной. Такая информация влечет за собой репутационные риски и банки не готовы её разглашать, и тем более говорить о последствиях и потерях. Следовательно, объективно оценить данные таблицы достаточно трудно, что и является одной из главных проблем развития кибербезопасности в стрене.

По словам зампреда правления Сбера Станислава Кузнецова, еженедельно на клиентов банка осуществляется 5000–5500 хакерских атак методами социальной инженерии. Тем не менее, годовые отчеты, публикуемые Сбером, дают нам возможность говорить о том, что система кибербезопасности банка на довольно высоком уровне. Согласно «отчету о воздействии за 2021 год», Сбер реализует систему антифрода, которая базируется на алгоритмах искусственного интеллекта (свыше 100 AI-моделей) с применением собственной графовой базы данных и аналитики [40]. В таблице 2.7 представлен ключевой показатель эффективности антифрода (отношение реализованного фрода к обороту денежных средств).

Таблица 2.7 – Ключевые показатели противодействия мошенничеству в ПАО Сбербанк в 2021 г. [40]

|  |  |  |  |
| --- | --- | --- | --- |
| Эффективность  антифрод-  системы | Количество наград в области антифрода | Размер спасенных средств клиентов, млрд руб. | Доля мошенничества с использованием социальной инженерии |
| 99% | 7 | Более 122 | 94% |

Антифрод Сбера занимает лидирующую позицию в мире – fraud basis point равен 0,13 б.п., что в 48 раз лучше аналогичного показателя международных платежных систем, а эффективность антифрода составляет 99% (+13% по сравнению в 2016 г.). Независимым аудитором оценен уровень зрелости кибербезопасности в Сбербанке, который составил 4,4 (средний показатель по Fortune 500 – 4,1) [40].

Опираясь на «отчет о воздействии за 2021 год» и интервью заместителя председателя правления ПАО "Сбербанк" Станислава Кузнецова, выделим следующие направления противодействия киберугрозам в ПАО «Сбербанк»:

1. интегрирована система фрод-мониторинга в режиме реального времени с системами мониторинга операторов связи. Все существующие каналы взаимодействия клиента и банка подключены к антифроду, что позволяет Сберу выявлять кросс-канальные атаки на своих клиентов. Особое внимание уделяется защите социально-незащищенных категорий граждан – услуга «Близкие рядом» позволяет подтверждать или отклонять проведение транзакций родственниками;
2. внедрены новые сервисы кибербезопасности в приложении «Сбербанк Онлайн», а именно функционал по предупреждению о мошеннических звонках, по установке ограничений на переводы и оплату в интернете, по оперативной блокировке доступа в дистанционных каналах к счетам и картам;
3. инициировано принятие законодательных инициатив в части усиления ответственности за незаконное распространение банковской тайны (216-ФЗ), ускоренной блокировки сайтов, незаконно собирающих ПДн (250-ФЗ), противодействия телефонному мошенничеству (319-ФЗ);
4. назначен ответственный за обработку и защиту персональных данных – институт Data Protection Officer (DPO) и создана кросс-блочная команда Института DPO для организации процессов обработки и защиты персональных данных;
5. защиту инфраструктуры обеспечивает Security Operation Center, сертифицированный в соответствии с международным стандартом ISO/IEC 27001. При этом 95% программного обеспечения является собственной разработкой;
6. внедрение принципов кибербезопасности для сотрудников, регулярное проведение обучений, видео конференций с разъяснениями. Внедрение системы мотивации, предусматривающей замечание/выговор/увольнение за нарушение правил кибербезопасности;
7. повышение уровня кибернетической грамотности клиентов: ведение блогов на популярных ресурсах, публикации в СМИ и выступления на ТВ. Созданы специальные проекты по повышению уровня киберграмотности населения: «Быть родителем. Быть киберзащитником», «Марафон кибербезопасности», видеопроект «Сбер против мошенников!»;
8. соглашения с ведущими российскими учебными заведениями и помощь в подготовке студентов, квалифицированных в вопросах кибербезопасности;
9. наличие сертификата соответствия международному стандарту по информационной безопасности от Британского института стандартов — BSI (Сбер – первый банк РФ, получивший его). Соответствие требованиям международного стандарта ISO/IEC 27001;
10. наличие в экосистеме Сбера дочерней компании Bi.Zone, которая учреждена для создания продуктов в области кибербезопасности, проведения экспертизы и расследования киберпреступлений, тестирования систем Сбера на предмет выявления уязвимостей, разработки рекомендаций по хеджированию киберрисков;
11. организация и первое проведение в 2018 г. Международного конгресса по кибербезопасности при поддержке Ассоциации банков России и АНО «Цифровая экономика». Планируется ежегодное проведение данного конгресса;

Таким образом, проанализировав информацию из открытых источников можем сделать вывод, что Сбер тратит большое количество ресурсов на обеспечение кибербезопасности по различным направлениям и благодаря этому обладает достаточно высоким уровнем устойчивости развития.

Кроме того, согласно статье «Ведомостей», Сбер ищет и другие возможные пути минимизации киберрисков, в том числе думает об их страховании. Но на российском страховом рынке киберстрахование крупных компаний пока развито слабо. Одни страховые компании сталкиваются с неготовностью банков допускать их к оценке собственной IT-инфраструктуры, другие – с недостаточной емкостью рынка страхования киберрисков. Законодательство в этой сфере не сформировано в полной мере в части определения ответственности за нарушения информационной безопасности.

Учитывая крупность бизнеса большинства коммерческих банков, для страховых компаний довольно рискованно принимать на себя обязательства по страхованию их киберрисков. Руководитель отдела страхования финансовых рисков АИГ Владимир Кремер заявил, что страховая сумма на случай ущерба, вызванного нарушением кибербезопасности, для банковского сектора очень высока (начинается от 25 млн долларов). То есть даже один крупный ущерб банка может пошатнуть стабильность страховой компании.

Однако в ближайшее время ситуация должна измениться и уже наблюдается определенная динамика. Так, популяризация страхования рисков кибербезопасности и повышения киберкультуры предусмотрела в национальном проекте «Цифровая экономика Российской Федерации».

Исходя из вышеизложенного можем заключить, что российский банковский сектор за последние пять лет демонстрирует рост по ключевым макроэкономическим и макропруденциальным показателям, что говорит об устойчивости его развития. Однако, анализ показал, что показали проявляют отрицательную динамику в периоды экономической нестабильности. В последние несколько нет, события 2020 г. и 2022 г. спровоцировали рост новой угрозы, прямо влияющей на устойчивость коммерческих банков, – угрозы кибербезопасности. Согласно проведенному анализу, с каждым годом количество киберпреступлений стремительно растет на фоне развития цифровых технологий в банковском секторе. Растет и объем потерь банков от их реализации. Сбербанк как один из лидеров российского финансового рынка по противодействию киберприступности демонстрирует довольно высокий уровень кибербезопасности. Основными стимулами развития этой сферы будут служить постоянное улучшение информационных технологий, совершенствование законодательной базы и формирование киберкультуры среди населения. Для совершенствования имеющихся подходов защиты от киберпреступлений считаем необходимым разрабатывать подходы к анализу и оценке данного вида рисков, а также развивать киберстрахование как эффективный инструмент минимизации ущерба.

**3 Разработка инструментария управления рисками кибербезопасности российских коммерческих банков**

**3.1 Разработка методического подхода к анализу и оценке рисков кибербезопасности**

Для оценки рисков кибербезопасности коммерческий банк должен определить свои ключевые бизнес-цели и активы информационных технологий, необходимые для достижения этих целей. Затем необходимо выявить кибератаки, которые могут негативно повлиять на эти активы, принять решение о вероятности возникновения этих атак и их возможном воздействии; в общем, создание полной картины среды угроз для конкретных активов. Это позволяет заинтересованным сторонам и группам безопасности принимать обоснованные решения о том, как и где внедрять элементы управления безопасностью, чтобы снизить общий риск до уровня, приемлемого для организации.

В этих целях нами рекомендуется разрабатывать экономико-математические модели прогнозирования направлений кибератак и оценки потенциального ущерба (рисков). Разработать универсальные модели для всех банков невозможно, поскольку в каждой из них отличаются цели и задачи менеджмента рисков, анализируемые активы и подходы к оценке. Чем раньше банки начнут свой путь и разработают собственный подход к моделированию управления рисками в области кибербезопасности, тем эффективнее они смогут управлять рисками и устанавливать контроль над ними.

Для поддержки моделирования управления рисками нами разработан методический подход к анализу и оценке рисков нарушения кибербезопасности, на основании которого коммерческим банкам рекомендуется выстраивать собственные механизмы управления рисками (см. рис. 3.1). Предлагаемый методический подход включает в себя следующие направления:

* направления анализа киберугроз;
* формирование сценариев экстремальных ситуаций, вызванных реализацией киберугроз;
* направления оценки рисков нарушения кибербезопасности.

****

Рисунок 3.1 – Методический подход к анализу и оценке киберрисков (составлено автором)

Методический подход разработан в соответствии со стандартом ISO/МЭК 27005-2011 на основе методики анализа киберугроз и оценки рисков информационно-технологической безопасности [68].

В ходе анализа киберугроз решаются следующие задачи:

1) установление контекста;

2) проведение аудита безопасности, включающего:

а) анкетирование критических активов,

б) выявление киберуязвимостей в активах информационно-технологической системы (ИТС),

в) оценка активов ИТС,

г) выявление угроз,

д) выявление типовых векторов атак;

3) оценка рисков.

Прежде чем начать анализ рисков важно установить контекст менеджмента, т. е. определить цель анализа, сферу действия и границы, а также определить основные критерии оценки. В зависимости от контекста, могут быть применены разные подходы менеджмента, причем подходы могут быть разными для каждой итерации. Анализ киберугроз сопровождается описанием ИТС, инвентаризацией, установлением значимости активов ИТС, которое предлагается осуществлять на основе скорректированных номинальных шкал с учетом индикативного анализа, а также категорированием уязвимостей и угроз.

Важным этапом установления контекста является определение критериев оценки рисков. Критерии не могут быть универсальными и устанавливаются каждым банком индивидуально в зависимости от бюджета и задач менеджмента. Помимо критериев оценки должен быть определен перечень критериев воздействия на риск, а также перечень критериев, при которых риск можно принять.

На втором этапе должны быть идентифицированы активы (подлежащие менеджменту риска) и связанные с ними бизнес-процессы. Далее идентифицируются:

1. киберугрозы и источники их возникновения;
2. имеющиеся и разрабатываемые средства контроля;
3. кибеуязвимости, которые могут стать целью киберугроз;
4. последствия реализуемых киберугроз.

Следовательно, анализ киберугроз в интеллектуальной системе осуществляется с помощью продукционной системы. Формируются перечни критических активов и выявленных уязвимостей, соответствующие им киберугрозы, а также типовые векторы атак, представляющие собой цепочку уязвимостей, угроз и целевых активов. На основе полученного результата формируются концепты и связи между ними для дальнейшего построения сценариев.

Формирование сценариев экстремальных ситуаций, вызванных реализацией киберугроз, основывается на системном анализе и исследованиях безопасности. В качестве инструмента сценарного анализа влияния киберугроз на возникновение экстремальных ситуаций предлагается применять байесовские сети доверия (БСД), зарекомендовавшие себя в исследованиях безопасности. На основе БСД менеджментом решаются задачи по вероятностному прогнозированию последствий для системы от использования уязвимостей нарушителем и реализации угроз кибербезопасности путем осуществления прямого вывода. Оценки ожидания проявления того или иного состояния в модели основываются на байесовских вероятностях.

Подход включает 5 основных этапов:

1) формирование концептов сценария и их взаимосвязей;

2) установление вероятностных характеристик, критериев и условий сценария;

3) проведение вычислительного эксперимента и определение вероятности наступления последствий ущербов;

4) построение частной модели угроз;

5) анализ альтернативных сценариев.

В работе частная модель угроз представлена в виде графовой вероятностной модели, описывающей причинно-следственную цепочку угроз кибернетической безопасности, причин их возникновения, последствий, а также вероятность их наступления и степень критичности экстремальной ситуации.

Сценарии оцениваются интегральным показателем вероятности возникновения экстремальной ситуации. Такие ситуации рассматриваются как пессимистический сценарий – набор событий и взаимосвязей между ними, которые приводят к максимальным потерям и ущербу в результате их возникновения и развития. Выполняется построение сценариев возникновения экстремальных ситуаций при известных условиях состояния ИТС банка и вероятных угрозах с учетом информации о распространенных векторах атак. На основе анализа сценариев принимаются управленческие решения как порядок действий, необходимых для достижения предпочтительных состояний и ситуаций.

Оценка рисков нарушения кибербезопасности направлена на:

1. выявление рисков,
2. их качественное или количественное оценивание,
3. ранжирование по установленным критериям.

Риск рассматривается как сочетание последствий некоторого события (инцидента) и связанной с ним возможности возникновения в соответствии с международным стандартом ISO: риск = f (угроза, уязвимость, последствия) [67]. Такой подход к оценке рисков позволит руководству банка распределять риски в соответствии с приоритетом согласно индивидуально установленным критериям.

Оценка рисков может быть качественной или количественной, либо комбинировать оценки. При первой итерации может быть применена качественная оценка для получения общих данных об уровне киберриска, при второй – количественная для большей детализации.

Качественную оценку рисков предлагается проводить с учетом возможности описания и классификации риска по шкале «допустимый», «средний», «критический», а также отображения рисков на тепловой карте и лепестковой диаграмме. Шкала может быть скорректирована в зависимости от обстоятельств или может быть разной при каждой итерации. Преимуществом качественной оценки является доступность в понимании и применении сотрудниками всех уровней, а недостатком – субъективность в выборе шкалы. Количественная оценка использует числовые данные, а значит зависит от точности и полноты данных. Недостатком количественной оценки является невозможность применения к недоступным данным. Тем не менее, коммерческим банкам мы рекомендуем использовать метод присвоения денежного значение (если это возможно), поскольку это даст больше информации для принятия решений. В таком случае на основании показателей риска можно будет определить сколько капитала необходимо банку для покрытия убытков.

После идентификации и оценки последствий должны быть оценены вероятности возникновения каждого из сценариев, также используя качественные и количественные методы оценки. Итогом должны стать сценарии киберинцидентов с их последствиями, а также вероятности их возникновения. На основе полученного перечня измеряются риски и присваиваются им уровни значений (ранжируются). В дальнейшем уровни рисков сравниваются с выбранными на первом этапе критериями оценивания риска. На этом этапе выбранные изначально критерии могут быть скорректированы для последующих итераций.

На основе полученного перечня рисков с присвоенными приоритетами руководство банка должно принять решения по их менеджменту для снижения, сохранения, избежания или переноса рисков (см. рис. 3.2). Решение должно основываться на результатах оценки, необходимом бюджете на реализацию, а также от выгоды, планируемой от реализации принятых решений. Решение о снижении риска следует принимать, когда затраты на реализацию экономически выгодны.

Перечисленные варианты обработки риска не исключают друг друга. Например, в отдельных случаях может быть эффективным сочетание снижения риска и его перенос. План обработки рисков должен основываться на приоритете, установленном на этапе ранжирования рисков.

После принятия решения по обработке риска, важно определить остаточные риски. Для этого риск необходимо повторно оценить с учетом результата, который планируется получить после его обработки. Итерации могут повторяться до тех пор, пока остаточный риск не будет соответствовать критериям принятия риска.

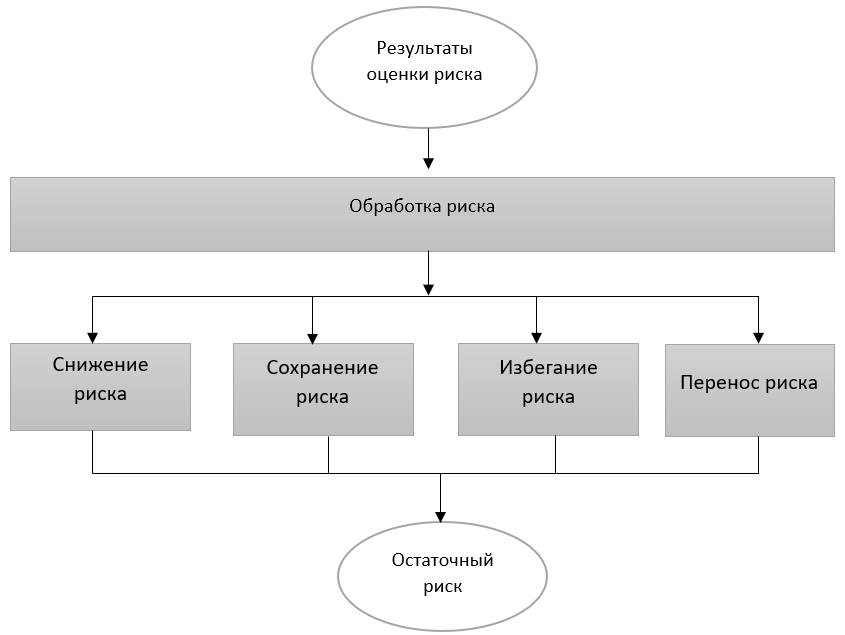


Рисунок 3.2 – Варианты обработки риска [68]

Таким образом, описанный подход к обеспечению безопасности направлен на определение уязвимостей и киберугроз, реализация которых может вызвать нарушение функционирования объекта в такой мере, что можно расценивать инцидент как экстремальную ситуацию. В качестве инструмента сценарного анализа влияния киберугроз на возникновение экстремальных ситуаций предлагается применять байесовские сети доверия, поскольку они зарекомендовали себя в исследованиях рисков в условиях неопределенности. Предложенные направления анализа и оценки рисков кибербезопасности направлены на снижение общего уровня киберриска и как следствия повышению устойчивости развития коммерческих банков.

**3.2 Рекомендации по совершенствованию инструментов страхования киберрисков на примере ПАО «Сбербанк»**

Несмотря на то, что банки из года в год выделяют достаточно ресурсов на обеспечение безопасности внутренних информационных систем, ни одна система не является 100% неуязвимой и риск возникновения хакерской атаки все ещё велик. И как следует из главы 2, если кибератака все же нанесла ущерб, затраты банка на устранение его последствий колоссальны. В таком случае эффективным финансовым инструментом минимизации ущерба является страхование рисков [49].

В данном параграфе речь будет идти о внешнем страховании. Так, например, страхование может включать следующие страховые продукты:

* страхование банка от перерывов в работе, вызванных киберинцидентами и техническим сбоем систем;
* сопутствующие расходы на IT-расследование, юридическое сопровождение, антикризисный PR и прочее;
* страхование третьих лиц от ущерба, причиненного им в связи с нарушением конфиденциальности данных.

На сегодняшний день уровень проникновения страхования киберугроз на российском рынке остается слабым, хоть и наблюдается прогресс. Как правило банки выбирают киберстрахование как дополнительное покрытие к основному полису, но этого недостаточно по ряду причин [55].

С учетом размера бизнеса Сбербанка – его годовая прибыль в несколько раз превышает капитал всех российских страховых компаний – ни одна из них в отдельности не сможет принять на себя обязательства по страхованию киберрисков банка, так как по мнению экспертов даже единичный значимый ущерб Сбербанка по этому риску станет «катастрофичным» для любой страховой компании. Учитывая это, при выборе страховой компании будем обращать внимание на возможность перестрахования рисков в зарубежных страховых компаниях.

При выборе киберстраховщика Сбербанк должен учитывать ряд различных факторов, в том числе финансовую стабильность поставщика, тип предоставляемого покрытия (например, взломы, программы-вымогатели, DDoS-атаки и соответствие нормативным требованиям) и стоимость. Важно знать, что действительно обеспечивает страховой полис, и, может быть, даже более важно, что нет. Важно работать с оператором, который имеет большой опыт работы на рынке и может продемонстрировать высокую финансовую стабильность.

Первой компанией в России, представившей страхование рисков киберугроз, стала ПАО «АИГ», обладающая опытом и экспертизой урегулирования страховых случаев в сфере кибербезопасности. AIG одной из первых применила широкий и единый подход к киберугрозам. На сегодняшний день AIG предоставляет клиентам доступ к услугам компаний, специализирующихся на кибербезопасности и расследованиях киберпреступлений, юридической консультации и антикризисному PR.

Однако, конъюнктура российского рынка в 2022 г. сложилась таким образом, что сотрудничество с международными компаниями несет за собой определенные риски. Под давлением санкций на российскую экономику некоторые страховые компании приняли решение сократить свое присутствие на рынке России или вовсе его покинуть. Чтобы исключить риск возникновения такой угрозы, отбирать страховщика будем только среди российских компаний.

Комплексную страховую защиту от киберугроз в России в настоящее время осуществляют компании «Альянс», «Ингосстрах», «СберСтрахование», «АльфаСтрахование» и «СОГАЗ» [47]. Их надежность и финансовая устойчивость подтверждена национальным рейтинговым агентством RAEX (Эксперт РА) [45]. В таблице 3.1 представлены основные характеристики и преимущества перечисленных компаний, которые предлагают услуги страхования киберрисков.

Таблица 3.1 – Сравнительная характеристика ведущих российских страховых компаний (составлено автором)

|  |  |  |  |
| --- | --- | --- | --- |
| Страховщик | Рейтинг надежности [45] | | Основные характеристики страхования |
|  |  | | 1. страховая защита покрывает: ущерб от перерывов в деятельности, расходы на восстановление системы, расходы на дешифровку данных (включая ПО), расходы по минимизации последствий и расследованию причин; 2. гибкий полис – возможность изменения параметров полиса размер франшизы/период ожидания и т.п.; 3. возможность перестрахования в компаниях с рейтингом надежности не ниже A- по международной шкале Standard and Poor’s: 4. возможность оплаты премии в рассрочку; 5. персональный менеджер, сопровождающий в режиме 24/7/365; 6. компания сотрудничает с ведущими компаниями в области информационной безопасности [53]. |
| АО «Согаз» | | ruAAA |
| СПАО «Ингосстрах» | ruAAA | | 1. комплексная страховая защита; 2. имеется продукт, разработанный специально для банков, включающий широкий перечень покрываемых убытков; 3. возможность электронного подписания документов; 4. комплексная защита не обеспечивает покрытия по убыткам, связанным с мошенническими действиями сотрудников страхователя [17]. |
| АО СК «Альянс» | ruA+ | | 1. страхование включает основное и расширенное страховое покрытие. К основному относится: ущерб третьему лицу, собственный убыток и покрытие расходов на расследование инцидентов; |

Продолжение таблицы 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| Страховщик | Рейтинг надежности | | Основные характеристики страхования |
|  |  | | 1. возможность предоставления максимально широкого покрытия в соответствии с требованиями бизнеса; 2. перестрахование 100% рисков в зарубежных страховых компаниях Allianz SE с рейтингом АА; 3. максимальная емкость собственного капитала – 100 млн. евро; 4. компания является одним из новаторов в области киберстрахования в мире и сотрудничает с ведущими провайдерами ИТ-безопасности [65]. |
|  | |  |
| ООО СК «СберСтрахование» | ruAAA | | 1. продукт по киберстрахованию включает в себя пять различных программ; под страховой защитой находятся программное обеспечение, корпоративная электронная почта, сайты, облачные сервисы и базы данных компаний; 2. индивидуальный подход; 3. для урегулирования убытков привлекаются эксперты компании BI.ZONE, ведущего российского эксперта в области урегулирования киберинцидентов; 4. полис действует в течение не менее12 месяцев [48]. |
| АО «АльфаСтрахование» | ruAAA | | 1. стандартные пакеты полиса покрывают риски утраты и искажения данных, программного обеспечения, разглашения персональных данных и включает расследование и диагностику кибератак; 2. финансовая организация может выбрать один из базовых страховых пакетов или составить индивидуальный, учитывая особенности бизнеса; |

Продолжение таблицы 3.1

|  |  |  |
| --- | --- | --- |
| Страховщик | Рейтинг надежности | Основные характеристики страхования |
|  |  | 1. возможность перестрахования рисков в ведущих западных страховых компаниях; 2. электронный документооборот [3]. |

Сравнительная характеристика ведущих российских страховых компаний, предоставляющих услуги в сфере кибербезопасности, продемонстрировала, что все они находятся примерно на одном и том же уровне развития. Чуть меньше информации получилось собрать с официальной страницы СберСтрахования, так, например, нам не известно предоставляет ли страховщик возможность перестрахования рисков в зарубежных страховых компаниях. Так же из недостатков СберСтрахования отметим невозможность оплаты полиса в рассрочку и невозможность изменения его параметров после заключения договора.

Очевидным преимуществом Ингосстрах является наличие комплексного продукта по страхованию киберрисков, разработанный специально для банков и других финансовых институтов. Данный полис включает широкий перечень страховых рисков, связанных с убытками в результате преступлений против финансовых организаций с использованием их компьютерных сетей и систем электронных расчетов. Однако на сайте не представлена информация о возможности индивидуального подхода к оформлению полиса, что является недостатком для таких крупных организаций как банки. Также на сайте нет информации о возможности перестрахования рисков кибербезопасности, что тоже важно.

Преимуществом АльфаСтрахования и Альянса является индивидуальный подход, Согаза – гибкий полис, а главный плюс всех трех компаний – это возможность перестрахования рисков в ведущих зарубежных страховых компаниях. Однако Альянсу присвоен рейтинг надежности ruA+, что значит, что у компании присутствует некоторая чувствительность к воздействию негативных изменений экономической конъюнктуры.

Учитывая все перечисленные преимущества и недостатки, а также характеристику из таблицы 3.1 Сбербанку рекомендовано сотрудничество с компаниями АО «Согаз» или АО «АльфаСтрахование» в целях комплексного страхования рисков в сфере кибербезопасности с обязательным перестрахованием рисков в зарубежных страховых компаниях. Обеим компаниям присвоен рейтинг ruAAA, что характеризует их максимальным финансовой надежности и устойчивости.

Сама процедура страхования киберрисков выглядит объемно и сложно. И поскольку банки не готовы предоставлять доступ к внутренней информации сторонним организациям, кроме страховой организации в договоре должна фигурировать и компания-аудитор информационной безопасности (ИБ), которая оценит риски и приготовит заключение для страховой компании.

Таким образом, Сбербанку нужно будет пройти следующие этапы:

* выбор страховщика, предлагающего комплексную услугу по страхованию киберррисков, с возможность перестрахования в зарубежной страховой компании;
* выбор экспертной компании для проведения аудита ИБ (из числа организаций, аккредитованных страховщиком);
* аудит и оценка рисков ИБ (проводится экспертной организацией);
* определение страховых случаев;
* определение размера страхового покрытия и страховых взносов;
* формирование договора на комплексную услугу киберстрахования.

К сожалению, для более широкого распространения киберстрахования на российском рынке отсутствует и законодательная база, и судебная практика. Серьёзным препятствием также является нехватка специалистов, имеющих представление о структуре таких рисков. То есть потребность к защите от киберриска есть, но пока к этому не готова российская страховая инфраструктура. Поэтому для минимизации рисков на отечественном рынке рекомендуем следующее:

1. использовать фронтинг. Поскольку страхование киберрисков является слишком рисковым для российских страховых компаний, им рекомендуется использовать фронтинг. В этом случае российским страховым компаниям лучше всего удерживать минимальную долю риска у себя, а оставшуюся передавать иностранному партнеру;
2. использовать передовые аналитические разработки (такие как блокчейн, андеррайтинг) для возможности оценки киберрисков, так как в российской практике нет общепринятой методики;
3. введение налоговых льгот для банков при страховании киберрисков, в том числе отнесение страховых премий по ним на себестоимость при бухгалтерском учёте;
4. введение банками требования к клиентам коммерческого кредита киберстрахования в дополнение к существующим программам управления рисками. Впрочем, и здесь стоит учитывать потенциальные последствия для конкуренции, если банк первым введет такое обязательство. Поскольку универсальной модели киберстрахования не существует, произвольное общее требование о страховании может негативно сказаться на выборе заемщиков.

Таким образом, поскольку достичь абсолютной неуязвимости системы невозможно, разумным инструментом минимизации ущерба и преодоления последствий утечки данных является страхование. Анализ рынка показал, что страхование киберрисков на российском рынке развито довольно слабо, есть только 5 компаний, предоставляющих услуги комплексного страхования, и даже для них такой вид страхования является рисковым. Проведя сравнительный анализ этим компаний, нами были выделены и рекомендованы для Сбербанка страховые компании АО «Согаз» и АО «АльфаСтрахование». Кроме того, страховой договор рекомендуем заключать с возможность перестрахования рисков в ведущих зарубежных страховых компаниях.

Резюмируя вышеизложенное, отметим, что предложенные мероприятия направлены на:

1. идентификацию, анализ и оценку киберрисков с целью их дальнейшего менеджмента;
2. совершенствование инструментов страхования киберрисков с целью минимизации возможных убытков.

Ключевой целью предложенных мероприятий является совершенствование обеспечения кибербезопасности в коммерческих банках, которое способно привести к снижению киберрисков и повышению устойчивости развития банков. Как мы выяснили в параграфе 1.1 совершенствование менеджмента операционных рисков, в которым относятся и риски кибербезопасности, способствует стабилизации финансового положения банка.

Если посредством грамотного менеджмента киберрисков снижается общий уровень рисков кибербезопасности, то банки смогут уменьшить резерв капитала на убытки от реализации операционных рисков, что в конечном итоге приведет к увеличению дохода.

Кроме того, снижения уровня рисков кибербезопасности косвенно влияет на репутацию коммерческих банков. Любое известное нарушение требований кибербезопасности мгновенно распространяется в СМИ, что способно привести к потере лояльности клиентов, а также к привлечению внимания Мегарегулятора.

Таким образом, предложенные мероприятия способствуют снижению рисков кибербезопасности, уменьшению резервов капитала, увеличению дохода и в итоге к увеличению устойчивости развития российских коммерческих банков.

**ЗАКЛЮЧЕНИЕ**

Финансовая система выполняет различные функции, такие как содействие платежам и расчетам, распределение кредита, передача риска и обеспечение ликвидности, а также преобразование сроков погашения и определение цены. Значительное нарушение любой из этих основных функций может вызвать финансовую нестабильность. Поэтому органы по обеспечению финансовой стабильности обеспокоены тем, каким образом финансовые рынки и учреждения могут распространять и усиливать шоки, независимо от их источника. Особый интерес представляет динамика уязвимостей, которая может привести к финансовым кризисам (например, набеги на банки, распродажа активов, потеря доверия). Исторически сложилось так, что эти факторы уязвимости приводили к глубоким рецессиям или депрессиям, дефляции и длительным последующим периодам низкого роста и безработицы.

Современный мир формируется цифровыми технологиями, а киберугрозы представляют собой значительный фактор риска для банковского сектора. Уязвимости системы безопасности приводят к информационному и физическому ущербу для финансовых систем, что, в свою очередь, вызывает проблемы безопасности на национальном и индивидуальном уровнях. Эти уязвимые места и особенно взаимодействие между ними могут сделать финансовые системы хрупкими и подверженными периодическим кризисам. Время и конкретные триггеры кризисов трудно предсказать. Это требует все больших инвестиций в кибербезопасность и уделения повышенного внимания снижению и управлению киберрисками.

В рамках поставленных задач магистерского исследования и на основе проведенного анализа были сделаны следующие выводы:

1. устойчивость банковской системы является сложноструктурированной категорией, отражающей свойства системы и условия ее функционирования. Вместе с тем, в настоящее время как следствие цифровизации экономики на передний план выходит информационная устойчивость. В целях развития информационной устойчивости для кредитных организаций становится крайне важным обеспечение кибербезопасности и эффективное управление киберрисками, которое поможет снизить количество и вероятность угроз со стороны кибермошенников и свести к минимуму величину потерь от данных угроз;
2. обеспечение кибербезопасности – это комплекс действий, направленных не только на защиту активов организации, но на защиту активов пользователей от угроз, совершаемых в киберпространстве с целью предотвращения убытков. Финансовые институты являются главными целями для киберпреступников, поскольку имеют широкой цифровое присутствие и являются сосредоточением огромного количества активов и ценных данных. Риски кибербезопасности охватывают как операционные, так и репутационные риски и в случае реализации кибератаки могут нанести колоссальный ущерб коммерческому банку. На устранение последствий кибератак банки затрачивают собственный капитал, а значит такая угроза напрямую воздействует на устойчивость коммерческих банков. Поскольку проблема обеспечения кибербезопасности становится всё более актуальной, банкам необходимо совершенствовать системы управления данным видом риска, чтоб обеспечить стабильное финансовое состояние и устойчивость развития;
3. важнейшим направлением развития кибербезопасности является международное сотрудничество, поскольку эффективно совладать с угрозой такого масштаба в одиночку не представляется возможным. Для результативности международного сотрудничества разработка стандартов на глобальном уровне должна сопровождаться развитием национального законодательства, проведением форумов и конференций, созданием условий для проведения исследований в сфере обеспечения кибербезопасности, подготовкой квалифицированных кадров и т. д. На уровне отдельной организации компании должны ответственно подходить к развитию своей системы кибербезопасности, а именно совершенствовать ПО, разрабатывать собственные модели оценки рисков кибербезопасности, страховать киберриски, повышать квалификацию всех сотрудников, способных стать жертвами киберпреступлений и т. д. На сегодняшний день кибербезопасность в российском банковском секторе развита недостаточно. Коммерческим банкам необходимо разрабатывать подход к оценке рисков, законодательную базу и методы управления киберрисками. Ведь то, как растёт количество киберпреступлений и какие приносит потери, он становится одной из главных угроз для банковского сектора, которая влияет на обеспечение его устойчивости;
4. за анализируемый период 2017–2021 гг. российский банковский сектор демонстрирует положительный рост почти по всем ключевым макроэкономическим и макропруденциальным показателям. Отрицательное абсолютное отклонение наблюдалось только по показателям текущей и мгновенной ликвидности, что было связано с нестабильной экономической конъюнктурой в стране. Одной из угроз, которая получила распространение как раз в период экономической нестабильности, является киберпреступность. Рост его количества и объема прямо влияет на устойчивость развития банков, поскольку огромные расходы на расследование и устранение последствий кибератак уменьшают величину собственного капитала. Основным методом хищения средств у клиентов коммерческих банков является социальная инженерия. Следовательно, чтоб избежать больших потерь и репутационных рисков, банкам следует развивать свою систему кибербезопасности;
5. для обеспечения банковской кибербезопасности определенной автоматизированной системы нет, как и нет заранее готового, стабильного решения. Это диктуется динамикой банковского сектора и связано с тем, что структура каждого коммерческого банка, функциональные связи между его подразделениями и отдельными сотрудниками уникальны, динамично развиваются и фактически никогда не повторяются. Только лишь прямое руководство банка на основе экономических показателей и анализа киберрисков решает, насколько критично нарушение кибербезопасности для компонентов своей информационной системы. И на основе этого разрабатывает собственный механизм управления киберрисками;
6. российский банковский сектор за последние пять лет демонстрирует рост по ключевым макроэкономическим и макропруденциальным показателям, что говорит об устойчивости его развития. Однако, анализ показал, что показали проявляют отрицательную динамику в периоды экономической нестабильности. В последние несколько нет, события 2020 г. и 2022 г. спровоцировали рост новой угрозы, прямо влияющей на устойчивость коммерческих банков, – угроза кибербезопасности. Согласно проведенному анализу, с каждым годом количество киберпреступлений стремительно растет на фоне развития цифровых технологий в банковском секторе. Растет и объем потерь банков от их реализации. Сбербанк как один из лидеров российского финансового рынка по противодействию киберприступности демонстрирует довольно высокий уровень кибербезопасности. Основными стимулами развития этой сферы будут служить постоянное улучшение информационных технологий, совершенствование законодательной базы и формирование киберкультуры среди населения. Для совершенствования имеющихся подходов защиты от киберпре-ступлений считаем необходимым разрабатывать подходы к анализу и оценке данного вида рисков, а также развивать киберстрахование как эффективный инструмент минимизации ущерба;
7. на основе проведенного исследования предложен методический подход к анализу и оценке киберрисков. Предложенные подходы в сравнении с традиционными подходами к обеспечению кибербезопасности направлены на определение уязвимостей и киберугроз, реализация которых может вызвать нарушение функционирования объекта в такой мере, что можно расценивать инцидент как экстремальную ситуацию;
8. поскольку достичь абсолютной неуязвимости системы невозможно, разумным инструментом минимизации ущерба и преодоления последствий утечки данных является страхование. Анализ рынка показал, что страхование кибер-рисков на российском рынке развито довольно слабо, есть только пять компаний, предоставляющих услуги комплексного страхования, и даже для них такой вид страхования является рисковым. Проведя сравнительный анализ этим компаний, нами были выделены и рекомендованы для Сбербанка страховые компании АО «Согаз» и АО «АльфаСтрахование». Кроме того, страховой договор рекомендуем заключать с возможность перестрахования рисков в ведущих зарубежных страховых компаниях;
9. предложенные мероприятия способствуют снижению рисков кибербезопасности, уменьшению резервов капитала, увеличению дохода и в итоге к увеличению устойчивости развития российских коммерческих банков.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Аналитика Банка России по информационный безопасности. URL: <https://www.cbr.ru/information_security/analitics/> (дата обращения: 16.08.2022)
2. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. – 2014. – №5 (8)
3. АльфаСтрахование. Комплексное страхование финансовых институтов. URL: <https://www.alfastrah.ru/corporate/imushchestvo-predpriyatiy/kompleksnoe-strakhovanie-finansovykh-institutov/> (дата обращения 21.10.2022)
4. Angara прокомментировала новый отчет Центробанка о киберпреступности и мошенничестве. URL: <https://club.cnews.ru/blogs/entry/otchet_tsentrobanka_o_kiberprestupnosti_i_moshennichestve> (дата обращения: 11.05.2022)
5. Базельский Комитет по банковскому надзору. Повышение устойчивости банковского сектора // консультативный материал. – 2009. URL: <http://www.cbr.ru/content/document/file/36682/1.pdf> (дата обращения: 14.02.2022)
6. Банки утаивают каждую пятую успешную кибератаку. URL: https://[www.securitylab.ru/news/489810.php](http://www.securitylab.ru/news/489810.php) (дата обращения: 17.09.2022)
7. Вяткин В.Н. Риск-менеджмент: Учебник / В.Н. Вяткин, В.А. Гамза, Ф. В. Маевский. Люберцы: Юрайт, – 2016. 353 с.
8. В России появился центр компетенций кибербезопасности. URL: <https://rg.ru/2018/05/22/v-rossii-poiavilsia-centr-kompetencij-kiberbezopasnosti.html> (дата обращения: 11.05.2022)
9. Гавриченко Н. В. Международный опыт устойчивости развития коммерческого банка // Научно-методический электронный журнал «Концепт». – 2017. – Т. 18. – C. 37–42. URL: <http://e-koncept.ru/2017/770382.htm> (дата обращения 12.05.2022)
10. ГА ООН приняла российскую резолюцию о борьбе с киберпреступностью. URL: <https://ria.ru/20191228/1562965015.html> (дата обращения: 24.05.2022)
11. Дерюгин Р. А. Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. – 2019. – №2
12. Доклад Конгресса ООН по предупреждению преступности и уголовному правосудию. URL: https://[www.unodc.org/congress/](http://www.unodc.org/congress/) (дата обращения: 12.05.2022)
13. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646. URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 11.05.2022)
14. Ильюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет // Дис. канд. юрид. наук. Волгоград, – 2008. – С. 47–89
15. Информация о международном форуме «AntiFraud Russia». URL: <http://vipforum.ru/conferences/antifraud_russia/> (дата обращения: 11.05.2022)
16. Информация о мероприятии Cyber Security Day 2022. URL: https://runet-id.com/event/csd22/ (дата обращения: 11.05.2022)
17. Ингосстрах. Страхование от электронных и компьютерных преступлений. URL: <https://www.ingos.ru/corporate/banks/e-crimes/> (дата обращения: 21.10.2022)
18. Курило А.П. Управление рисками информационной безопасности: учебное пособие для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А. И. Толстой – 2-е изд., испр. М.: Горячая линия – Телеком, – 2015, 130 c.
19. Конвенция Совета Европы о киберпреступности ETS № 185
20. Коломасова Р. А. Мировые тенденции страхования информационных рисков и проблемы его внедрения в российскую практику // E-Scio. – 2019. – №6 (33)
21. Как интернет спасли от гибели. История SOPA и PIPA. URL: <http://www.cnews.ru/news/top/kak_internet_spasli_ot_gibeli.istoriya> (дата обращения: 11.05.2022)
22. Как Россия будет бороться с киберпреступностью. Путин назвал 5 шагов. URL: https://gov.cnews.ru/news/top/2018-07-06\_putin\_prizval\_strany\_nebyt\_egoistami\_v\_tsifrovoj (дата обращения: 17.08.2022)
23. Коммюнике совещания «Группы восьми». URL: [http://kremlin.ru/ supplement/3179/print](http://kremlin.ru/%20supplement/3179/print) (дата обращения: 12.05.2022)
24. Концепция стратегии кибербезопасности Российской Федерации. URL: [http://council.gov.ru/media/files/41d4b3dfbdb 25cea8a73.pdf](http://council.gov.ru/media/files/41d4b3dfbdb%2025cea8a73.pdf) (дата обращения: 12.05.2022)
25. Как Сбербанк борется с киберпреступностью. URL: [https://tass.ru/ ekonomika/5082607](https://tass.ru/%20ekonomika/5082607) (дата обращения 16.08.2022)
26. Как сберечь миллион: модель оценки киберрисков. URL: <https://bosfera.ru/bo/kak-sberech-million-model-ocenkikiberriskov> (дата обращения: 22.09.2022)
27. Киберпреступность и киберконфликты: Россия. URL: https://www.tadviser.ru/index.php/Статья:Киберпреступность\_и\_киберконфликты\_:\_Россия (дата обращения: 18.10.2022)
28. Лаврушин О. И. Деньги, кредит, банки // учебное пособие. – 2010. – 9-е изд., стер.
29. Маслаченков Ю. С. Устойчивость коммерческого банка // Бюллетень финансовой информации. – 1997. – №4
30. Марамыгин М. С., Шатковская Е. Г., Логинов М. П., Мокеева Н. Н., Прокофьева Е. Н., Заборовская А. Е., Долгов А. С., Банковское дело и банковские операции // учебник. – 2021. – C. 45
31. Мусина В. Ф. Байесовские сети доверия как вероятностная графическая модель для оценки экономических рисков // Тр. СПИИРАН, – 2013. – №25. С. 235–254
32. Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. Научный журнал. – 2013. – № 5 (10)
33. Ожегов С. И. Словарь русского языка. М. – 1953, 848 с.
34. Официальный сайт ПАО «Сбербанк». URL: [http://www.sberbank.ru/ ru/about/today](http://www.sberbank.ru/%20ru/about/today) (дата обращения: 10.02.2022)
35. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах. URL: <https://cbr.ru/Collection/Collection/File/32122/Attack_> 2019-2020.pdf (дата обращения: 15.06.2022)
36. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. URL: [https://www.cbr.ru/Collection/Collection/File/ 32189/Review\_of\_transactions\_2019.pdf](https://www.cbr.ru/Collection/Collection/File/%2032189/Review_of_transactions_2019.pdf) (дата обращения: 15.06.2022)
37. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год. URL: [https://www.cbr.ru/Collection/Collection/File/ 32190/Review\_of\_transactions\_2020.pdf](https://www.cbr.ru/Collection/Collection/File/%2032190/Review_of_transactions_2020.pdf) (дата обращения: 15.06.2022)
38. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: [https://cbr.ru/analytics/ib/operations\_survey\_ 2021/#i](https://cbr.ru/analytics/ib/operations_survey_%202021/#i) (дата обращения: 15.06.2022)
39. Официальный ежегодный отчет о киберпреступности за 2019 год. URL: https://[www.herjavecgroup.com/wp-](http://www.herjavecgroup.com/wp-)content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (дата обращения: 15.06.2022)
40. Отчет о воздействии за 2021 год. URL: <https://www.sberbank.com/> common/img/uploaded/files/pdf/normative\_docs/sber\_impact\_report\_for\_2021\_ru. pdf (дата обращения: 16.08.2022)
41. Петров А. Ю. Анализ кредитоспособности коммерческого банка // Бухгалтерия и банки. – 1999. – №7
42. Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности. URL: https://[www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступ](http://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступ) ности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd (дата обращения: 11.05.2022)
43. Политика ЦБ в сфере защиты информации (кибербезопасности). URL: [http://www.tadviser.ru/index.php/Статья:Политика\_ЦБ\_в\_сфере\_защиты\_ информации\_(кибербезопасности)](http://www.tadviser.ru/index.php/Статья:Политика_ЦБ_в_сфере_защиты_%20информации_(кибербезопасности)) (дата обращения: 11.05.2022)
44. Политика России в сфере международной кибербезопасности. URL: https://www.tadviser.ru/index.php/Статья:Политика\_России\_в\_сфере\_международной\_кибербезопасности (дата обращения: 11.05.2022)
45. Рейтинги финансовой надежности страховых компаний. URL: <https://www.raexpert.ru/ratings/insurance/?sort=rating&type=asc> (дата обращения: 21.10.2022)
46. Риски – понятие и виды. Классификация рисков. Основные характеристики рисков. URL: <http://www.grandars.ru/student/fin-m/vidy-riskov.html> (дата обращения: 12.09.2022)
47. Самые надежные страховые компании России – 2021. Рейтинг Forbes. URL: <https://www.forbes.ru/rating/435567-samye-nadezhnye-strahovye-kompanii-rossii-2021-reyting-forbes> (дата обращения: 21.10.2022)
48. СберСтрахование. Киберстрахование. URL: <https://sberbankins.ru/> products/cyber/ (дата обращения: 21.10.2022)
49. Сипратов Р. О. Страхование киберрисков в условиях функционирования банковских экосистем // Финансовая экономика. – 2022. – № 8. С. 134‑139
50. Суворова А. П. Риск-менеджмент // Поволжский государственный технологический университет. Йошкар-Ола: ПГТУ, – 2018. – 176 с.
51. Соколова А. А., Губина М.Е. Подходы к пониманию терминов «надежность», «стабильность» и «устойчивость» коммерческих банков и их сравнительная характеристика // Вестник Северо-Кавказского федерального университета. – 2018. – № 1 (64), – 137 с.
52. Сотрудничество России и США в киберпространстве. URL: <https://inosmi.ru/military/20170809/240006295.html> (дата обращения: 12.02.2022)
53. Согаз. Страхование киберрисков. URL: [https://www.sogaz.ru/corporate/ respons/cyberrisks/](https://www.sogaz.ru/corporate/%20respons/cyberrisks/) (дата обращения: 21.10.2022)
54. Степашин: кибертерроризм наносит России серьезный финансовый удар. URL: https://[www.kommersant.ru/doc/3482441](http://www.kommersant.ru/doc/3482441) (дата обращения: 16.09.2022)
55. Страхование кибер-рисков – Страхование от компании AIG в России. URL: https://[www.aig.ru/business/products/cyber-edge](http://www.aig.ru/business/products/cyber-edge) (дата обращения: 12.10.2022)
56. Сбербанк сообщил о мощнейшей в его истории DDoS-атаке. URL: <https://www.rbc.ru/business/21/01/2020/> 5e26a8a69a79475cb4f039a5 (дата обращения: 21.06.2022)
57. Сбербанк (информационная безопасность). URL: <http://www.tadviser>. ru/index.php/ (дата обращения: 03.06.2022)
58. Сколько стоит безопасность. Анализ процессов обеспечения ИБ в Российских компаниях. URL: <https://www>.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf (дата обращения: 12.08.2022)
59. Топ-5 главных рисков кибербезопасности в 2020 году. URL: [https://news.rambler.ru/other/43534097/?utm\_content=news\_media&utm\_medium =read\_more&utm\_source=copylink](https://news.rambler.ru/other/43534097/?utm_content=news_media&utm_medium%20=read_more&utm_source=copylink) (дата обращения: 14.06.2022)
60. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно- правовые меры борьбы // Дис канд. юрид. наук. Владивосток, – 2005. – 235 C.
61. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 18.02.2020) // Собрание законодательства РФ, 17.06.1996. – № 25, ст. 2954
62. Федеральный закон от 10.07.2002 № 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" // СПС «КонсультантПлюс»
63. Хакеры придут, все деньги заберут. URL: [https://www.banki.ru/news/ columnists/?id=9423714](https://www.banki.ru/news/%20columnists/?id=9423714) (дата обращения: 17.09.2022)
64. ЦБ фиксирует рост числа хакерских атак на банки РФ. URL: https:// www.m24.ru/news/tehnologii/24082022/493933 (дата обращения: 17.09.2022)
65. Allianz. Страхование Киберрисков. URL: [https://allianz.ru/2022/products/ business/bizotvet/cyberriskinsurance/](https://allianz.ru/2022/products/%20business/bizotvet/cyberriskinsurance/) (дата обращения: 21.10.2022)
66. Gable K.A. Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent / Kelly A. Gable // Vanderbilt Journal of Transnational Law. – 2010. – Vol. 43, № 1. – P. 57-118
67. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity
68. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management
69. Jones Sam Global alert to prepare for fresh cyber-attacks // Financial Times. – 2017
70. K. Najaf, M. I. Mostafiz, R. Najaf, Fintech firms and banks sustainability: Why cybersecurityrisk matters? // International Journal of Financial Engineering. – 2021. – Vol. 8, No. 2
71. Leukfeldt E.R. Organised cybercrime and social opportunity structures: a proposal for future research directions / E.R. Leukfeldt // The European Review of Organised Crime. – 2015. – № 2. – P. 91-103
72. Steve Morgan, Top 6 Cybersecurity Predictions And Statistics For 2021 To 2025 // Cybercrime Magazine. URL: <https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/> (дата обращения: 02.08.2022)
73. S. Treasury Department Office of Financial Research. Cybersecurity and Financial Stability: Risks and Resilience. – 2017