Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет
имени первого Президента России Б.Н. Ельцина»

Институт экономики и управления

Кафедра банковского и инвестиционного менеджмента

ДОПУСТИТЬ К ЗАЩИТЕ ПЕРЕД ГЭК

Зав. кафедрой _____

М.Я.Ходоровский _____
(подпись) (Ф.И.О.)
«_____»__июня_____2020 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

РЕКОНСТРУКЦИЯ МОДЕЛИ КИБЕРБЕЗОПАСНОСТИ В РОССИЙСКИХ БАНКАХ (НА ПРИМЕРЕ ПАО «СБЕРБАНК РОССИИ»)

Научный руководитель: Кондюкова Е.С., подпись
к.ф.н., доцент

Нормоконтролер: Федоренко М.О., подпись
ст. преподаватель

Студент группы ЭУМ-281001, Вигриянова Ю.С. подпись

Екатеринбург
2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире важнейшим конкурентным фактором в банковском секторе является внедрение инноваций и развитие информационных технологий. Однако данный процесс сопровождается также появлением новых видов мошенничества. Наибольший интерес для киберпреступников представляет финансовый сектор. Проблема развития киберпреступности является крайне актуальной и злободневной вследствие масштабов потерь, которые ежегодно несут кредитные организации по всему миру. Однако, на текущем этапе моделирование кибер-рисков, в том числе в банковском секторе, развито слабо ввиду новизны проблемы, отсутствия исторической практики борьбы с киберпреступностью на уровне отдельных организаций, а также сложности в анализе и оценке данного вида рисков.

В связи с этим, целью данной работы явилась реконструкция модели оценки кибер-рисков для российских коммерческих банков.

Для решения поставленной цели были определены представленные ниже задачи:

1. Выделение понятия «кибербезопасность», рассмотрение его основных характеристик;
2. Изучение основных подходов к обеспечению кибербезопасности в банковском секторе России и мира;
3. Сравнительный анализ особенностей кибер-рисков в российской и мировой практике;
4. Идентификация проблем, порождающих развитие киберпреступности, а также путей их решения;
5. Обзор методики оценки рисков кибербезопасности, применяемой в ПАО «СБЕРБАНК РОССИИ»;
6. Разработка рекомендаций по совершенствованию методологии оценки кибер-рисков российских коммерческих банков;

7. Практическое применение разработанного подхода к оценке на примере ПАО «Сбербанк России».

Предмет исследования – экономические отношения, возникающие в процессе оценки рисков кибербезопасности кредитных организаций.

Объект исследования – российский коммерческий банк ПАО «Сбербанк России».

В процессе написания работы были применены такие методы исследования, как теоретический анализ, системный подход, обобщение, сравнение, классифицирование, измерение, наблюдение, моделирование а также метод прогнозирования.

В процессе диссертационного исследования проанализированы работы, посвященные проблеме глобального развития киберпреступности, а также методам обеспечения кибербезопасности кредитных организаций. Весомый вклад в исследование данных вопросов внесли отечественные учёные: Тропина Т.Л., Дерюгин Р. А., Журавленко Н.И., Алпеев А.С., а также зарубежные: Leukfeldt E.R., Gable K.A., Boes S.

Научная новизна диссертационной работы заключается:

– в совершенствовании существующих моделей оценки рисков кибербезопасности и разработке авторского подхода к оценке на основании методик CRAMM и ГРИФ;

– в оценке экономической эффективности разработанной методологии на примере ПАО «Сбербанк России».

Практическая значимость данного исследования заключается в оценке текущего состояния киберпреступности в банковском секторе России и мира, а также в совершенствовании подхода к оценке кибер-рисков для российских коммерческих банков, который впоследствии может быть использован ими в практической деятельности для повышения кибербезопасности кредитной организации.

Теоретической и методологической основой написания работы явились учебное пособие Курило А.П. «Управление рисками информационной

безопасности»; учебники Черновой Г.В. «Страхование и управление рисками» и Вяткина В.Н. «Риск-менеджмент», законодательные акты США, Великобритании и Германии в области киберпреступности; Конвенция Совета Европы о киберпреступности; Доклады ООН, PwC, Kaspersky Lab, ФинЦЕРТА; а также статьи в различных периодических изданиях и новостных ресурсах; официальный сайт Центрального Банка Российской Федерации (Банка России), ПАО «Сбербанк России» и др.

Поставленные цель и задачи определили логику изложения и структуру выпускной квалификационной работы, которая состоит из введения, трёх глав, заключения и списка использованной литературы. В данной работе в первой главе рассматриваются теоретические аспекты управления кибер-рисками в коммерческом банке, обозреваются основные подходы к обеспечению кибербезопасности в банковском секторе России и мира, а также предлагаются пути решения проблем киберпреступности для отечественного банковского сектора. Вторая глава содержит анализ деятельности ПАО «СБЕРБАНК РОССИИ» в процессе формирования системы кибербезопасности. Третья глава содержит рекомендации по совершенствованию системы минимизации кибер-рисков в банковском секторе, а также апробацию результатов на примере ПАО «СБЕРБАНК РОССИИ». В заключении делаются основные выводы по итогам проделанного исследования.

1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ КИБЕР-РИСКАМИ В КОММЕРЧЕСКОМ БАНКЕ

1.1 ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ И ЕЕ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Понятие кибербезопасности является относительно молодым, поэтому не имеет общепринятого определения.

Согласно Федеральному закону «О безопасности» № 390-ФЗ безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [9].

Под кибератакой понимается предумышленно организованная совокупность действий с участием программно технических средств, направленная на нанесение экономического, технического или информационного ущерба [15].

Таким образом, опираясь на представленные определения, можно сформулировать понятие кибербезопасности, как комплекс действий стратегического характера, направленный на защиту от нанесения экономического, технического или информационного ущерба вследствие угроз, совершаемых с помощью программно технических средств, а также в результате ежедневной работы с информационными сетевыми технологиями.

Кибербезопасность обеспечивает защиту от возникновения убытков из-за действий злоумышленников, которые совершаются при помощи телекоммуникационных технологий, т.е. борется с проявлением кибер-рисков.

Основные характеристики кибер-рисков [55].

1) IT-природа. Кибер-риск характеризуется как информационно-технологическая категория, занимая определённое место в современной экономике и продолжая всё больше проникать в сферу экономической деятельности предприятий, коммерческих банков и других субъектов. Эволюция информационных технологий является главной предпосылкой развития кибер-рисков.

2) Объективность проявления. В связи с тем, что в современном мире практически любая деятельность на предприятиях и в банках сопровождается применением IT-технологий, то кибер-риск является объективным явлением, т.е. сопровождает все операции. В независимости от того, что ряд параметров кибер-риска зависит от субъективных управленческих решений, свойство его объективного проявления остаётся неизменным.

3) Вероятность возникновения. Сущность состоит в том, что в процессе финансово-хозяйственной деятельности предприятий (банков) кибер-риск может осуществиться, а может и нет. Вероятность того, что произойдет кибератака, определяется действием различных объективных и субъективных факторов, однако вероятностная принадлежность кибер-риска является его устойчивой характеристикой.

4) Непредсказуемость возникновения. Кибер-риск является сложно прогнозируемым и сопровождается трудностями в оценке из-за крайней скрытности киберпреступников. Мошенники владеют этим преимуществом, которое достигается применением различных механизмов шифрования и анонимности.

5) Ожидаемая неблагоприятность последствий. Риск в финансово-хозяйственной деятельности характеризуется и соотносится с уровнем возможных отрицательных последствий. Одной из основных характеристик кибер-риска является то, что он всегда сопряжен с какими-либо неблагоприятными результатами. Зачастую кибер-риски могут приводить не только к потере прибыли, но и капитала предприятия (банка), что в свою очередь является причиной банкротства.

6) Изменчивость уровня. Уровень кибер-риска не всегда одинаков. Он изменяется во времени и зависит от множества объективных и субъективных факторов (например, от качества программного обеспечения; уровня защиты от киберугроз предприятия (банка); квалификации персонала и т.п.).

7) Субъективность оценки. Несмотря на то, что кибер-риск является объективным по своей сути, его оценочный показатель — уровень риска — носит субъективный характер. Эта субъективность (неоднозначность оценки) характеризуется различным уровнем качества информации, её достоверности и полноты; квалификацией сотрудников отдела риск-менеджмента, их компетентности и опыта, а также другими факторами.

8) Трансграничность. Одной из важнейших характеристик кибер-риска является неограниченность в пространстве [26]. Таким образом, кибермошенник и пострадавшая от него сторона могут находиться на расстоянии тысяч километров, что не помешает совершению преступления.

В связи с тем, что киберпреступления охватывают широкий пласт общественных отношений, предусматривают использование различного оборудования и имеют множество способов совершения, существует несколько подходов к их классификации.

Конвенцией Совета Европы [3] виды киберпреступлений объединены в пять групп, представленных в таблице 1.

Таблица 1 – Классификация киберпреступлений в соответствии с Конвенцией Совета Европы[1]

Группа	Содержание
1	Преступления, направленные против компьютерных данных и систем
2	Противоправные деяния, связанные с использованием технологий
3	Правонарушения, связанные с содержанием данных или контентом
4	Нарушение авторских и смежных прав
5	Деяния, посягающие на общественную безопасность

[1] Составлено автором по: [3]

Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

Вторую группу составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами).

Правонарушения третьей группы связаны с содержанием данных или контентом.

Нарушение авторских и смежных прав относится к четвертой группе, выделение определенных видов преступлений в которой отнесено к законодательству конкретных государств.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в пятую группу киберпреступлений.

Также существует детализированная классификация киберпреступлений в зависимости от их совершения и криминальных целей, предложенная Д. А. Ильюшиным. [18] В перечень преступлений, совершаемых с использованием сети Интернет, включаются:

1) Неправомерное подключение;

2) Создание и распространение вредоносных программ;

3) Незаконное хранение, распространение, демонстрация информации, запрещенной к свободному обороту;

4) Нарушение авторских и смежных прав, а также незаконное использование чужого товарного знака;

5) Мошенничество в сфере услуг Интернет;

6) Хищение электронных реквизитов и сбыт поддельных кредитных либо расчетных карт;

7) Незаконное предпринимательство в сети Интернет;

8) Вымогательство;

9) Кибертерроризм.

Наиболее актуальным вопрос развития киберпреступности остается, в частности, для мирового банковского сообщества. Так, по статистике, в 2018 году суммарные убытки компаний во всем мире от кибератак достигли 1,5 трлн. $, а в 2019 году ущерб мировой экономике превысил 2 трлн. $.

Согласно статистике, приведенной ООН, ежегодный экономический ущерб от хищения онлайн-данных в банковском секторе составляет свыше 100 млрд. $. [33] К числу похищаемых данных относятся сведения о кредитных картах, паролях, логинах и других личных параметров клиентов кредитных учреждений.

Таким образом, для кредитных организаций очень важно обеспечение кибербезопасности и эффективное управление кибер-рисками, которое поможет снизить количество и вероятность угроз со стороны кибермошенников и свести к минимуму величину потерь от данных угроз.

Согласно докладу «Управление рисками и кибербезопасность», подготовленному компанией Price water house Coopers (PwC), ключевыми аспектами кибербезопасности являются [34]:

1) Определение уровня допустимого риска и пороговых значений ущерба;

2) Определение приемлемого остаточного риска и лимитов принятия риска;

3) Обеспечение методикой оценки рисков необходимой точности и финансовых значений оценки;

4) Установление прозрачной связи бизнес-процессов и критичных активов;

5) Распределение новых ролей и ответственности между компетентными специалистами;

6) Определение допустимых сроков закрытия выявленных рисков;

7) Определение ключевых индикаторов риска и установление порядка мониторинга рисков;

8) Определение положения кибер-рисков в системе корпоративного управления рисками;

9) Соответствие уровней принятия решений полномочиям лиц;

10) Регулярное предоставление лицам, принимающим решения, достоверной отчетности о кибер-рисках.

1.2 СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ

Термин «кибербезопасность» (согласно опубликованному Международной организацией по стандартизации и Международной электротехнической комиссией стандарту в области кибербезопасности ISO/IEC 27032:2012) характеризуется как безопасность в киберпространстве или как сохранение конфиденциальности, целостности, доступности и других важных свойств активов пользователей и организаций типа аутентичности, учетности и надежности в киберпространстве [11].

Кибератривы, существующие в киберпространстве и требующие защиты, подразделяются на физические (существуют в реальном мире) и виртуальные (существуют только в киберпространстве) [25].

В стандарте ISO/IEC 27032:2012 также охарактеризована взаимосвязь терминов «кибербезопасность», «сетевая безопасность», «безопасность приложений, «безопасность в Интернете» и «безопасность ключевых систем информационной инфраструктуры», которая отражена на рисунке 1.

Рисунок 1 – Взаимосвязь кибербезопасности с другими видами безопасности в соответствии со стандартом ISO/IEC 27032:2012 [11]

Согласно Концепции стратегии кибербезопасности Российской Федерации [43] кибербезопасность – это совокупность условий, при которых все составляющие киберпространства защищены от любой угрозы и нежелательного воздействия. При этом киберпространство – среда, образованная совокупностью коммуникационных каналов Интернета и других сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а информационное пространство – совокупность всей информационной деятельности человечества. Отсюда следует, что киберпространство является сложноорганизованной средой, имеющей трансграничный характер, и крайне сложно организовать регулирование его безопасности.

Согласно стандарту ISO/IEC 27032:2012, угрозы кибербезопасности можно подразделить на две большие группы [11]:

— угрозы для активов пользователя;

— угрозы для активов организации.

Угроза кибербезопасности из потенциальной возможности превращается в реальную кибератаку в случае, когда соответствующими уязвимостями воспользуется некоторый источник – субъект, которым может быть физическое лицо, материальный объект или физическое явление [13]. В случае реализации потенциальная угроза становится кибератакой, т.е. попыткой проникновения в информационную инфраструктуру, которая может неблагоприятно отразиться на кибербезопасности.

Таким образом, нельзя не отметить, насколько важно обеспечивать кибербезопасность в современной экономике, ведь потери могут быть просто колоссальны [27]. Борьба с киберпреступностью ведется на всех уровнях: международном, государственном, региональном, отраслевом и на уровне отдельно взятых субъектов (в частности, кредитных организаций).

Организация экономического сотрудничества и развития (ОЭСР), Совет Европы, Европейский союз (ЕС), Организация Объединенных Наций (ООН) и Интерпол играют важную роль в координации международных усилий, построении международного сотрудничества в борьбе с преступлениями в сфере высоких технологий.

Первое всестороннее исследование проблемы киберпреступности и уголовно-правовых мер по борьбе с ней в международном масштабе было предпринято ОЭСР, которая в период 1983-1985 гг. изучала возможности гармонизации норм, предусматривающих уголовную ответственность за киберпреступления [23]. Выводы ОЭСР изложены в докладе «Преступления, связанные с компьютером: анализ правовой политики».

14 декабря 1990 года Генеральной Ассамблеей ООН была принята резолюция [54], призывающая государства – члены ООН увеличить усилия по борьбе с компьютерной преступностью, модернизируя национальное уголовное законодательство, содействовать развитию в будущем структуры

международных принципов и стандартов предотвращения, судебного преследования и наказания в области компьютерной преступности.

В 1995 году была проведена первая международная конференция Интерпола по компьютерной преступности, подтвердившая обеспокоенность международного сообщества распространением киберпреступности. В последующем подобные конференции были проведены Интерполом в 1995, 1996, 1998 и 2000 гг.

В мае 2000 «Большая восьмерка» провела конференцию по киберпреступности, главной темой которой была координация усилий по борьбе с преступностью в сети Интернет. На этой встрече было выпущено коммюнике [42], декларирующее, что страны будут принимать соответствующие усилия для выработки совместного похода к высокотехнологичным преступлениям, типа киберпреступлений, которые могут серьезно угрожать безопасности глобального информационного сообщества.

Продуктом многолетних усилий Совета Европы стала принятая 23 ноября 2001 года в Будапеште Конвенция Совета Европы о киберпреступности [3]. Это один из важнейших документов, регулирующих правоотношения в сфере глобальной компьютерной сети и пока единственный документ такого уровня. Подготовка Конвенции была длительным процессом – за четыре года было составлено 27 проектов. Заключительная версия, содержащая преамбулу и четыре главы, датируемая 25 мая 2001 года, была представлена Европейской комиссии по борьбе с киберпреступностью на 50-м пленарном заседании 18-22 июня 2001 года.

И все же, несмотря на усилия, предпринимаемые на международном уровне, перечисленные выше, все они должны быть, прежде всего, связаны с действиями по реформированию уголовного законодательства на национальном уровне. Национальные и международные усилия должны дополнять друг друга, обеспечивая глобальное внимание к проблемам киберпреступности и обусловливая координацию шагов по борьбе с

киберпреступностью и унификацию национальных законодательств. В данном контексте особое внимание привлекают обсуждения проектов законов SOPA и PIPA в США [38].

В Российской Федерации уголовно-правовая борьба с киберпреступностью базируется на основании гл. 28 УК РФ, в которой преступления в сфере компьютерной информации выделены отдельным институтом [5]. Также в 2016 году президентом была утверждена Доктрина информационной безопасности РФ, которая содержит систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере [35].

На Международном конгрессе по кибербезопасности 2018 г. Владимир Путин озвучил список мер по киберзащите страны [39]. Перечень состоит из пяти основных шагов:

– выработка новых комплексных решений, включающих создание необходимых правовых условий, способствующих более эффективной работе спецслужб по реагированию на киберугрозы;

– создание системы автоматизированного обмена информацией об угрозах;

– базирование используемого в России программного обеспечения (ПО) и инфраструктуры на сертифицированных российских решениях;

– повышение уровня подготовки российских ИБ-специалистов;

– улучшение системы обмена данными о киберугрозах с другими странами.

В 2017 году Россия предложила проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности [53]. Генассамблея ООН приняла предложенную резолюцию по борьбе с киберпреступностью, несмотря на противодействие со стороны США [32].

Что касается научно-исследовательской стороны вопроса, в РФ пока отсутствуют комплексные исследования по кибертерроризму и киберпреступности как явлениям, охватывающим собой весь спектр

преступлений, совершаемых в глобальных информационных сетях. В основном работы российских ученых посвящены либо совершенствованию уголовной ответственности за совершение компьютерных преступлений, либо направлены на изучение криминологической характеристики компьютерной преступности в России.

Исследованию киберпреступности именно как глобального явления пока посвящены работы только зарубежных ученых, которые не затрагивают ни российских реалий, ни российское законодательство. В России на эту тему до настоящего времени появляются только научные статьи.

Однако последнее время можно наблюдать и некоторые практические шаги. Так, уже стала традиционной Неделя безопасного Рунета (в 2020 году проходила С 11 по 18 февраля), координатором которой выступает Центр безопасного Интернета РФ при поддержке РОЦИТ, РАЭК, Лаборатории Касперского, Координационного центра доменов .ru и .рф, а также Ростелеком-Солар. В организации и проведении мероприятия также принимают активное участие ведущие представители Интернет-индустрии, общественные и некоммерческие организации, а также представители государства [37].

Также ежегодно с 2010 года проводится Международный форум AntiFraud Russia, который является одним из главных событий в области борьбы с высокотехнологичным мошенничеством, прежде всего, в банковской и телекоммуникационной отрасли, а также в сфере электронной коммерции [36].

Сбербанк является одним из самых активных участников в борьбе с киберпреступностью в российском банковском секторе. Он предлагает новые проекты, открывает центры по кибербезопасности, также проводит форумы и конференции, соответствующие проблематике. Одним из ключевых его проектов является Международный конгресс по кибербезопасности, который проводится с 2018 года.

Таким образом, резюмируя вышесказанное, можно выделить основные существующие направления борьбы с киберпреступностью:

1. Международное сотрудничество. В связи с масштабом и глобальностью проблемы развития киберпреступности противодействовать ей ни одна страна в одиночку эффективно не может. Поэтому ключевым направлением борьбы с киберпреступностью является деятельность международных организаций (ОЭСР, ООН, Интерпол, ЕС и др.), сотрудничество отдельно взятых государств, разработка мер, а также заключение соглашений и договоров.

2. Борьба с киберпреступностью на уровне отдельного государства:

— Совершенствование законодательства. Развитие законодательной деятельности существенно отстает от развития информационных технологий, в том числе новых форм киберпреступности, поэтому органы власти концентрируют внимание на возникшей проблеме и разрабатывают (совершенствуют) нормативно-правовые акты, ужесточая санкции за киберпреступления и т.п.;

— Проведение различных конференций, форумов, создание условий для проведения научных исследований в области обеспечения кибербезопасности;

— Создание государственных центров кибербезопасности, способных разрабатывать новые подходы в области защищенных открытых информационных технологий и готовить высококвалифицированные кадры для компаний-лидеров мирового IT-рынка;

— Централизация управления кибербезопасностью, создание единого регулятора (в РФ – центр компетенций кибербезопасности) [31].

3. Борьба с киберпреступностью на уровне отдельной организации (банка):

— Совершенствование программного обеспечения, средств защиты (антивирусов и т.п.);

— Разработка моделей оценки кибер-рисков;

— Внедрение новых технологий, позволяющих снизить риск возникновения кибератак (блокчейн и т.п.);

— Страхование кибер-рисков;

— Повышение квалификации всех работников организации, деятельность которых связана с компьютерными технологиями, способными стать жертвой кибератаки.

1.3 СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ОСОБЕННОСТЕЙ КИБЕР-РИСКОВ В РОССИЙСКОЙ И МИРОВОЙ ПРАКТИКЕ

Киберпреступность, являющаяся настоящей эпидемией XXI века, затрагивает абсолютно все страны мира в том или ином масштабе. Больше всего от этой проблемы страдают развитые и развивающиеся страны. Потери, которые несет мировая экономика, в том числе мировой банковский сектор, просто колоссальны и продолжают ежегодно расти.

Так, исследовательская компания Cybersecurity Ventures в своём ежегодном отчете о киберпреступности за 2019 год прогнозирует, что к 2021 году киберпреступность будет стоить миру более 6 трлн.$ по сравнению с 3 трлн.$ в 2015 году [50]. Расходы на кибербезопасность в совокупности превысят 1 трлн.$ за 5-летний период с 2017 по 2021 год.

В 2019 году кибербезопасность стала широко обсуждаемой темой в политике. Отключение электроэнергии в Венесуэле, открытые военные операции в киберпространстве между конфликтующими государствами и целенаправленная дестабилизация Интернета в некоторых странах создали чрезвычайно опасные прецеденты, которые могут привести к социально-экономическому ущербу и дестабилизировать ситуацию в пострадавших государствах [68].

Аналитики антивирусной компании McAfee выделили основные факторы, послужившие причиной роста мирового уровня киберпреступности [48]:

— все более изощренные хакерские атаки;

— быстрое внедрение новых технологий киберпреступниками;

— упрощение совершения деяний в связи с появлением и развитием киберпреступности как услуги;

— расширение рынка киберкриминальных услуг;

— распространение криптовалют и др.

В отчёте об угрозах McAfee Labs выделили целевые секторы экономики, подверженные атакам кибермошенников, в 2018 – 2019 гг., опираясь на число зарегистрированных компанией нарушений. Результат представлен на рисунке 2. Также на основании числа зарегистрированных нарушений был выделен топ-10 векторов атак кибермошенников, представленный на рисунке 3.

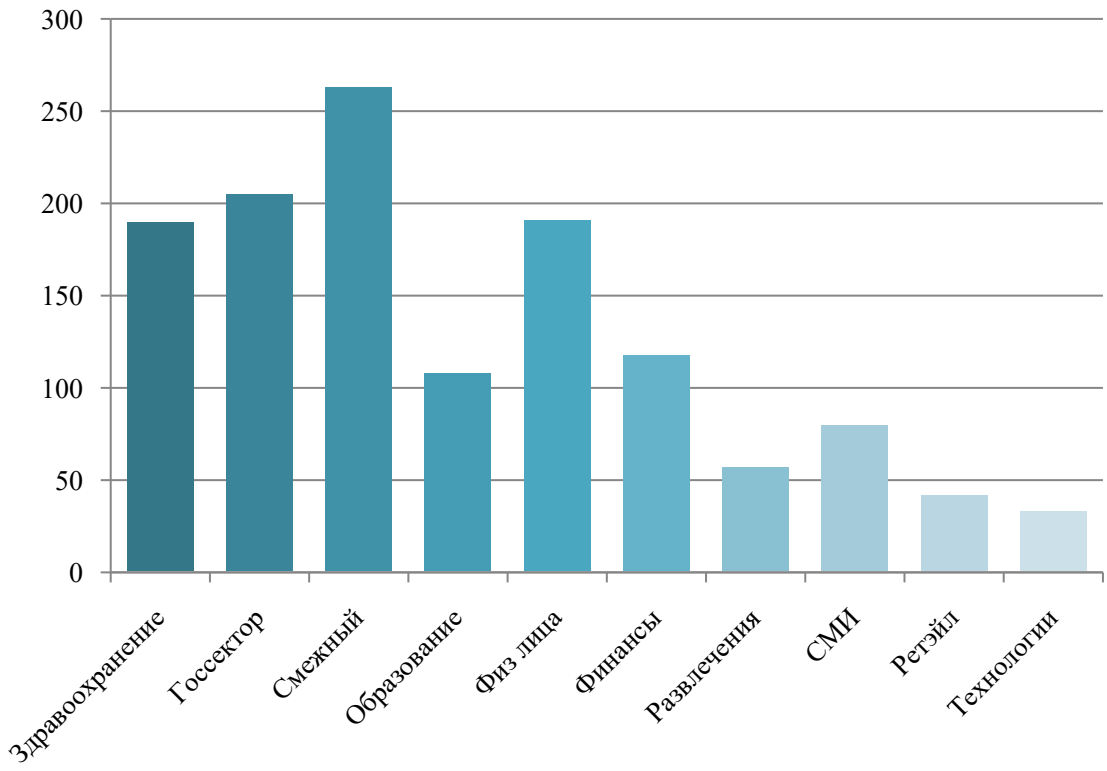

Рисунок 2 – Топ 10 целевых секторов киберпреступников

в 2018 –2019 гг. [48]

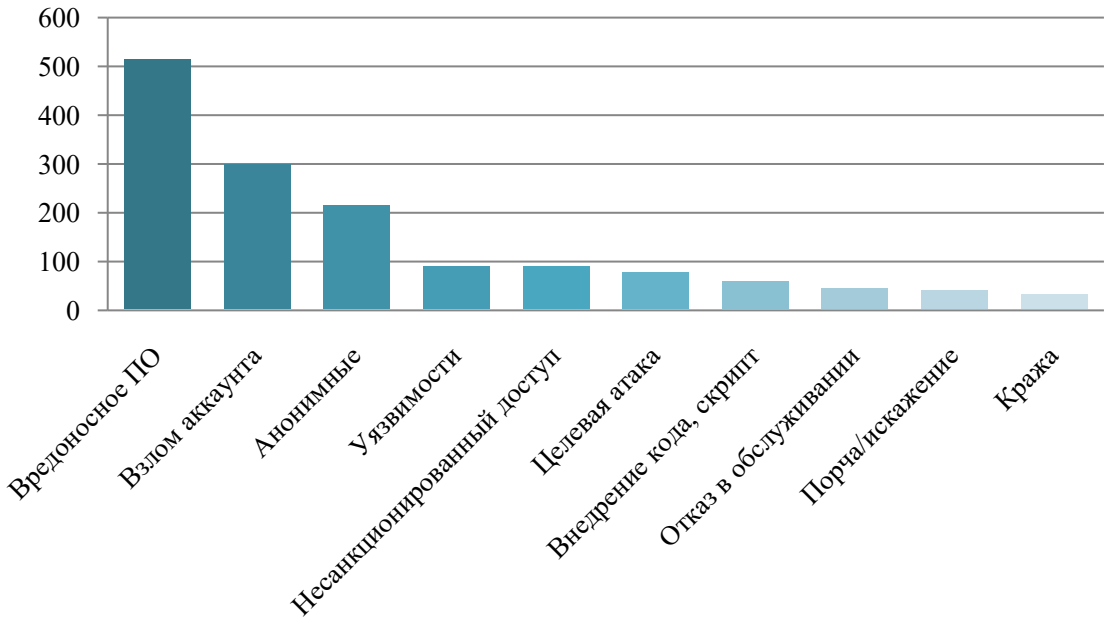

Рисунок 3 – Топ 10 векторов атак киберпреступников в 2018 –2019 гг. [48]

Для того, чтобы сравнить величину ущерба от киберпреступности в мире и в России, были рассмотрены крупнейшие утечки данных за 2019 год. Выделенные мировые инциденты представлены в таблице 2, а российские – в таблице 3.

Таблица 2 – Самые крупные утечки данных в мире в 2019 г.[2]

Дата	Ущерб
30.01.2019	2,2 млрд. уникальных имен пользователей и паролей свободно распространялись хакерами на форумах и торрент-трекерах (845 ГБ данных и около 25 млрд. записей).
25.02.2019	Был обнаружен дамб данных MongoDB размером 150 ГБ на незащищённом сервере, который был не запаролен. База содержала порядка 800 млн. адресов электронной почты, из которых 4 млн. содержали ещё и номера телефонов
24.05.2019	Крупная американская страховая компания First American Financial Corporation допустила утечку 885 млн. оцифрованных данных клиентов: банковские реквизиты, номера социального страхования, квитанции о транзакциях и т.д.
02.07.2019	На незащищенном сервере были обнаружены почти 2 млрд. пользовательских записей «Умного дома» китайской компании Orvibo,

[2] Составлено автором по: [64]

	которые содержали различную информацию – от кодов сброса учетных записей до паролей пользователей.

Окончание таблицы 2

Дата	Ущерб
22.11.2019	На незащищенном сервере обнаружено 1,2 млрд. пользовательских данных, которые содержат почти 50 млн. домашних и мобильных телефонных номеров и связанных с ними профилей в популярных соц. сетях: Facebook, Twitter, LinkedIn, Github, а также 622 млн. уникальных адресов электронной почты.

Таблица 3 – Самые крупные утечки данных в России в 2019 г. [2]

Дата	Ущерб
27.02.2019	За сумму подписки в 750 руб./сутки или 2 500 руб./месяц можно было получить доступ к базе 30 млн. автовладельцев, которые оплачивали парковку в Москве при помощи мобильного приложения Департамента транспорта Москвы или просто по номеру телефона (данные включали в себя госномера, VIN-номера, номера ПТС и СТС , даты, места и продолжительность стоянки)
23.09.2019	С сервера оператора фискальных данных (ОФД) «Дримкас» утекло 76 млн. записей, которые содержали полные реквизиты фискальных чеков, включая порядковые номера, дату и время, ФИО продавца, количество товара, их названия и цены
01.10.2019	В Интернете были обнаружены 20 млн. налоговых деклараций российских граждан, которые больше года были доступны без пароля на сервере Amazon Elasticsearch. Данные содержали ФИО, адреса, статусы резидентов, номера паспортов, телефонные номера, суммы налогов.
07.10.2019	Данные 9 млн. абонентов широкополосного доступа в Интернет от «Билайн» выложили в сеть. Сотрудники издательства, у которых подключен или был когда-то подключен интернет от «Билайна», нашли в базе свое полное ФИО, адрес, мобильный и домашний телефоны.

Проанализировав крупнейшие утечки данных в России и мире, можно сделать вывод о том, что кибератаки в России (по сравнению с мировыми) имеют меньшие масштабы, что можно оценить как положительный фактор. Однако, однозначных выводов делать нельзя, так как сравнение было достаточно условным и опиралось лишь на хищение данных, исследовался лишь 2019 год и для сравнения было взято мировое сообщество в целом, а не какая-либо конкретная страна.

В таблице 4 представлен сравнительный анализ уровня развития механизмов противодействия киберпреступности в России, США, Германии и Великобритании.

Таблица 4 – Современное состояние противодействия киберпреступности в странах мира [16]

Критерий	Опыт России	Опыт США	Опыт Германии	Опыт Великобритании
1	2	3	4	5
Понимание киберпреступности (законодательное)	Совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства [5]	Компьютерный шпионаж; несанкционированный доступ к информации; компьютерное мошенничество; умышленное или по неосторожности повреждение защищенных компьютеров; угрозы, вымогательство, шантаж, совершаемые с использованием компьютерных технологий и др. [1]	Все преступления, совершаемые с использованием оборудования для сбора, обработки и передачи информации или средств связи	Использование компьютера с намерением обеспечить доступ к программе или данным, содержащимся в любом компьютере, если этот доступ заведомо неправомочен; доступ к компьютеру, при помощи которого изменяются или уничтожаются программы или данные; данные копируются или перемещаются в место, отличное от того, где они содержатся.[2]
Нормативно-правовое регулирование	№ 149-ФЗ "Об информации, информационных технологиях и защите информации"; № 152 ФЗ "О персональных данных"; УК РФ; КоАП РФ	Закон "О мошенничестве и злоупотреблении с использованием компьютеров" (Computer Fraud and Abuse Act, CFAA); "Патриотический акт" (статьи о кибертерроризме)	УК Германии; Конвенция Совета Европы № 185 о киберпреступности; ФЗ "О защите персональных данных Германии"; Конвенция о защите частных лиц в отношении автоматической обработки персональных данных	Закон "О неправомерном использовании компьютерных технологий" (Computer Misuse Act); Положение "О частной информации и электронной связи"; Конвенция Совета Европы № 185 о киберпреступности; Закон "О защите данных" (Data Protection Act)
Конвенция № 185	Нет	Да		
Ответственность за киберпреступления	Уголовная, административная и гражданско-правовая ответственность. Максимальное наказание - до 7 лет лишения свободы	Предусматриваются денежные штрафы, тюремное заключение. Максимальное наказание - до 30 лет лишения свободы. Кроме того, в США действует система простого арифметического сложения наказаний за различные эпизоды в общем преступном деянии.	Предусматриваются денежные штрафы, тюремное заключение. Максимальное наказание - до 5 лет лишения свободы [6]	Предусматриваются следующие виды наказания: штраф; тюремное заключение. Максимальное наказание составляет 5 лет лишения свободы.

Как показали результаты анализа, законодательное понимание киберпреступности в каждой из стран совпадает и предполагает хищение данных посредством информационных технологий, а нормативно-правовое регулирование поэтапно развивается. Конвенцию Совета Европы о киберпреступности ETS № 185 подписали 46 стран, однако Россия к ним не присоединилась [3]. Что касается ответственности за киберпреступления, она схожа для различных стран: это штрафы и тюремные заключения, однако в США санкции носят более жесткий характер, чем в других странах.

Лаборатория Касперского (международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих киберугроз) регулярно проводит исследования в области современного мирового состояния киберпреступности и публикует на своем официальном сайте его результаты. В одном из последних отчетов «Kaspersky Security Bulletin: Статистика 2019» [69] был выделен топ 10 стран, подвергшихся атакам троянцев-шифровальщиков, который представлен в таблице 5 (при расчетах были исключены страны, в которых число пользователей «Лаборатории Касперского» менее 50 000).

Трояны-шифровальщики – это разновидность зловредных программ, достаточно распространенная в последнее время у кибермошенников, которая при попадании на компьютер шифрует ценные файлы таким образом, что их нельзя открыть, а за расшифровку создатели трояна требуют крупный выкуп.

Таблица 5 – Топ-10 стран, подвергшихся атакам троянцев-шифровальщиков [69]

	Страна	Доля атакованных пользователей среди всех пользователей продуктов «Лаборатории Касперского» в стране, %
1	Бангладеш	13,78
2	Узбекистан	7,20
3	Мозамбик	6,08
4	Туркменистан	4,23
5	Эфиопия	3,97
6	Непал	3,86
7	Афганистан	2,45
8	Вьетнам	2,34
9	Китай	1,94
10	Индия	1,91

За период с ноября 2018 года по октябрь 2019 года троянцы-шифровальщики атаковали 755 485 уникальных пользователей, в том числе 209 679 корпоративных пользователей и 22 440 пользователей, связанных с малым и средним бизнесом [69].

Также в отчёте была представлена статистика распределения по странам онлайн-источников атак на компьютеры пользователей, заблокированных продуктами «Лаборатории Касперского» (рисунок 4) и топ стран, в которых пользователи подвергались наибольшему риску заражения через интернет (таблица 6).

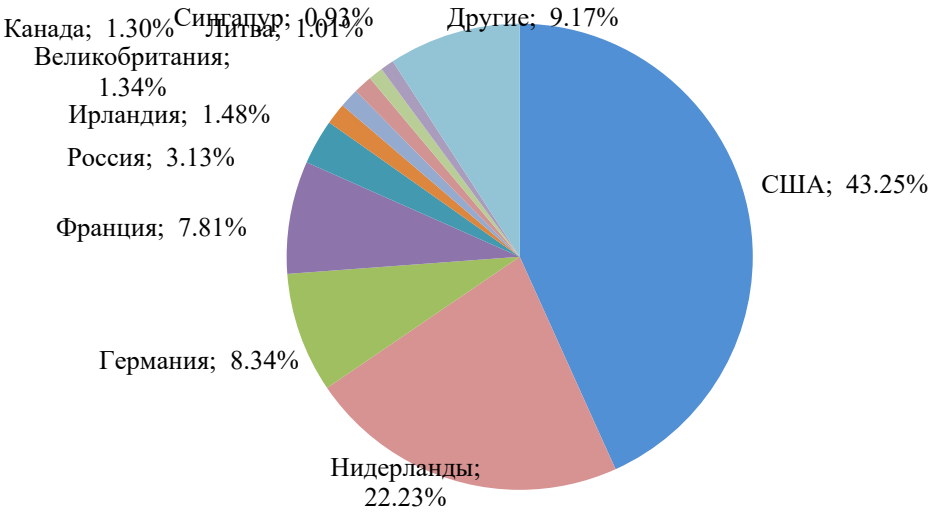

Рисунок 4 – Распределение источников веб-атак по странам, ноябрь 2018 г. – октябрь 2019 г. [69]

Таблица 6 – Топ-20 стран, подвергшихся наибольшему риску заражения через Интернет [69]

	Страна	Доля атакованных пользователей среди всех пользователей продуктов «Лаборатории Касперского» в стране, %
1	Алжир	33,02
2	Венесуэла	30,25
3	Тунис	29,50
4	Греция	26,07
5	Сербия	25,80
6	Бангладеш	24,95
7	Молдова	24,78
8	Азербайджан	24,74
9	Беларусь	24,52
10	Польша	24,13
11	Монголия	24,05
12	Филиппины	23,89
13	Марокко	23,87
14	Латвия	23,22
15	Катар	22,94
16	Вьетнам	22,57
17	Тайвань, провинция Китая	22,13
18	Франция	21,99
19	Португалия	21,97
20	Италия	21,96

За отчетный период решения «Лаборатории Касперского» отразили 975 491 360 атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира. При этом 90,83% от общего количества этих интернет-ресурсов были расположены всего в 10 странах.

В отчёте Лаборатории Касперского [69] представлена статистика банковских угроз, а также вредоносных программ для банкоматов и терминалов оплаты. На рисунке 5 отражено число пользователей, атакованных финансовым вредоносным ПО.

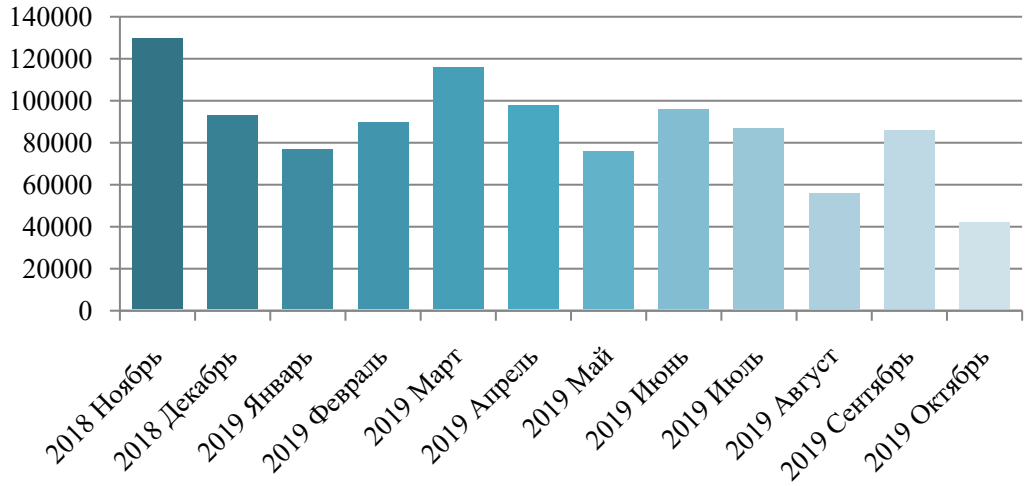

Рисунок 5 – Количество пользователей, атакованных финансовым вредоносным ПО, ноябрь 2018 г. – октябрь 2019 г. [69]

Чтобы оценить и сравнить степень риска заражения банковским вредоносным ПО, которому подвергаются компьютеры пользователей в разных странах мира, в каждой стране (количество пользователей «Лаборатории Касперского» ≥ 10 000) была подчитана доля пользователей продуктов «Лаборатории Касперского», которые столкнулись с этой угрозой в отчетный период, от всех пользователей в стране (таблица 7).

Таблица 7 – Топ-10 стран по доле атакованных пользователей банковским вредоносным ПО [69]

	Страна	Доля атакованных пользователей среди всех пользователей продуктов «Лаборатории Касперского» в стране, %
1	Беларусь	2,8
2	Южная Корея	2,6
3	Венесуэла	2,6
4	Китай	2,4
5	Греция	2,1
6	Мальдивские острова	2,0
7	Узбекистан	2,0
8	Камерун	1,9
9	Сербия	1,9
10	Афганистан	1,8

Таким образом, мировой рынок киберпреступлений активно развивается и приносит всё больше и больше потерь. Одной из ключевых целей кибермошенников по прежнему остаются кредитно-финансовые организации, и с каждым годом махинации преступников становятся всё более изощренными.

Ситуация с киберпреступностью в России совпадает с мировой и также имеет тенденцию постоянного увеличения. По словам главы Ассоциации юристов России Сергея Степашина, на сегодняшний день одной из популярных форм терроризма становится кибертерроризм [61]. «Ежегодный ущерб от киберпреступлений в России – в среднем $2 млрд. Для сравнения: в Бразилии – $8–15 млрд, в Индии – $4–8 млрд, в КНР – $25–26 млрд, в ЮАР – $0,6 млрд. Это серьезный финансовый удар по нашей стране», – считает Степашин. Также он отметил, что в России пора создать единый реестр лиц, представляющих киберугрозу.

По итогам 2019 года компания Positive Technologies, специализирующаяся на разработке программного обеспечения в области информационной безопасности, предоставила исследование, в котором отражены актуальные киберугрозы [28]. Ключевые выводы данного исследования:

- За 2019 год количество уникальных кибератак ежемесячно увеличивалось, и по итогам года на 19% превысило число кибератак в 2018 году.
- Наибольшее количество кибератак зафиксировано на госучреждения, промышленность, медицину, сферу науки и образования и финансовую отрасль. На эти отрасли пришлось более половины всех кибератак на юридические лица (54%).
- Доля атак на предприятия промышленной отрасли выросла до 10% против 4% в 2018 году. Преимущественно кибератаки производятся с использованием вредоносного ПО (90%).

– Доля целевых атак (по сравнению с массовыми атаками) выросла по сравнению с 2018 годом на 5 п.п. и составила 60%.

– Доля кибератак, направленных на хищение информации составила 60% против юридических лиц и 57% против частных лиц. Информация как и прежде представляет высокую ценность для кибермошенников. Наибольший интерес вызывают персональные данные, учетные записи и данные банковских карт.

– Количество заражений вредоносным ПО в 2019 году на 38% превысило аналогичный показатель 2018 года, что обусловлено не только модернизацией ВПО, но и способов его доставки.

– Одной из наиболее актуальных киберугроз для компаний по всему миру являются троянцы-шифровальщики. На их долю пришёлся 31% заражений ВПО среди юридических лиц.

Также в данном исследовании было проанализировано число атак на государственные и финансовые организации, промышленные и IT-компании. Результаты представлены на рисунке 6.

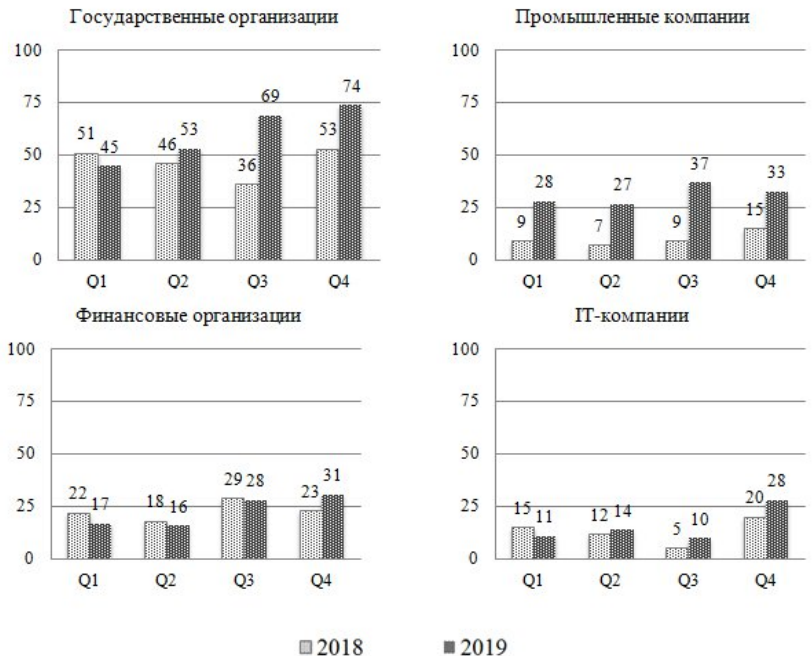

Рисунок 6 – Число атак на государственные и финансовые организации, промышленные и IT-компании за 2018-2019 гг.[3]

[3] Составлено автором по: [28]

Согласно оценке Positive Technologies количество кибератак на госсектор, промышленные компании и IT-компании ежеквартально растёт, однако в финансовом секторе наблюдается снижение числа кибератак в первых трёх кварталах, что является позитивным фактором для отечественной финансовой системы. Также в отчёте сказано, что большинство кибератак не предается огласке из-за репутационных рисков, в связи с этим оценить точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп.

В июне 2015 года начал свою работу Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) Банка России. ФинЦЕРТ является структурным подразделением главного управления безопасности и защиты информации Банка России (ГУБиЗИ).

По итогам 2019 года Банк России поделился аналитикой работы системы обработки инцидентов ФинЦЕРТ и Автоматизированной системы «Фид-АнтиФрод» [47]. Важно отметить, что усилия ЦБ по привлечению банков к обмену информацией и предоставлению отчетности были не напрасны – улучшилось качество и объём данных итоговой аналитической работы. Ключевые выводы, основанные на данном отчёте [66]:

– 69% всех мошеннических операций по переводу средств совершено с использованием социальной инженерии путем обмана клиентов, объем хищений составляет 5723,5 млн. руб., на фоне общего объема операций с использованием электронных средств платежей — 7,3 трлн. руб.;

– средняя стоимость хищения составляет: для физических лиц — 10 тыс. руб. (тенденция к множеству некрупных хищений), для юридических — 152 тыс. руб.;

– основное количество инцидентов связано с операциями по оплате товаров и услуг в интернете (CNP-транзакции) и методов социальной инженерии (мошенничества);

– в географических лидерах: Москва и Центральный федеральный округ, Санкт-Петербург, Уральский, Приволжский и Дальневосточный федеральные округа;

– доля объема операций без явного согласия клиентов составляет 0,0023%;

– банкам удалось возместить клиентам порядка 935 млн. руб., что составляет 15% от похищенных сумм.

Согласно ежегодному докладу компании Group-IB в 2019 году рынок кибермошенничества в России не только остановился в росте, но и показал падение. Он сократился почти на треть, до уровня 2016 года. В 2019 году объем киберпреступности составил 63,5 млн. долларов. Это на 27% ниже аналогичного показателя 2018 года, сообщили в пресс-службе Group-IB [68].

Также в отчёте Финцерта говорится о том, что в 2019 г. наблюдалось снижение количества попыток атак на организации кредитно-финансовой сферы. Интерес преступных групп, ранее активно атаковавших банки и другие организации кредитно-финансовой сферы России, сместился в сторону стран СНГ и дальнего зарубежья [49].

В связи с последними событиями во всём мире и активным развитием пандемии коронавируса вопрос кибербезопасности становится как нельзя актуальным. 13 марта 2020 года антивирусная компания Eset выпустила сообщение о том, как киберпреступники наживаются на коронавирусе [67].

Мошенники распространяют информацию от лица Всемирной организации здравоохранения (ВОЗ), призывая пользователей перейти по вредоносным ссылкам, тем самым похищая личную информацию и платежные данные, получая доступ к счетам жертв. Также злоумышленники прибегают к фейковым благотворительным акциям по поиску вакцины от коронавируса, а также к фейковым объявлениям о продаже медицинских масок и антисептиков для рук. Так, за февраль 2020 г. в Великобритании заработали на подобной кампании не менее 800 000 фунтов стерлингов ($1 млн.) [67].

Таким образом, сравнительный анализ текущего состояния рынка киберпреступности в России и мире показал, что в целом количество и качество кибератак продолжает ежегодно расти, сопровождаясь увеличением ущерба как для отечественной экономики, так и экономик других стран. Касаемо банковского сектора РФ, имеются некоторые положительные тенденции: в 2019 году величина ущерба значительно снизилась. Это связано с тем, что кредитные организации начали активно инвестировать денежные средства в укрепление своей информационной безопасности, а также с деятельность Банка России. Однако, несмотря на это, кибермошенники, обладая широкими знаниями в области компьютерных технологий, со временем смогут изобрести новые виды атак, спастись от которых не смогут даже самые защищенные банки. Поэтому кибербезопасность требует постоянного внимания и мониторинга.

1.4 АКТУАЛЬНЫЕ ПРОБЛЕМЫ УПРАВЛЕНИЯ КИБЕР-РИСКАМИ В БАНКОВСКОМ СЕКТОРЕ И ПУТИ ИХ РЕШЕНИЯ

Внедрение современных информационных технологий и инноваций, которое направлено на улучшение жизни человечества, а также процессы глобализации и интеграции параллельно с собой несут активное развитие новых методов мошенничества. Киберпреступность, как один из ключевых современных видов мошенничества, уже превратилась в глобальную международную проблему. Развитие киберпреступности происходит очень динамично, и постоянно возникают новые проблемы.

Основные проблемы, порождающие развитие киберпреступности:

– Сложность в определении источника угрозы – трудности в распознавании, откуда поступила атака и кто является её инициатором, из-за всё более изощренных методов мошенников;

– Сложность выработки мер противодействия – трудоёмкость выработки мер противодействия киберпреступности и оценки кибер-рисков из-за некомпетентности участников финансового рынка в вопросах кибербезопасности;

– Надежда на стандартные средства защиты – убежденность некоторых участников рынка в том, что стандартные средства защиты, такие как обновленный антивирус, последняя версия операционной системы, использование межсетевых экранов или средств предотвращения утечек (DLP), остановят злоумышленников на одном из этапов развития атаки [21];

– Транснациональность сети и отсутствие механизмов контроля – децентрализованная структура сети и отсутствие национальных границ в киберпространстве обусловили возможности для роста преступности;

– Количество пользователей сети Интернет – с увеличением числа пользователей возрастают следующие факторы риска: увеличивается зависимость общества от информационных технологий, его уязвимость к различного рода информационных посягательствам; увеличивается возможность использования сети для совершения преступлений;

– Автоматизация и быстрота использования – увеличение риска совершения множественных преступлений без особых финансовых и временных затрат, а также появление у мошенников возможности аккумулировать большую финансовую прибыль путём хищения небольших сумм у тысячи пользователей, что создаёт проблемы обнаружения преступлений и возбуждения уголовных дел;

– Анонимность сети Интернет – различные способы остаться незамеченным в Интернете зачастую несут за собой стремление к совершению противоправных действий;

– Несовершенство законодательства – нормативно-правовое регулирование в сфере киберпреступности развито слабо. Зачастую присутствует неопределенность в выделении элементов состава

киберпреступления, так как при точном их описании в законодательных актах это приведет к снижению универсальности применения закона, а также снижению возможности охвата быстро появляющихся новых видов кибератак.

– Напряженная политическая обстановка в мире – нежелание некоторых отдельных государств сотрудничать по вопросам кибербезопасности [60];

– Сокрытие фактов о произошедших кибератаках – стремление организаций не разглашать информацию о том, что они стали жертвой кибермошенников, и уровне потерь. Большинство организаций не хотят терять свою деловую репутацию, поэтому стараются скрыть информацию о совершенных преступлениях [30]. Отсюда возникают проблемы обнаружения и предотвращения таких преступлений.

– Неэффективность работы органов внутренних дел, включающая несоответствие уровня оснащения правоохранительных органов современными технологиями уровню кибермошенников; неразвитость методологии цифровой криминалистики; а также неэффективное взаимодействие с государством, обществом и учреждениями в сфере кибербезопасности [17].

– Нехватка квалифицированных кадров – в 2020 году число незаполненных вакансий в сфере кибербезопасности вырастет: если в 2014 году их число составляло 1 млн., то к 2020 году — 3,5 млн. дефицит квалифицированных кадров в этой области вызывает серьезную озабоченность специалистов [63].

Пути решения рассматриваемых проблем, предлагаемые автором, представлены в таблице 8.

Таблица 8 – Основные проблемы, порождающие развитие киберпреступности, и пути их решения [4]

№	Проблема	Пути решения
1	2	3
1	Сложность в определении источника угрозы	Инвестиции в исследования в области кибербезопасности, выделение грантов, всяческое стимулирование IT-специалистов
2	Анонимность сети Интернет	
3	Сложность выработки мер противодействия	Обучение финансистов и экономистов основам кибербезопасности, повышение их компетентности в вопросах защиты от кибератак; увеличение числа и качества проводимых форумов
4	Надежда на стандартные средства защиты	
5	Транснациональность сети и отсутствие механизмов контроля	Партнерство крупнейших Интернет-ресурсов с целью пресечения кибератак
6	Быстро возрастающее количество пользователей сети Интернет	Повышение IT-грамотности пользователей Интернета, дабы избежать киберпреступлений вследствие невнимательности, незнания и прочих человеческих факторов
7	Автоматизация и быстрота использования	
8	Несовершенство законодательства	Ужесточение наказания за киберпреступления; классификация наказаний в зависимости от видов кибератак; внедрение новых нормативно-правовых актов по рассматриваемой проблеме
9	Напряженная политическая обстановка в мире	Стремление к международному сотрудничеству, создание благоприятных условий для партнерства с другими государствами, проведение международных форумов/совещаний/встреч
10	Сокрытие фактов о произошедших кибератаках	Ужесточение санкций за сокрытие информации о произошедших кибератаках, поддержка организаций-жертв в СМИ для снижения риска потери деловой репутации
11	Неэффективность работы органов внутренних дел	Стимулирование правоохранительных органов к расследованию киберпреступлений, обеспечение их надлежащим оборудованием и навыками, предоставление возможности получить доп. квалификацию сотрудникам
12	Нехватка квалифицированных кадров	Формирование культуры поддержки безопасности и повышения ценности выполняемых специалистами по кибербезопасности функций, инвестиции в сотрудников, получение ими доп. квалификации и переобучение

Таким образом, для борьбы с киберпреступностью необходимо сотрудничать с другими государствами, вырабатывая международные методы противодействия. На данный момент Россия разрабатывает различные документы для международного сотрудничества, в частности

[4] Составлено автором

внедрила конвенцию о киберпреступности, учитывающую Конвенцию ООН против коррупции, Конвенцию ООН против транснациональной организованной преступности, Конвенцию Совета Европы о киберпреступности, а также ряд других антитеррористических конвенций. России необходимо продолжать стремиться к международному сотрудничеству, выдвигая свои предложения и поддерживать инициативы других стран, несмотря на напряженную политическую обстановку.

Также немаловажна борьба с киберпреступностью на государственном уровне. Основой служит, конечно же, разработка и внедрение новых законов, а также внесение изменений в существующие нормативно-правовые акты. Рекомендуется ужесточить наказания за киберпреступления, максимальное из которых на данный момент – до 7 лет лишения свободы. Также рекомендуется ужесточить санкции за сокрытие информации о совершенных кибератаках.

Государству или определенным компаниям необходимо периодически проводить мероприятия по увеличению уровня IT-грамотности пользователей Интернета, чтобы избежать киберпреступлений вследствие человеческих факторов. Организациям, в частности коммерческим банкам, следует обратить внимание на обучение финансистов и экономистов основам кибербезопасности, повышение их компетентности в вопросах защиты от кибератак.

Важно проведение различных конференций, форумов и повышение их качества. Необходимо привлекать топовых IT-специалистов на такие мероприятия, чтобы они могли поделиться своим опытом.

Коммерческим банкам для обеспечения кибербезопасности рекомендуется разрабатывать экономико-математические модели прогнозирования направлений кибератак и оценки потенциального ущерба (рисков). Также необходимо разрабатывать собственные системы защиты информации, оптимизируя процессы обмена файлами внутри банка, и использовать специальные системы идентификации, определяющие наличие

прав на доступ информации для защиты внутренней сети банка наряду с мощными антивирусами и специальными аппаратными модулями безопасности. Популярными разработчиками банковских защитных систем можно назвать таких лидеров рынка с обширным опытом в данной сфере как Group IB, Лаборатория Касперского, Cisco и Data Protection Systems.

Несмотря на сложные системы защиты, у банка не всегда получится отклонить хакерскую атаку. В случае, если кибератака все же нанесла урон, затраты банка на устранение ее последствий колоссальны и доходят до миллионов и, в более редких случаях, до миллиардов долларов США. В них входит множество расходов, таких как: расходы на IT-расследование; восстановление системы; услуги юристов; восстановление репутации и др.

В таком случае эффективным экономическим инструментом является *страхование кибер-рисков.* Первой компанией, которая представила страхование рисков киберугроз на российском рынке, стала AIG в России (ПАО «АИГ»), обладающая обширным опытом и экспертизой урегулирования страховых случаев в данной сфере [62]. Однако, кибер-страхование не особо развито на российском рынке, его предлагает всего несколько компаний, несмотря на то, что в рамках правительственной программы «Цифровая экономика» было выдвинуто предложение о том, чтобы сделать страхование кибер-рисков обязательным для стратегических отраслей экономики, к которым относится и банковская сфера.

Таким образом, управление кибер-рисками в российском банковском секторе на современном этапе развито слабо. Необходимо усовершенствовать подход к оценке данного вида рисков, законодательную базу, а также методы управления. Ведь то, как стремительно растёт количество киберпреступности и какие потери за собой несёт, становится одной из главных проблем для современных коммерческих банков, которую нужно решать незамедлительно.

2 АНАЛИЗ ДЕЯТЕЛЬНОСТИ ПАО «СБЕРБАНК РОССИИ» В ПРОЦЕССЕ ФОРМИРОВАНИЯ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

2.1 ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКАЯ ХАРАКТЕРИСТИКА ПАО «СБЕРБАНК РОССИИ»

Коммерческий банк ПАО «Сбербанк» является крупнейшим банком Российской Федерации и стран СНГ [51]. Основным акционером и учредителем Сбербанка выступает Центральный банк Российской Федерации, который владеет 50% уставного капитала плюс одна голосующая акция. Другими акционерами банка являются международные и российские инвесторы. Ключевые характеристики Сбербанка представлены в таблице 9.

Таблица 9 – Основные характеристики ПАО «Сбербанк» на 2020 год[5]

Дата основания банка	Количество территориальных банков	Количество подразделений в 83 субъектах федерации	Активы (на 02.2020)	Чистая прибыль (по итогам 2019 г.)
1841 год	11	14 200	28 956 млрд. руб.	870,1 млрд. руб.

Сбербанк основан в 1841 году, прошел значительный путь развития и на сегодняшний день представляет собой лидера российского банковского сектора по общему объему активов. Банк является основным кредитором российской экономики и занимает крупнейшую долю на рынке вкладов.

Одной из главных особенностей Сбербанка является его способность к переменам и движению вперед, ведь он является также лидером по

[5] Составлено автором по: [51]

внедрению инноваций, современных технологий и всегда оказывается на шаг впереди.

Согласно годовому отчёту, по состоянию на 2019 год на долю лидера российского банковского сектора приходится 30,5% совокупных банковских активов, а также 41% кредитного портфеля физических лиц. Доля Сбербанка в ключевых сегментах финансового рынка РФ на 2019 г. (в сравнении с предыдущим годом) представлена в таблице 10.

Таблица 10 – Доля ПАО «Сбербанк» в основных сегментах российского финансового рынка, %

	2018	2019
Активы	30,4	30,5
Кредиты частным лицам	41,4	41,0
Кредиты корпоративным клиентам	32,7	31,4
Вклады частных клиентов	45,1	43,8
Средства корпоративных клиентов	23,1	22,0

С целью сделать обслуживание клиентов более удобным, технологичным и современным, Сбербанк постоянно совершенствует возможности дистанционного управления счетами клиентов. В банке создана система удаленных каналов обслуживания, в которую входят [51]:

– мобильные приложения «Сбербанк Онлайн2 для смартфонов (более 50 млн. активных пользователей);

– веб-версия «Сбербанк Онлайн» (14,5 млн. активных пользователей);

– SMS-сервис «Мобильный банк» (более 76 млн. активных пользователей);

– одна из крупнейших в мире сетей банкоматов и терминалов самообслуживания (более 100 тыс. устройств).

В декабре 2018 г. зампред правления Сбербанка Лев Хасис огласил, что компания планирует построить экосистему вокруг Сбербанка, объединяющую финансовые и нефинансовые услуги [44]. Сбербанк активно участвует в совместных предприятиях с другими компаниями, такими как Яндекс.Маркет, Rambler.group, Mail.ru Group и др. Так появились интернет-магазины «Беру» и «Bringly», онлайн-кинотеатр Окко и другие digital-продукты и сервисы Rambler, Фудплекс, сервис «Работа.ру», «Корус Консалтинг СНГ», «DocDoc». Также банк имеет собственные разработки. Это «ДомКлик», «Поговорим» и «СберМобайл», «SberCloud», «Сбербанк-АСТ», «Сбер решения», «Bi.Zone» и др.

Таким образом, можно отметить, что практически все новые проекты, в которые вкладывает средства Сбербанк, являются Интернет-платформами и сервисами или виртуальными продуктами. Это связано с актуальностью и популярностью данных продуктов, однако сопровождается рядом рисков, ключевым из которых является риск киберпреступности.

Приложение «Сбербанк Онлайн» для смартфонов является самым популярным среди всех российских банковских мобильных приложений [58]. С его помощью клиенты могут контролировать состояние своих карт, вкладов, счетов; просматривать операции и получать выписки по счетам; открывать вклады и получать информацию по ним; получать информацию об имеющихся кредитах и оформлять их; осуществлять переводы и различного рода платежи и т.д.

Приложение «Сбербанк Онлайн» имеет встроенную антивирусную систему, что характеризует его как относительно безопасное, однако огромное количество пользователей и их финансовых ресурсов делает приложение привлекательной целью для хакеров и мошенников, которые способны обойти защиту или ввести в заблуждение пользователей и произвести хищение их денежных средств.

2.2. КОМПЛЕКСНЫЙ АНАЛИЗ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ БАНКА

Коммерческим организациям, в особенности – 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 частности мелкие банки.

Поэтому Центральный Банк РФ занимается контролем и регулирует обеспечение кибербезопасности в коммерческих банках России [52]. Ключевые меры Банка России по обеспечению кибербезопасности в отечественном кредитно-финансовом секторе представлены в таблице 11.

Таблица 11 – Деятельность ЦБ РФ по обеспечению кибербезопасности банковского сектора за период 2016-2019 гг. [6]

Год	Меры
2016	• Публикация рекомендаций по обеспечению информационной безопасности (ИБ) в части предотвращения утечек информации (осуществляются на добровольной основе); • Создание лаборатории для защиты банков от киберугроз на базе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT); • Масштабная проверка безопасности онлайн-банкинга; • Блокировка сайтов с вредоносным контентом, относящихся к сфере финансовых рынков, на основе данных, полученных от ЦБ.
2017	• Разработка единой стратегии информационной безопасности банков; • Проведение проверок систем ДБО; • Создание центра безопасности для средних и малых банков; • Внедрение Госстандарта защиты информации для банков ГОСТ Р 57580.1-2017; • Внедрение системы обмена информацией о кибератаках на банки; • Разработка стандартов по аутсорсингу кибербезопасности; • Введение поправок в положение ЦБ, включающих расширение списка требований при переводе денежных средств в Интернете. • Ужесточение требований к ИБ кредитных организаций (разработка политики взаимодействия с аутсорсерами и постоянный мониторинг); • Поправки к законопроекту о противодействии хищению денежных средств; • Содействие во введении в российских учебных заведениях образовательных программ по кибербезопасности в финансовой сфере; • Предложение ЦБ о включении ответственных за ИБ и ИТ в советы директоров публичных компаний.

[6] Составлено автором по: [52]

Окончание таблицы 11

Год	Меры
2018	• С 1.07.18 – банки обязаны сообщать о хакерских атаках в ЦБ (ранее это происходило на добровольной основе); • Изменение формы отчетности, предоставляемой банками в ЦБ, отражающей экономические показатели, связанные с кибератаками (обязанность отражать величину ущерба); • Создание «песочницы» и её тестирование; • Открытие Центра компетенции по противодействию нелегальной деятельности на финансовом рынке; • Определение перечня угроз безопасности для биометрических данных; • Внедрение нового стандарта по ИБ (СТО БР ИБФО-1.5-2018); • Формирование нового департамента ИБ ЦБ (разделение Главного управления безопасности и защиты информации на 2 подразделения); • Обязанность банков проверять устройства клиентов при переводе денег; • Разработка законопроекта о защите информации в некредитных финорганизациях; • Заключение соглашения о взаимодействии в сфере ИБ с несколькими странами ЕАЭС; • Регулярное внесение в антифрод-систему счетов мошенников для вывода денег.
2019	• Предложение создать аутсорсинговую компанию под патронажем ЦБ, которая будет осуществлять ИБ-защиту небольших банков; • Ужесточение требований к банкам по защите информации (Положение № 683-П); • Реализация пилотного проекта по подтверждению электронной почты банковских клиентов; • Внедрение нового наказания для банков (штрафы и усиление надзора) за плохую киберзащиту (анализ риск-профиля по уровню ИБ); • Внедрение документа «Основные направления развития ИБ кредитно-финансовой сферы на период 2019–2021 годов»; • Штрафование первых двух банков за отсутствие систем антифрода (10.10.2019); • Выявление в ходе проверок более 700 нарушений в сфере ИБ; • Утверждение требований к разработке и оценке соответствия ГОСТу ПО и мобильных приложений.

Вопреки всем усилиям количество кибератак растёт ежегодно, однако кредитные организации постепенно учатся им противостоять. Сбербанк, как крупнейший банк в России, Центральной и Восточной Европе, является очень привлекательной целью для кибермошенников. Известные случаи кибератак на ПАО «Сбербанк» консолидированы в таблице 12.

Таблица 12 – Последствия известных случаев кибермошенничества в ПАО «Сбербанк» за период 2013-2019 гг. [7]

Год	Кибератака	Последствия
2013	Массовые атаки на клиентов «Сбербанк Онлайн»; вирусные атаки; DDoS-атаки на инфраструктуру; скимминг	Предотвращён ущерб на сумму более 6 млрд. руб. Информация о потерях банка недоступна.
2014	Массовые атаки на клиентов; вирусные атаки; фишинг; скимминг; DDoS-атаки	Предотвращён ущерб со счетов клиентов на сумму более 2,9 млрд. руб., а также от скимминга – около 4,7 млрд. руб. Ущерб от атак: 16.12.2014 – 300 млрд. руб., 300 млрд рублей, 22.12.2014 —1,3 трлн. руб.

[7] Составлено автором по: [51, 57, 65]

Окончание таблицы 12

Год	Кибератака	Последствия
2015	Атаки, применяемые с технологией социальной инженерии; DDoS-атаки; фишинг; скимминг	Предотвращён ущерб на сумму свыше 4,8 млрд. руб.
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	Предотващён ущерб на сумму 40 млрд. руб. Ущерб от фишинговых атак свыше 5 млн. руб.
2018	Социальная инженерия; DDoS-атаки; взлом банкоматов; 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	Социальная инженерия; DDoS-атаки; взлом банкоматов; 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.

В таблице представлена хронологическая информация по произведенным кибератакам на ПАО «Сбербанк» за период 2013-2019 гг.

Объективно оценить данные таблицы достаточно непросто, так как информация неполная. Банки не стремятся раскрывать данные о совершаемых кибератаках и, тем более, о последствиях и потерях. Это представляет собой одну из главных проблем развития киберпреступности в России.

Также в январе 2020 г. Сбербанк столкнулся с самой масштабной DDoS-атакой, которая была в 30 раз мощнее, чем самая мощная атака за всю историю Сбербанка. Она была осуществлена с помощью автономных устройств IoT (Internet of Things — интернет вещей). Сбербанк отразил атаку без последствий [59].

Таким образом, можно отметить, что Сбербанк имеет высокий уровень кибербезопасности и не только защищает себя и своих клиентов, но также способствует национальному и мировому сотрудничеству в борьбе с киберпреступностью. Опираясь на интервью заместителя председателя правления ПАО «Сбербанк» Станислава Кузнецова [40], были выделены основные направления борьбы с киберпреступностью в ПАО «Сбербанк»:

1. Защита CORE-систем – ключевых, корневых систем, в которых хранится вся информация о счетах и клиентах, методом внедрения самых современных технологий и процессов управления безопасностью. Существует несколько периметров, и любые попытки проникнуть в инфраструктуру Сбербанка отражаются на разных уровнях защиты.

2. Изменение подходов к разработке продуктов. Раньше разрабатывались продукты и затем производился анализ их безопасности, а сейчас – при обсуждении концепции продукта для программистов изначально устанавливаются некие безусловные принципы безопасности, которые реализуются в программном коде;

3. Фокусировка на защите клиентов путём успешной работы центра фрод-мониторинга, который при проведении нестандартных операций связывается с клиентом и помогает избежать мошеннических действий со стороны киберпреступников. Эффективность центра фрод-мониторинга Сбербанка имеет один из лучших показателей в мире – около 97% мошеннических операций хеджируются и пресекаются;

4. В случае проведения кибератаки проведение исследования с целью выявления мошенников;

5. Внедрение принципов киберкультуры, проведение учений среди сотрудников, ведение разъяснительной работы;

6. Работа Операционного центра кибербезопасности (Security Operation Center), который в круглосуточном режиме мониторит все киберугрозы вокруг систем Сбербанка;

7. Наличие сертификата соответствия международному стандарту по информационной безопасности от Британского института стандартов — BSI (Сбербанк – первый банк РФ, получивший данный сертификат);

8. Запуск работы Академии кибербезопасности, которая проводит обучение не только среди сотрудников Сбербанка, но и других кредитных организаций и правоохранительных органов;

9. Соглашения с ведущими учебными заведениями страны и помощь в подготовке студентов, способных разбираться в вопросах кибербезопасности;

10. Наличие дочерней компании Bi.Zone, которая образована для создания продуктов в области кибербезопасности, проведения экспертизы и расследования, тестирования систем Сбербанка на предмет выявления уязвимостей, разработки рекомендаций по хеджированию кибер-рисков. Компания Bi.Zone сотрудничает с Интерполом;

11. Организация Международного конгресса по кибербезопасности при поддержке Ассоциации банков России и АНО «Цифровая экономика». Впервые конгресс прошёл в 2018 году, планируется его ежегодное проведение.

Таким образом, проанализировав основные направления борьбы с киберпреступностью, можно сделать вывод о том, что Сбербанк тратит огромное количество средств на обеспечение кибербезопасности и благодаря этому имеет один из наименьших уровней ущерба от кибермошенников среди коммерческих банков России. Издержки на кибербезопасность занимают значительную статью расходов в финансовой политике коммерческого банка.

2.3. АНАЛИЗ МОДЕЛИ ОЦЕНКИ РИСКОВ КИБЕРБЕЗОПАСНОСТИ БАНКА

Одним из ключевых направлений борьбы с киберпреступностью в современном банковском секторе является разработка экономико-математических моделей прогнозирования направлений кибератак и оценки потенциального ущерба (рисков).

Моделирование кибер-рисков организаций, в частности коммерческих банков, развито слабо ввиду новизны проблемы и сложности оценки таких рисков. Банки не стремятся раскрывать информацию об имеющихся средствах защиты от кибермошенников, а также о произошедших кибератаках и причиненном ущербе.

Модель оценки рисков кибербезопасности Сбербанка постоянно совершенствуется, чтобы быть актуальной и действенной в связи со стремительной эволюцией кибератак, которые с каждым днем становятся все изощреннее и мощнее.

Прототип, на котором базируется текущая модель оценки кибер-рисков Сбербанка был представлен в конце 2017 года Надеждой Симачевской, менеджером по методологии кибербезопасности Сбербанка России [41].

Несмотря на то, что существует множество моделей оценки рисков, специалисты Сбербанка решили разработать собственную методику оценки кибер-рисков, потому что при выборе подходящего метода столкнулись с рядом проблем:

– все методики слабо адаптируются к большому объёму обрабатываемой информации и значительному количеству банковских процессов (обусловлено масштабами, ведь Сбербанк – крупнейший банк СНГ);

– нецелесообразность использования подходов, требующих оценки стоимости активов, потому что ценность не всякого актива банка можно оценить количественно (например, сложно оценить, какова ценность продукта «Сбербанк Онлайн»), а также потому, что ценность таких активов изменяется ежедневно, и оценить эту динамику достаточно непросто;

– неуниверсальность использования методов сценарного анализа, которые подразумевают, что вероятность реализации инцидента равна произведению вероятностей всех событий, которые в итоге привели к нему. Данные модели подходят не для всех видов риска. Так, они эффективны для

анализа сбоев и нарушения доступности, но не подходят для оценки риска утечки информации;

– сложность использования балльных методов оценки рисков, ввиду необходимости их доработки, которая позволила бы объединять многочисленные факторы, влияющие на риск, в единую оценку и т.д.

Ключевые аспекты, на которые опирались специалисты при создании инструмента оценки кибер-рисков:

1) Объективное представление об уровне кибератаки;

2) Простота и удобство в процессе оценки;

3) Привлечение к оценке рисков кибербезопасности экспертов разного профиля (из безопасности, бизнеса, IT и т.п.);

4) Универсализация методики оценки для возможности сравнения результатов оценки и ранжирования их по уровню важности;

5) Возможность оценки динамики уровня риска при изменении тех или иных внешних или внутренних факторов.

При разработке методики за основу была взята классическая формула риска (1), это вероятность наступления иницидента, умноженная на величину возможного ущерба [12].

$$R = U * p \qquad (1)$$

где U – величина возможного ущерба,

p – вероятность наступления рискового события.

Был выделен перечень риск-факторов, оказывающих влияние на два ключевых показателя (U и p), который представлен в таблице 13.

Таблица 13 – Система риск-факторов [41]

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

Таким образом, оценка риска кибербезопасности проводится в 3 этапа.

Первый этап. Формирование системы риск-факторов для оцениваемого вида риска. Для каждого вида кибер-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 7 и 8). Уровень риска определяется произведением оценок ущерба и вероятности, установленных экспертом.

РИСК-ФАКТОРЫ				
Угроза (частота реализации)	Уязвимость (частота использования)	Потенциал нарушителя	Эффективность защитных мер	Вероятность
1 раз в день и чаще	1 раз в день и чаще	• Пользователи АС • Администраторы АС • Спецслужбы • Террористические и преступные группы • Хакеры	Несущественная	Событие точно произойдёт
От 1 раза в месяц до 1 раза в день	От 1 раза в месяц до 1 раза в день	• Конкурирующие организации • Разработчики ПО и техники	Невысокая	Событие скорее всего произойдёт
От 1 раза в год до 1 раза в месяц	От 1 раза в год до 1 раза в месяц	• Бывшие сотрудники • Третьи лица, привлекаемые по договору	Высокая	Событие возможно произойдёт
Реже 1 раза в год	Реже 1 раза в год	• Лица без квалификации	Очень высокая	Событие скорее всего не произойдёт

РИСК-ФАКТОРЫ						
Категория информации	Критичность АС	Нарушение процессов	Клиенты и партнеры	Регуляторы	Репутация (огласка в СМИ)	Ущерб
Коммерческая тайна	Очень критичная	Сбои в нескольких процессах Сворачивание процессов и направлений	Потеря доверия значительной части клиентов и партнеров Появление судебных исков	Внеплановые проверки Крупные штрафы до приостановки действия лицензии	Федеральный и международный уровень	Высокое воздействие
Банковская тайна, ПДн	Высоко критичная	Сбои в единичных процессах	Массовое недовольство клиентов Отток части клиентов и партнеров	Штрафы Повышенное внимание в виде писем и запросов	Интернет	Среднее воздействие
Служебная информация	Критичная	Повлияет на скорость процесса, но не приведёт к сбоям	Недовольство клиентов, не приводящее к оттоку	Предписания при проверках без наложения штрафов	Региональный уровень	Низкое воздействие
Общедоступная информация	Не критичная	Не повлияет	Недовольство единичных клиентов (не VIP)	Без предписаний	Не произойдёт	Незначительное воздействие

Рисунок 7 – Критерии оценки риск-факторов показателя вероятности [41]

Рисунок 8 – Критерии оценки риск-факторов показателей ущерба [41]

Также на данном этапе определяется вес каждого риск-фактора, чтобы снизить воздействие на итоговый показатель риска некритичных для него факторов. Так, например, для риска утечки информации некритичной будет являться оценка ущерба от нарушения процессов, тогда как параметр «категория информации» выступает решающим, и его вес необходимо повысить. Веса факторов оцениваются по шкале от 1 до 9.

Третий этап. Вычисление рейтинга кибер-риска. На данном этапе видно существенное отличие методики Сбербанка от всех остальных. Преимущество состоит в том, что можно объединить большое количество полученных мнений и весов в одном значении рейтинга риска (R) в отличие

от, например, классического табличного метода, при котором уровень риска находится на пересечении соответствующей строки вероятности и столбца ущерба, не имея возможности оперировать большим количеством мнений экспертов.

Для вычисления итогового рейтинга риска (R) методика Сбербанка использует матричный метод вычислений, агрегирующий 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 14.

Таблица 14 – Система определения соответствующего рейтингу (R) уровня риска [41]

Рейтинг риска	Низкий	Средний	Высокий	Критический
R	$R < 0{,}25$	$0{,}25 \leq R < 0{,}5$	$0{,}5 \leq R < 0{,}75$	$0{,}75 \leq R$

Таким образом, модель оценки кибер-рисков Сбербанка способствует решению ключевых задач по обеспечению кибербезопасности банка:

– Результат оценки представляет собой спектр значений рейтинга риска, что даёт возможность сравнения результатов оценки и их ранжирования по уровню важности;

– Существует возможность оценки динамики уровня риска при небольшом изменении тех или иных риск-факторов;

– Методика применима при любых масштабах оценки;

– Алгоритм и критерии оценки достаточно понятны для всех сотрудников, включая бизнесменов и работников отдела безопасности;

– Процесс оценки экспертами не требует крупных временных затрат и является простым и удобным в применении.

3 РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ МЕТОДОЛОГИИ ОЦЕНКИ КИБЕР-РИСКОВ В ПАО «СБЕРБАНК РОССИИ»

3.1. ОБЩИЕ РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ МИНИМИЗАЦИИ КИБЕР-РИСКОВ В БАНКОВСКОЙ СФЕРЕ

На современном этапе чем более развит в «цифровом» аспекте рынок, тем более он подвержен «издержкам цивилизации» в виде информационных потерь. Увеличение неопределенности в глобальной конкурентной среде подтверждает актуальность поиска новых подходов для обеспечения информационной безопасности, в частности, кибербезопасности предприятия/банка на внешних рынках и стимулирование потенциала их развития.

В параграфе 1.2 данной магистерской диссертации были обособлены основные существующие направления борьбы с киберпреступностью, включающие международное сотрудничество, борьбу на уровне отдельного государства, а также на уровне отдельной организации (банка). Опираясь на уже существующие методики защиты от кибермошенников, автором предложены общие рекомендации по совершенствованию системы минимизации кибер-рисков в банковской сфере, включающие следующие направления:

Международное сотрудничество.

Одним из важнейших направлений борьбы является взаимовыгодное сотрудничество стран, разработка всеобщих направлений деятельности законодательных органов, учёных, специалистов в области IT-технологий, направленных на борьбу с преступлениями в глобальных информационных сетях. В рамках международного сотрудничества нашей стране необходимо:

– Участвовать в разработке нормативных актов международного характера, привлекая к этому не только чиновников, но и IT-специалистов, так как в данном случае необходимы специальные знания в сфере информационных технологий и программного обеспечения.

– Разработать (либо участвовать в разработке в сотрудничестве с другими государствами) единый глобальный акт, регламентирующий порядок противодействия киберпреступникам, а также закрепляющий все ключевые понятия для того, чтобы избежать различной трактовки терминологии и сущности совершаемых преступлений в разных странах.

– Проводить международные форумы, конференции и научные выставки по кибербезопасности (а также принимать участие в проводимых другими странами).

Совершенствование нормативно-правовой базы.

В России фундаментом правового регулирования отношений в Интернет-сфере является Конституция РФ [4]. Основным законом, регулирующим свободу доступа к информации, является № 149-ФЗ "Об информации, информационных технологиях и защите информации" [8]. Также Указом Президента от 5 декабря 2016 г. № 646 утверждена Доктрина информационной безопасности Российской Федерации [7].

Общий анализ отечественного законодательства позволяет сделать вывод о том, что понятие «киберпреступность», «киберпреступление» и «кибертерроризм» на национальном уровне не закреплено, лишь регламентированы отдельные виды преступлений [20]. Так, в главе 28 УК РФ выделены наиболее значимые преступления в компьютерной сфере [5].

Действия кибермошенников на территории РФ в зависимости от цели и мотивов могут предполагать уголовную, административную и гражданско-правовую ответственность. Наибольшую роль по юридической нагрузке играет уголовная ответственность. Максимальными санкциями, применяемыми к киберпреступникам, согласно УК РФ являются штраф до 500 000 руб., а также лишение свободы до 7 лет [5].

Таким образом, на основании рассмотренной нормативно-правовой базы РФ в отношении действий киберпреступников предлагаются следующие рекомендации:

– Разработка федерального законопроекта в области кибербезопасности, включающего введение общепринятых понятий киберпреступности на законодательном уровне, методы борьбы с ней, типы компьютерных преступлений, учитывая интересы ведущих IT-специалистов страны, предпринимателей и научного сообщества;

– Доработка и усовершенствование законодательных актов РФ в соответствии с новыми видами киберпреступности;

– Структурирование государственной нормативно-правовой базы в области кибербезопасности;

– Выделение отдельным пунктом кибертерроризма в силу его отличий от иных киберпреступлений в части наличия террористической идеологии, целей, направленности на запугивание населения;

– Ужесточение наказаний за киберпреступления, в частности, за атаки на финансовые организации;

– Введение поправок, предусматривающих санкции за сокрытие информации о произошедших кибератаках.

Повышение качества образования подготовки технических и юридических кадров.

Необходимо повысить привлекательность специальностей, связанных с информационными технологиями, выделять больше бюджетных мест по данным направлениям, а также увеличить часовую нагрузку по предметам, связанным с обучением информационным технологиям студентов всех специальностей. Это необходимо, так как киберпреступность развивается абсолютно во всех отраслях, поэтому экономисты, доктора, инженеры и др. также должны быть «подкованы» в основах IT, чтобы избежать кибератак, происходящих вследствие человеческих факторов.

Также важно уделить внимание подготовке сотрудников органов внутренних дел (ОВД). Необходимо разрабатывать новые темы, разделы, спецкурсы, посвященные расследованию преступлений в сфере информационных технологий, кибербезопасности и информационной безопасности.

Создание эффективного взаимодействия ОВД с государством, обществом и учреждениями.

Необходимо сформировать систему оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями и операторами сотовой связи. Сведения следует получать путём длительных процедур согласования, направления запросов, писем в службу безопасности, проведения следственных действий судебного санкционирования [17]. Это повлияет на раскрытие преступлений «по горячим следам», упростит процесс расследования, не позволяя преступникам скрыть следы противоправных действий.

Развитие механизма страхования кибер-рисков.

Страхование от кибер-рисков как отдельный продукт – редкость для отечественного рынка. Например, программы страхования от кибер-угроз предлагают «АльфаСтрахование», «Сбербанк Страхование», «Согаз», «Альянс» и ещё нескольких крупных игроков рынка [22]. Некоторые страховые компании предлагают расширить классический полис имущественного страхования и включают в него риск кибер-угроз.

На текущем этапе для более широкого распространения данного вида страхования отсутствует и законодательная база, и судебная практика. Также серьёзным препятствием является нехватка в российских страховых компаниях специалистов, имеющих представление о структуре рисков. Поэтому для развития кибер-страхования на отечественном рынке рекомендуется:

– Использовать фронтинг. Так как страхование кибер-рисков является недостаточно перспективным и слишком рисковым, на помощь

отечественным страховым компаниям может прийти фронтинг [14]. В этом случае российским страховым компаниям лучше всего удерживать минимальную долю риска у себя, а оставшуюся передавать иностранному партнеру;

– Повысить квалификацию сотрудников страховых компаний для возможности выхода на рынок страхования кибер-угроз;

– Использовать передовые аналитические разработки (такие как блокчейн, андеррайтинг) для возможности оценки кибер-рисков, так как в отечественной практике нет общепринятой методики;

– Совершенствовать виртуальное обслуживание и цифровое распределение для сокращения издержек, получения конкретных положительных результатов и совершенствования рынка страхования кибер-рисков [19];

– Введение налоговых льгот при страховании кибер-рисков, в том числе отнесение страховых премий по ним на себестоимость при бухгалтерском учёте.

3.2. РАЗРАБОТКА МЕТОДА ОЦЕНКИ РИСКОВ КИБЕРБЕЗОПАСНОСТИ

После проведения анализа множества существующих моделей оценки рисков был сделан вывод, что для разработки подхода к оценке кибер-рисков в качестве основы подойдет далеко не каждый метод. В конечном итоге было решено взять за основу качественного метода алгоритм, использующийся в методике CRAMM [29]; а количественный метод позаимствовать из алгоритма методики ГРИФ [46].

Целью данного исследования не является разработка программного обеспечения и рассмотрение других технических сторон данной проблематики, поэтому подход будет основан только на теоретических рекомендациях и описании алгоритмов, которые впоследствии могут стать основой для создания специальных программ.

Основные этапы предлагаемого подхода к оценке кибер-рисков и их краткая характеристика представлены в таблице 15.

Таблица 15 – Основные этапы предлагаемого подхода к оценке кибер-рисков

№	Наименование	Краткая характеристика
1	Подготовительный	Определение размеров рассматриваемой информационной системы банка; границ принятия риска; перечня основных киберугроз; участников проведения анализа кибер-рисков
2	Исследовательский	Выделение информационных ресурсов – потенциальных целей кибератак, сканирование системы на наличие уязвимостей
3	Оценка рисков	Анализ уровня кибер-рисков в банке с применением количественных и качественных методов
4	Прогнозный	Прогноз дальнейших действий по управлению кибер-рисками; составление планов; внедрение различных предложений по кибербезопасности банка
5	Завершающий	Генерация отчётов; расчет различных финансовых показателей по итогам проведенного исследования

На *подготовительном этапе* определяются размеры рассматриваемой информационной системы, выделяются границы принятия риска, а также категории персонала и пользователей, принимающих участие в исследовании, и их роль в анализе кибер-рисков. Кроме того на данном этапе из классов основных источников киберугроз выделяются те, которые присущи данному банку. За основу предлагается взять перечень источников угроз информационной безопасности кредитных организаций, представленный в Рекомендациях в области стандартизации Банка России (РС БР ИББС-2.5-2014) [10].

На второй стадии проводится более подробное исследование выявленных на первом этапе угроз. Происходит выделение информационных ресурсов, которые могут стать целью кибератаки, а также сканирование системы на наличие уязвимостей.

Этап оценки рисков является важнейшим этапом в предлагаемой методике. Предполагается, что оценка кибер-рисков будет осуществляться следующим образом.

За основу взята классическая теория риска [24], т.е. риск соотносится с ожиданием потерь, которые могут наступить в результате реализации того или иного неблагоприятного события. Сначала уровень риска определяется качественным методом, а затем рассчитывается количественная величина.

При проведении качественной оценки используется метод получения индивидуального мнения членов экспертной группы, нежели метод коллективной работы, так как это позволяет повысить объективность оценки и снизить зависимость мнений экспертов друг от друга. Метод получения индивидуального мнения членов экспертной группы основан на предварительном сборе информации от экспертов, опрашиваемых независимо друг от друга, с последующей отработкой полученных данных.

Качественная оценка кибер-риска осуществляется на основе видоизмененного алгоритма, использующегося в *методике CRAMM* (CCTA Risk Analysis and Management Method) [29]. (Модель оценки рисков кибербезопасности в ПАО «Сбербанк», рассмотренная в параграфе 2.3 данной магистерской диссертации, также частично основана на методике CRAMM). Сущность данного алгоритма состоит в рассмотрении трёх основных показателей:

- уровня угрозы;
- уровня уязвимости;
- размера ожидаемых потерь.

Уровень угроз оценивается, в зависимости от экспертной оценки, как «очень высокий», «высокий», «средний», «низкий» и «очень низкий».

Мнение экспертов переводится в количественную составляющую на основании таблицы 16.

Таблица 16 – Шкала перевода экспертных мнений в количественную составляющую при оценке уровня угрозы

Уровень угрозы	
Экспертная оценка	Значение в %
"очень низкий"	0 – 20%
"низкий"	21 – 40%
"средний"	41 – 60%
"высокий"	61 – 80%
"очень высокий"	81 – 100%

Для *оценки уровня уязвимости* каждого вида кибер-риска эксперты определяют перечень актуальных угроз, уязвимостей и мер защиты (таблица 17).

Таблица 17 – Критерии оценки риск-факторов при определении уровня уязвимости кибер-риска

Балл	*Риск-факторы*				*Вероятность*
	Угроза (частота реализации)	Уязвимость (частота использования)	Потенциал нарушителя	Эффективность защитных мер	
4	1 раз в день и чаще	1 раз в день и чаще	- Пользователи автоматизированной системы (АС); -Администраторы АС; -Спецслужбы; -Террористические и преступные группы; - Хакеры	Несущественная	Событие точно произойдет
3	1 раз в день - 1 раз в месяц	1 раз в день - 1 раз в месяц	- Конкурирующие организации; -Разработчики ПО и техники	Невысокая	Событие скорее всего произойдет
2	1 раз в месяц - 1 раз в год	1 раз в месяц - 1 раз в год	-Бывшие сотрудники; -Третьи лица, привлекаемые по договору	Высокая	Событие возможно произойдет
1	Реже 1 раза в год	Реже 1 раза в год	-Лица без квалификации	Очень высокая	Событие скорее не произойдет

Эксперты, независимо друг от друга, оценивают каждый риск-фактор по четырёхбалльной шкале. По результатам оценки подсчитывается вероятность наступления неблагоприятного события в процентах.

Для *оценки размера ожидаемых потерь* эксперты проводят анализ критериев оценки риск-факторов показателя ущерба в соответствии с таблицей 18.

Таблица 18 – Критерии оценки риск-факторов при определении размера ожидаемых потерь

Балл	*Риск-факторы*						*Ущерб*
	Категория информации	Критичность АС	Нарушение процессов	Клиенты и партнеры	Регуляторы	Репутация (огласка в СМИ)	
4	Коммерческая тайна	Очень критичная	Сбои в нескольких процессах; сворачивание процессов и направлений	Потеря доверия значительной части клиентов и партнеров; появление судебных исков	Внеплановые проверки; крупные штрафы до приостановки действия лицензии	Федеральный и международный уровень	Высокое воздействие
3	Банковская тайна, персональные данные	Высоко критичная	Сбои в единичных процессах	Массовое недовольство клиентов; отток части клиентов и партнеров	Штрафы; повышенное внимание в виде писем и запросов	Интернет	Среднее воздействие
2	Служебная информация	Критичная	Влияние на скорость процесса без приведения к сбоям	Недовольство клиентов, не приводящее к оттоку	Предписания при проверках без наложения штрафов	Региональный уровень	Низкое воздействие
1	Общедоступная информация	Не критичная	Не повлияет	Недовольство единичных клиентов (не VIP)	Без предписаний	Не произойдет	Незначительное воздействие

Аналогично оценке уровня уязвимости эксперты, независимо друг от друга, оценивают каждый риск-фактор по четырёхбалльной шкале. По результатам оценки подсчитывается величина ущерба от наступления неблагоприятного события с переводом в 10-ти балльную шкалу.

При переходе от качественного анализа к количественному вводятся названия переменных, которые являются основными в алгоритме методики количественной оценки. Для наглядности входные параметры для качественного и количественного анализа представлены в таблице 19.

Таблица 19 – Соответствие входных переменных качественного и количественного методов оценки кибер-рисков

Качественная оценка	Количественная оценка		
	Обозначение	Описание	Единицы измерения
Уровень угрозы	ER	Критичность реализации угрозы	%
Уровень уязвимости ресурса	P(V)	Вероятность реализации угрозы	%
Размер ожидаемых финансовых потерь	D	Критичность ресурса	От 1 до 10

Количественная оценка производится на основе алгоритма из методики ГРИФ [46].

1. Рассчитывается уровень угрозы по уязвимости (*Th)* на основе критичности *(ER)* и вероятности реализации кибератаки *(P(V)).* Расчёт производится по формуле 2:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100} \qquad (2)$$

Значение *Th* находится в интервале от 0 до 1.

2. Рассчитывается уровень угрозы по всем уязвимостям (*CTh)*, через которые возможна реализация данной угрозы. Расчёт производится по формуле 3:

$$CTh = 1 - \prod_{j=1}^{n} (1 - Th_j) \qquad (3)$$

Значение С*Th* находится в интервале от 0 до 1.

3. Аналогично рассчитывается общий уровень угроз по ресурсу (*CThR*) (учитывая все угрозы, действующие на ресурс). Расчёт производится по формуле 4:

$$CThR = 1 - \prod_{j=1}^{n} (1 - CTh_j) \qquad (4)$$

Значение C*ThR* находится в интервале от 0 до 1.

4. Рассчитывается риск по ресурсу *(R)* как произведение общего уровня угроз по ресурсу (*CThR*) и критичности ресурса *(D)* (формула 5):

$$R = CThR \times D \qquad (5)$$

Значение *R* находится в интервале от 0 до 10. В случае, когда анализируется только один определенный вид ресурса, то количественная оценка на данном этапе завершается и уровень кибер-риска по рассматриваемому ресурсу определяется по шкале, представленной в таблице 20.

Таблица 20 – Шкала определения уровня кибер-риска по рассматриваемому ресурсу *(R)*

Уровень кибер-риска	Низкий		Средний			Высокий			Критический	
Значение R	1	2	3	4	5	6	7	8	9	10

5. На заключительном этапе количественной оценки рассчитывается кибер-риск по информационной системе *(CR)*. Расчёт производится по формуле 6:

$$CR = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_j}{100}\right)\right) \times 100 \qquad (6)$$

Значение *CR* находится в интервале от 0 до 100. Таким образом, уровень кибер-риска по информационной системе в целом определяется по шкале, схожей с предыдущей и представленной в таблице 21.

Таблица 21 – Шкала определения уровня кибер-риска по информационной системе *(CR)*

Уровень кибер-риска	Низкий		Средний			Высокий			Критический	
Значение *CR*	10	20	30	40	50	60	70	80	90	100

Четвертый этап методики включает в себя дальнейшие действия по управлению выявленными кибер-рисками; составление краткосрочных, среднесрочных и долгосрочных планов обработки рисков, усовершенствование систем безопасности банка, разработка и внедрение различных предложений по кибербезопасности кредитной организации.

Завершающий этап разработанной методики включает работу с документацией и отчетами по проделанному анализу. Также на данном этапе рассчитывают различные финансовые показатели, такие как: окупаемость инвестиций в кибербезопасность (ROI); показатель ожидаемых потерь (ALE); затраты на реализацию данной методики оценки кибер-рисков и т. д.

3.3 «ПИЛОТНАЯ» ПРАКТИКА ПРИМЕНЕНИЯ ОЦЕНОЧНОГО ПОДХОДА НА ПРИМЕРЕ ПАО «СБЕРБАНК РОССИИ»

Результатом проведенного исследования явился разработанный подход к оценке кибер-рисков, основанный на распространенных методиках оценки рисков информационной безопасности (CRAMM и ГРИФ). Для проверки корректности данной методики проведена её апробация на примере российского коммерческого банка – ПАО «Сбербанк России».

Всесторонний анализ и оценка совокупного кибер-риска коммерческого банка (или даже какого-либо одного вида кибер-рисков) по разработанной методике является крайне ответственной и непростой задачей.

Для оценки действенности разработанного алгоритма, проведена качественная и количественная оценка кибер-риска от реализации трёх угроз, связанных с хакерскими атаками на мобильное приложение банка. Для примера был выбран коммерческий банк – ПАО «Сбербанк».

Первый этап.

1. Определение размеров рассматриваемой информационной системы.

Информационная система банка является очень обширной и в большинстве своем представляет собой банковскую тайну. Поэтому вследствие ограниченности информации было решено рассмотреть в качестве исследуемой системы – мобильное приложение «Сбербанк Онлайн», как один из наиболее критичных компонентов IT-инфраструктуры.

2. Выделение границ принятия риска.

Риск будет относиться к категории допустимого, если по результатам качественной оценки все три показателя (уровень угрозы; уровень уязвимости; размер ожидаемых финансовых потерь) будут иметь значение ниже 20%.

3. Распределение ролей.

– ответственный за изменение параметров методики оценки рисков в случае выявления её недостаточной эффективности;

– ответственный за оценку кибер-рисков;

– ответственный за ошибки и нарушения в разработанной методике оценки рисков;

– ответственный за разработку планов обработки кибер-рисков.

4. Выделение актуальных киберугроз (по источникам), уязвимостей и потенциальных потерь.

– Ресурсы: информационные, финансовые, программные.

– Угрозы по источникам: связанные с внутренними/внешними нарушителями кибербезопасности, с техническими сбоями и др.

– Уязвимости: недостаточный уровень технической защиты; низкий уровень качества мобильного приложения; низкая квалификация персонала в вопросах кибербезопасности и т.п.

– Потери: конфиденциальности, целостности и доступности информации; финансовые потери; потеря репутации банка и др.

Второй этап.

На предыдущей стадии исследования было решено остановиться на таком виде кибератаки, как атака мобильного приложения. На втором этапе (более подробного исследования выявленных угроз) выделены самые ценные ресурсы, которые могут стать потенциальной целью атаки мобильного приложения коммерческого банка (таблица 22).

Таблица 22 – Ресурсы, которые могут стать потенциальной целью кибератаки мобильного приложения «Сбербанк Онлайн» (по классам ресурсов)

Класс ресурса	Потери
Информационные	Персональные данные клиентов
	Информация о счетах
	Информация о транзакциях
	Информация о вкладах/депозитах, кредитах
Финансовые	Прямой финансовый ущерб
	Хищение средств со счетов клиентов различными косвенными способами
	Потеря банком части своих доходов из-за временного приостановления работы
	Финансовые затраты банка на устранение последствий кибератаки
Временные	Затраты на выявление источника кибератаки
	Временные затраты на восстановление работы и устранение последствий кибератаки
	Затраты на возможные судебные разбирательства

Третий этап.

Необходимо составить перечень угроз и уязвимостей, через которые могут быть реализованы кибератаки и определить уровень риска качественным методом.

При оценке кибер-рисков на уровне коммерческого банка экспертам в области информационной безопасности и кибербезопасности рекомендуется

составить список вопросов, в результате ответов на которые будут получены оценки уровня угрозы; уровня уязвимости и размера ожидаемых потерь. В текущем исследовании данные величины будут определены автором.

Таким образом, по риску кибератаки на мобильное приложение банка выделено три угрозы, каждая из которых реализуется при помощи ряда уязвимостей, таких как:

– низкий уровень технической защиты;

– недостаточность инвестиций банка в обеспечение кибербезопасности;

– некомпетентность клиента в основах безопасности (самостоятельное раскрытие личной информации по незнанию);

– низкая квалификация персонала IT-отдела банка;

– привлекательность хищения (крупные суммы на счетах клиентов);

– личная неприязнь третьих лиц к данному банку и т.п.

В рамках данного исследования было решено выделить по одной ключевой уязвимости для каждой из угроз (таблица 23).

Далее была произведена экспертная оценка трёх основных показателей:

– уровня угрозы;

– уровня уязвимости;

– размера ожидаемых потерь.

Результаты оценки представлены в таблице 23.

Таблица 23 – Результаты качественной оценки основных угроз и уязвимостей исследуемой системы

Угроза	Уязвимость	Уровень угрозы	Уровень уязвимости, балл	Размер ожидаемых потерь, балл
1. Целевая хакерская атака на мобильное приложение с возможностью обхода средств защиты с целью хищения денежных средств. Результат: хищение денежных средств со счета клиента	Привлекательность хищения (крупные суммы на счетах клиентов)	Средний	13 из 16	16 из 24
2. Хакерская атака на мобильное приложение для получения личной информации о клиенте с целью дальнейших мошеннических операций Результат: хищение персональной информации о клиенте	Некомпетентность клиента в основах безопасности (самостоятельное раскрытие личной информации по незнанию)	Средний	13 из 16	15 из 24
3. Хакерская атака на мобильное приложение с целью выведения из строя мобильного банкинга и ослабления бдительности банка, а также с целью снижения деловой репутации банка Результат: потеря части доходов банка из-за длительного временного простоя; возможна потеря деловой репутации в случае раскрытия информации об атаке	Низкий уровень технической защиты и кибербезопасности банка	Высокий	12 из 16	21 из 24

Качественная оценка начинается с *оценки уровня* перечисленных *угроз*. В целом для Сбербанка самой критичной является третья угроза, так как потери от данного типа угрозы влияют в совокупности на весь банк, это и недополучение доходов банка в связи с длительными временными простоями, и потеря репутации, которая также повлияет на весь банк негативно. Поэтому уровень угрозы № 3 решено определить, как «высокий». На основании таблицы 16 определено, что данный уровень угрозы соответствует интервалу 61–80%, таким образом, решено остановиться на значении – 70%. Угрозы № 1 и № 2 схожи по своему воздействию на банк, обе приведут к возможной потере клиентов, однако первая угроза

сопровождается реальными финансовыми потерями, что наиболее критично. Поэтому решено определить уровень угроз № 1 и № 2 как «средний», однако после перевода показателя в процентное значение угрозе № 1 присваивается значение – 60 %, а угрозе № 2 – 55 %.

Для *оценки уровня уязвимости* проведена оценка по нескольким риск-факторам, результаты которой представлены в таблице 24.

Таблица 24 – Результаты оценки уровня уязвимости

Угроза	*Риск-факторы, баллы*				*Сумма баллов*
	Угроза (частота реализации)	Уязвимость (частота использования)	Потенциал нарушителя	Эффективность защитных мер	
1	3	4	4	2	13
2	3	4	4	2	13
3	2	4	4	2	12

Чтобы рассчитать *уровень уязвимости,* выставленные баллы были переведены в проценты:

$$\text{Угроза № 1: } \frac{13 \text{ баллов}}{16 \text{ баллов}} \times 100\% = 81{,}25\%$$

$$\text{Угроза № 2: } \frac{13 \text{ баллов}}{16 \text{ баллов}} \times 100\% = 81{,}25\%$$

$$\text{Угроза № 3: } \frac{12 \text{ баллов}}{16 \text{ баллов}} \times 100\% = 75\%$$

Для *определения размера ожидаемых потерь* проведена оценка по нескольким риск-факторам, результаты которой представлены в таблице 25.

Таблица 25 – Результаты оценки размера ожидаемых потерь

Угроза	*Риск-факторы, баллы*						*Сумма баллов*
	Категория информации	Критичность АС	Нарушение процессов	Клиенты и партнеры	Регуляторы	Репутация (огласка в СМИ)	
1	4	2	3	3	2	2	16
2	3	2	3	3	2	2	15
3	4	4	4	2	3	4	21

Чтобы рассчитать *размер ожидаемых потерь,* выставленные баллы были переведены в 10-ти балльную шкалу (что понадобится при количественной оценке риска):

$$\text{Угроза № 1: } \frac{16 \text{ баллов}}{24 \text{ баллов}} \times 10 = 6{,}667$$

$$\text{Угроза № 2: } \frac{15 \text{ баллов}}{24 \text{ баллов}} \times 10 = 6{,}25$$

$$\text{Угроза № 3: } \frac{21 \text{ баллов}}{24 \text{ баллов}} \times 10 = 8{,}75$$

По результатам качественной оценки получено, что ни один риск не является приемлемым, соответственно необходимо проведение количественной оценки.

Переходя к количественному анализу, необходимо ввести переменные, применяемые в данном алгоритме методики (таблица 26).

Таблица 26 – Входные переменные качественного и количественного методов оценки кибер-рисков

Обозначение в качественной оценке	Уровень угрозы	Уровень уязвимости ресурса	Размер ожидаемых потерь
Обозначение в количественной оценке	ER (Критичность реализации угрозы)	P(V) (Вероятность реализации угрозы)	D (Критичность ресурса)
Угроза № 1	60 %	81,25 %	6,667 из 10 баллов
Угроза № 2	55 %	81,25 %	6,25 из 10 баллов
Угроза № 3	70 %	75 %	8,75 из 10 баллов

Для удобства первая угроза обозначена Th_1, вторая – Th_2, а третья – Th_3. Вычисление уровня кибер-риска количественным методом:

1. Расчёт уровня угрозы по уязвимости (*Th)* на основе критичности *(ER)* и вероятности реализации кибератаки *(P(V))*:

$$Th_1 = \frac{60}{100} \times \frac{81{,}25}{100} = 0{,}4875$$

$$Th_2 = \frac{55}{100} \times \frac{81{,}25}{100} = 0{,}4469$$

$$Th_3 = \frac{70}{100} \times \frac{75}{100} = 0{,}525$$

2. Значения показателей угрозы по всем уязвимостям (*CTh)* в данном исследовании равны значениям показателей из 1 этапа количественной оценки *(Th),* так как на начальном этапе исследования было условно принято, что каждая угроза может быть реализована только через одну уязвимость, поэтому:

$$CTh_1 = Th_1 = 0{,}4875$$

$$CTh_2 = Th_2 = 0{,}4469$$

$$CTh_3 = Th_3 = 0{,}525$$

3. Расчёт общего уровня угроз по ресурсу (*CThR*) (учитывая все угрозы, действующие на ресурс):

$$CThR = 1 - (1 - 0{,}4875) \times (1 - 0{,}4469) \times (1 - 0{,}525) \approx 0{,}865$$

4. Расчёт риска по ресурсу *(R).*

Прежде чем рассчитать риск по ресурсу необходимо определить значение показателя *D*, как среднее по имеющимся значениям уровня ожидаемых потерь по трём угрозам:

$$D = (6{,}667 + 6{,}25 + 8{,}75) / 3 = 7{,}222$$

Таким образом, *риск по ресурсу* равен:

$$R = 0{,}865 \times 7{,}222 = 6{,}247$$

Так как данное исследование ограничивается оценкой кибер-риска только по мобильному приложению «Сбербанк Онлайн», то расчет риска по информационной системе (*CR)* не является целесообразным. Поэтому, завершая количественную оценку, необходимо обратиться к шкале оценки кибер-риска, представленной в таблице 27.

Таблица 27 – Шкала определения уровня кибер-риска по рассматриваемому ресурсу

Уровень кибер-риска	Низкий		Средний			Высокий			Критический	
Значение R	1	2	3	4	5	6	7	8	9	10

Прогнозный и завершающий этапы.

Полученный результат *R = 6,247* попадает в интервал «высокого» уровня кибер-риска. Это означает, что мобильное приложение Сбербанка с достаточно высокой вероятностью подвержено кибератакам. Это объясняется тем, что мобильное приложение Сбербанка имеет множество уязвимостей, а кибермошенники с каждым днём находят всё более изощренные способы хищения. Так, очень важным фактором по прежнему остается *человеческий фактор*. Пользователи зачастую сами виноваты во взломе из-за некомпетентности в базовых вопросах безопасности, которые рекомендуют [45]:

– не разглашать данные о логинах, паролях и прочую личную информацию третьим лицам, кем бы они не являлись;

– не совершать переходы по сторонним ссылкам в Интернете;

– использовать только официальные мобильные приложения, разработанные Сбербанком для своих клиентов;

– не вводить паспортные данные, номера телефонов или другие персональные данные при подтверждении операций;

– для установки приложений использовать смартфон с оригинальным ПО производителя и т.п.

Также существуют и другие немаловажные опасности. Например, *не все сотрудники банка являются компетентными* в вопросах кибербезопасности, что также может повлечь риск кибератаки. Для этого Сбербанк запустил Академию кибербезопасности [56] для корпоративного обучения основам кибербезопасности.

Касаемо *технической защиты* Сбербанк также постоянно совершенствуется и внедряет современные технологии и процессы управления безопасностью [40].

Таким образом, оценив кибер-риски мобильного приложения Сбербанка, был сделан вывод, что «Сбербанк Онлайн» с достаточно высокой вероятностью подвержен кибератакам. Это вполне объяснимо масштабами данного банка, его привлекательностью для мошенников, количеством пользователей и т.д. Однако высокий уровень кибер-риска не означает, что Сбербанк не сможет отразить атаку и спастись от мошенников, ведь Сбербанк на данный момент является одним из самых активных борцов с киберпреступностью в России [40]. На текущем этапе Сбербанк разрабатывает и планирует ввести множество новых методов защиты, а также высококвалифицированного персонала; проводит различные конференции, форумы и конгрессы по кибербезопасности; сотрудничает с мировыми организациями по вопросам рассматриваемой проблемы.

3.4 ПЕРСПЕКТИВЫ РАЗВИТИЯ РАЗРАБОТАННОГО ПОДХОДА К ОЦЕНКЕ КИБЕР-РИСКОВ

Таким образом, в результате проведенного исследования был разработан подход к оценке кибер-рисков кредитных организаций, который имеет свои преимущества и недостатки, представленные в таблице 28.

Таблица 28 – Преимущества и недостатки разработанной методики оценки кибер-рисков коммерческих банков

Преимущества	Недостатки
1) Дает представление о размере кибер-риска в банке	1) Зависит от субъективного экспертного мнения
2) Дает возможность отслеживать динамику кибер-риска	2) Требует формирования списка риск-факторов для каждой оценки
3) Позволяет оценить кибер-риск как в целом по банку, так и по отдельным ресурсам	3) Несёт большие временные и кадровые затраты на проведение оценки
4) Имеет понятную структуру и порядок оценки, простые расчёты	4) Не дает прогнозного количества кибератак и величины вероятного ущерба (в денежном выражении)

Данная методика способна помочь коммерческим банкам в оценке кибер-рисков, однако имеет существенный недостаток – субъективность экспертного мнения. Минимизировать данный недостаток можно путем привлечения экспертов из различных областей, не заинтересованных в результатах и стремящихся к максимальной объективности.

В целом методика получилась достаточно структурированной, воспользоваться ей сможет как человек, связанный с IT-отраслью, так и любой финансист, так как основной груз работы при проведении анализа и оценки ложится на плечи экспертов.

Вместе с тем, можно отметить следующие базовые направления повышения эффективности и качества оценки кибер-рисков в банковском секторе:

– повышение объективности оценки на основе набора и использования статистических данных по рискам;

– формирование базового перечня риск-факторов для наиболее критичных систем, что позволит оптимизировать процесс оценки;

– совершенствование методов построения модели с применением других методик оценки банковских рисков;

– преобладание количественной оценки риск-факторов над качественной и т.д.

ЗАКЛЮЧЕНИЕ

Развитие информационных технологий, происходящее в современном мире, несет за собой негативные последствия в виде развития киберпреступности, которая не стоит на месте и постоянно порождается новыми видами атак, инструментов и методов, которые позволяют мошенникам проникать в наиболее сложные и контролируемые среды, наносить большой урон и зачастую оставаться незамеченными. Особую популярность среди кибермошенников получил финансовый сектор экономики, в частности коммерческие банки. «Кибер-риск» представляет для банков одну их самых популярных угроз и требует к себе особого внимания.

Борьба с киберпреступностью ведется на всех уровнях: международном, государственном, региональном, отраслевом и на уровне отдельно взятых субъектов (в частности, кредитных организаций).

Однако, потери от кибератак продолжают ежегодно увеличиваться и по прогнозам к 2021 году киберпреступность будет стоить миру более 6 трлн.$ по сравнению с 3 трлн.$ в 2015 году.

Опираясь на исследование компании Positive Technologies, были выделены ключевые аспекты совершённых кибератак за 2019 год:

- количество уникальных кибератак ежемесячно увеличивалось, и по итогам года на 19% превысило число кибератак в 2018 году;
- наибольшее количество кибератак зафиксировано на госучреждения, промышленность, медицину, сферу науки и образования и финансовую отрасль (в сумме – 54 %);
- доля атак на предприятия промышленной отрасли выросла до 10% против 4% в 2018 году;
- доля целевых атак (по сравнению с массовыми атаками) выросла по сравнению с 2018 годом на 5 п.п. и составила 60%;

- доля кибератак, направленных на хищение информации составила 60% против юридических лиц и 57% против частных лиц;
- количество заражений вредоносным ПО в 2019 году на 38% превысило аналогичный показатель 2018 года;
- одной из наиболее актуальных киберугроз для компаний по всему миру являются троянцы-шифровальщики (31% заражений ВПО среди юридических лиц).

Анализ современных тенденций киберпреступности в России показал, что они схожи с мировыми и сопровождаются аналогичными проблемами. Однако, после анализа статистики величины ущерба российских банков от кибератак, было выявлено что в 2019 году объём ущерба снизился. Вероятно, опыт предыдущих лет, когда происходил настоящий бум киберпреступности, заставил банки всерьез заняться своей кибербезопасностью, что многим помогло избежать потерь.

Также в ходе исследования были выделены основные проблемы киберпреступности:

- сложность в определении источника угрозы;
- анонимность сети Интернет;
- сложность выработки мер противодействия киберпреступности;
- надежда на стандартные средства защиты;
- транснациональность сети и отсутствие механизмов контроля;
- количество пользователей;
- автоматизация и быстрота использования;
- несовершенство законодательства;
- напряженная политическая обстановка в мире;
- сокрытие фактов о произошедших кибератаках;
- неэффективность работы органов внутренних дел
- нехватка квалифицированных кадров.

Для решения выявленных проблем, были разработаны пути решения, включающие мировое сотрудничество; совершенствование законодательной базы; проведение форумов и конференций, мероприятий по увеличению IT-грамотности пользователей Интернета; обучение сотрудников банков основам кибербезопасности; разработка банками экономико-математических моделей прогнозирования направлений кибератак и оценки потенциального ущерба (рисков) и др.

Поэтому в рамках данного исследования было решено модернизировать методику оценки кибер-рисков для кредитных организаций, базируясь на известных методах оценки рисков информационной безопасности – CRAMM и ГРИФ. Разработанная методика включается в себя количественную и качественную оценку, по большей части базируясь на экспертных оценках. Модель получилась достаточно логичной и структурированной, понятной не только лицам, причастным к IT-отрасли, но и финансистам, бизнесменам и др.

По итогам разработки методика была апробирована на крупнейшем российском коммерческом банке ПАО «Сбербанк». Полученные результаты были проанализированы, сформулированы основные преимущества и недостатки предлагаемой методики. Также были определены перспективные направления повышения эффективности и качества оценки:

– повышение объективности оценки на основе набора и использования статистических данных по рискам;

– формирование базового перечня риск-факторов для наиболее критичных систем, что позволит оптимизировать процесс оценки;

– совершенствование методов построения модели с применением других методик оценки банковских рисков;

– преобладание количественной оценки риск-факторов над качественной и т.д.

Элементы новизны исследования заключается в том, что была предложена систематизация теоретических представлений в сфере

управления кибер-рисками, углубленно рассмотрен понятийный аппарат. Основные задачи исследования, как в части систематизации теоретических основ управления кибер-рисками, так и в области разработки методического подхода к оценке кибер-рисков коммерческого банка были решены.

Несомненно, киберпреступность будет развиваться и далее, трансформируя методы мошенничества в более изощренные формы. Необходимо предвидеть действия злоумышленников, создавать систему ограничений, блокирующую киберпреступность. Укрепление системы кибербезопасности финансового сектора в современном мире должно минимизировать масштабные потери финансовых организаций. Однако создание стратегических основ безопасности на уровне банковской системы и отдельно взятых банковских учреждений может стать серьезным барьером для экономических преступлений в информационном поле.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Закон «О мошенничестве и злоупотреблении с использованием компьютеров» от 21.10.1984 (США)

2. Закон «О неправомерном использовании компьютерных технологий» от 1990 г. (Великобритания)

3. Конвенция Совета Европы о киберпреступности ETS № 185

4. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. - 04.08.2014. - № 31. - ст. 4398

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 18.02.2020)// Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954

6. Уголовный кодекс ФРГ в редакции от 13 ноября 1998 г.

7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

9. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 06.02.2020) "О безопасности"

10. Рекомендации в области стандартизации Банка России (РС БР ИББС-2.5-2014) «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» от 01.06.2014

11. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

12. Вяткин В.Н. Риск-менеджмент: Учебник / В.Н. Вяткин, В.А. Гамза, Ф.В. Маевский. - Люберцы: Юрайт, 2016. - 353 с.

13. Курило А.П. Управление рисками информационной безопасности [Текст]: 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 с.

14. Чернова Г.В. Страхование и управление рисками : учебник для бакалавров / Г. В. Чернова [и др.] ; под ред. Г. В. Черновой. — 2-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 767 с.

15. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. №5 (8).

16. Вигриянова Ю.С. Современные тенденции развития киберпреступности в банковском секторе. / Ю.С.Вигриянова, Г.С.Чеботарёва // Весенние дни науки ВШЭМ: сборник докладов международной конференции студентов, аспирантов, молодых учёных. 2017. – С. 113-116

17. Дерюгин Р. А. Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. №2.

18. Ильюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: Дис. канд. юрид. наук. Волгоград, 2008. С. 47 – 89. 3 Мещеряков В. А. Указ. соч. С. 70.

19. Коломасова Р.А. Мировые тенденции страхования информационных рисков и проблемы его внедрения в российскую практику // E-Scio. 2019. №6 (33).

20. Кумышева М.К., Геляхова Л.А. К вопросу о киберпреступности в России и мире // Пробелы в российском законодательстве. 2018. №4

21. Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. Научный журнал. 2013. № 5 (10)

22. Просветова А.А., Дубкова Е.В. Кибер-страхование как способ обеспечения информационной безопасности // Международный журнал гуманитарных и естественных наук. 2020. №4-3.

23. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. ... канд. юрид. наук. Владивосток, 2005. – 235 с.

24. Bessis Joell. Risk-management in Banking. Australia: Jonh Wilev and Sons, LTD, 2013. P. 11.

25. Boes S. Fighting cybercrime: joint effort / S. Boes, E.R. Leukfeldt // Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. - Cincinnati: Springer. - 2016. - P. 185-205.

26. 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.

27. 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.

28. Актуальные киберугрозы: итоги 2019 года [Электронный ресурс] // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/

29. Анализ методики CRAMM [Электронный ресурс] // URL: http://studbooks.net/2024790/informatika/analiz_metodiki_cramm

30. Банки утаивают каждую пятую успешную кибератаку [Электронный ресурс] // URL: https://www.securitylab.ru/news/489810.php

31. В России появился центр компетенций кибербезопасности [Электронный ресурс] // URL: https://rg.ru/2018/05/22/v-rossii-poiavilsia-centr-kompetencij-kiberbezopasnosti.html

32. ГА ООН приняла российскую резолюцию о борьбе с киберпреступностью [Электронный ресурс] // URL: https://ria.ru/20191228/1562965015.html

33. Доклад Конгресса ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс] // URL: https://www.unodc.org/congress/

34. Доклад PWC: Управление рисками и кибербезопасность [Электронный ресурс] // URL: http://files.runet-id.com/2017/csf17/07feb.csf17-3.2--chaplygin.pdf

35. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646 [Электронный ресурс] // URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

36. Информация о международном форуме «AntiFraud Russia» [Электронный ресурс] // URL: http://vipforum.ru/conferences/antifraud_russia/

37. Информация о мероприятии Cyber Security Day 2020 [Электронный ресурс] // URL: https://runet-id.com/event/sid20

38. Как интернет спасли от гибели. История SOPA и PIPA [Электронный ресурс] // URL: http://www.cnews.ru/news/top/kak_internet_spasli_ot_gibeli.istoriya

39. Как Россия будет бороться с киберпреступностью. Путин назвал 5 шагов [Электронный ресурс] // URL: https://gov.cnews.ru/news/top/2018-07-06_putin_prizval_strany_ne_byt_egoistami_v_tsifrovoj

40. Как Сбербанк борется с киберпреступностью [Электронный ресурс] // URL: https://tass.ru/ekonomika/5082607

41. Как сберечь миллион: модель оценки киберрисков [Электронный ресурс] // URL: https://bosfera.ru/bo/kak-sberech-million-model-ocenki-kiberriskov

42. Коммюнике совещания «Группы восьми» [Электронный ресурс] // URL: http://kremlin.ru/supplement/3179/print

43. Концепция стратегии кибербезопасности Российской Федерации. [Электронный ресурс] // URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

44. К чему приложил руку «Сбер»: Okko, DocDoc, «Ситимобил», «Беру» и ещё больше двух десятков интернет-сервисов [Электронный ресурс] // URL: https://vc.ru/story/76802-k-chemu-prilozhil-ruku-sber-okko-docdoc-sitimobil-beru-i-eshche-bolshe-dvuh-desyatkov-internet-servisov

45. Меры безопасности при работе с приложениями и сервисам Сбербанка [Электронный ресурс] // URL: https://sber-info.ru/mery-bezopasnosti-pri-rabote-s-prilozheniyami-i-servisam-sberbanka/

46. Методика оценки риска ГРИФ из состава Digital Security Office [Электронный ресурс] // URL: http://citforum.ru/products/dsec/grif/

47. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год [Электронный ресурс] // URL: https://cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf

48. Отчет об угрозах 2019 года [Электронный ресурс] // URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

49. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России 1.09.2018 – 31.08.2019 [Электронный ресурс] // URL: https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF

50. Официальный ежегодный отчет о киберпреступности за 2019 год [Электронный ресурс] // URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

51. Официальный сайт ПАО «Сбербанк» [Электронный ресурс] // URL: http://www.sberbank.ru/ru/about/today

52. Политика ЦБ в сфере защиты информации (кибербезопасности) [Электронный ресурс] // URL: http://www.tadviser.ru/index.php/Статья:Политика_ЦБ_в_сфере_защиты_информации_(кибербезопасности)

53. Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности

[Электронный ресурс] // URL: https://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd

54. Резолюция Генеральной Ассамблеи ООН [Электронный ресурс] // URL: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/570/12/IMG/NR057012.pdf?OpenElement

55. Риски - понятие и виды. Классификация рисков. Основные характеристики рисков [Электронный ресурс] // URL: http://www.grandars.ru/student/fin-m/vidy-riskov.html

56. Сбербанк запускает Академию кибербезопасности [Электронный ресурс] // URL: https://www.securitylab.ru/blog/personal/Business_without_danger/343137.php

57. Сбербанк (информационная безопасность) [Электронный ресурс] // URL: http://www.tadviser.ru/index.php/Статья:Сбербанк_(информационная_безопасность)

58. Сбербанк Онлайн: описание сервиса, функции, возможности [Электронный ресурс] // URL: https://bankspec.ru/sbol/sberbank-onlajn-opisanie/

59. Сбербанк сообщил о мощнейшей в его истории DDoS-атаке [Электронный ресурс] // URL: https://www.rbc.ru/business/21/01/2020/5e26a8a69a79475cb4f039a5

60. Сотрудничество России и США в киберпространстве [Электронный ресурс] // URL: https://inosmi.ru/military/20170809/240006295.html

61. Степашин: кибертерроризм наносит России серьезный финансовый удар [Электронный ресурс] // URL: https://www.kommersant.ru/doc/3482441

62. Страхование кибер-рисков – Страхование от компании AIG в России [Электронный ресурс] // URL: https://www.aig.ru/business/products/cyber-edge

63. Топ-5 главных рисков кибербезопасности в 2020 году [Электронный ресурс] // URL:https://news.rambler.ru/other/43534097/?utm_content=news_media&utm_medium=read_more&utm_source=copylink

64. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома [Электронный ресурс] // URL: https://vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma

65. Хакеры придут, все деньги заберут [Электронный ресурс] // – URL: https://www.banki.ru/news/columnists/?id=9423714

66. Angara прокомментировала новый отчет Центробанка о киберпреступности и мошенничестве [Электронный ресурс] // URL: https://club.cnews.ru/blogs/entry/otchet_tsentrobanka_o_kiberprestupnosti_i_moshennichestve

67. ESET предупреждает о действиях киберпреступников в связи с эпидемией коронавируса [Электронный ресурс] // URL: https://www.esetnod32.ru/company/press/center/eset-preduprezhdaet-o-deystviyakh-kiberprestupnikov-v-svyazi-s-epidemiey-koronavirusa/

68. Hi-Tech Crime Trends 2019/2020 [Электронный ресурс] // URL: https://www.group-ib.ru/resources/threat-research/2019-report.html

69. Kaspersky Security Bulletin 2019. Статистика [Электронный ресурс] // URL: https://securelist.ru/kaspersky-security-bulletin-2019-statistics/95264/