

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc73140703)

[1 Теоретические аспекты исследования киберпреступности 5](#_Toc73140704)

[1.1 Понятие и сущность киберпреступности 5](#_Toc73140705)

[1.2 Киберпреступления в экономической сфере 11](#_Toc73140706)

[2. Анализ борьбы с киберпреступностью в современном мире 15](#_Toc73140707)

[2.1 Особенности и проблемы борьбы с киберпреступностью в России 15](#_Toc73140708)

[2.2 Перспективы усиления кибербезопасности в России 18](#_Toc73140709)

[ЗАКЛЮЧЕНИЕ 22](#_Toc73140710)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 24](#_Toc73140711)

# **ВВЕДЕНИЕ**

Сегодня мы живем и работаем в мире глобальных возможностей взаимодействия. Стремительное увеличение количества персональных компьютеров, свободный доступ к Интернету и быстро развивающийся рынок новых коммуникационных устройств изменили и способы проведения досуга, и методы ведения бизнеса. Меняются и способы совершения преступлений. Доступность глобальных цифровых технологий открывает новые возможности недобросовестным лицам. И бизнесмены, и потребители лишились миллионов долларов «с помощью» обладающих компьютерными знаниями преступников.

Данная тема курсовой работы актуальна в наше время, так как за последние несколько десятилетий объем исследований в области киберпреступности вырос в геометрической прогрессии, ведь технологические достижения также создали множество возможностей для правонарушителей совершать различные формы преступлений.

*Проблема* киберпреступности основана на том, что во многих случаях правоохранительные органы отстают от преступников, испытывая недостаток технологий и квалифицированного персонала для отражения новой и быстро растущей угрозы.

*Целью* курсовой работы является изучение источников и факторов, приводящих к появлению киберпреступлений, а также их влияние на все сферы общественной жизни.

На основании представленной цели можно выделить следующие *задачи* курсовой работы:

- рассмотреть сущность понятия киберпреступность,

- оценить влияние преступлений в киберпространстве на экономическую сферу жизни,

- изучить причины, приводящие к появлению киберпреступлений,

- исследовать современную статистику по количеству киберпреступлений в России,

- выявить перспективы дальнейшей динамики проблемы.

*Объектом исследования* курсовой работы является киберпреступность как явление в современном обществе.

*Предметом исследования* курсовой работы является изучение сущности киберпреступности, ее видов и методов борьбы с ней.

Теоретической базой исследования в данной курсовой работе послужили основные теории о компьютерной преступности, сформированные различными авторами.

Эмпирическая база исследования включает в себя учебную литературу по основам киберпреступности и методам борьбы с ней, статьи и публикации современных авторов, связанные с тематикой работы.

Методологической базой исследования послужили как общенаучные, а именно, историко-логический метод, метод научных абстракций, так и частные методы исследования, такие как наблюдение и сбор фактов, сравнение, анализ и синтез, графическое отражение данных.

Данная курсовая работа состоит из введения, двух глав, заключения и списка литературы. В первой главе рассмотрены теоретические аспекты и причины возникновения киберпреступности. Во второй главе анализировалось современное состояние и статистика киберпреступлений в России и перспективы усиления эффективности борьбы с ней. В заключении работы подведены основные итоги и выводы на основании проведенного исследования.

# **1 Теоретические аспекты исследования киберпреступности**

## **1.1 Понятие и сущность киберпреступности**

В наш век технического прогресса, новых технологий и инновационной экономики уже ни у кого не вызывает сомнений необходимость использования электронно-вычислительных машин, компьютерных систем, глобальных информационных сетей в различных сферах политической, социально-экономической, духовно-культурной жизни общества, и в повседневной жизни обычного человека.

Продолжающее развитие и совершенствование прикладных технических наук, компьютерных технологий, глобальных информационных сетей в условиях рыночной экономики обусловили и совершение большого количества общественно опасных деяний - «компьютерных» преступлений, посредством которых преступники осуществляют несанкционированный доступ к компьютерной информации, незаконное копирование, блокирование, модификацию и уничтожение компьютерной информации.

Что отличает киберпреступность от традиционной преступной деятельности? Очевидно, что одним из отличий является использование компьютерных технологий. До того, как они стали повсеместно распространённой вещью, преступникам не нужен был компьютер для совершения мошенничества, торговли интеллектуальной собственностью, кражи личных данных или нарушения чьей-либо частной жизни. Все эти виды деятельности существовали до того, как префикс «кибер» стал повсеместным.

Исследователи, изучающие масштабы этого вида преступной деятельности в различных странах, сформулировали определение самого термина, а также определили основные незаконные практики, которые составляют киберпреступность.

Киберпреступление — это все виды криминальной активности, совершаемые с помощью информационных технологий. Киберпреступление может совершаться с помощью различных методов и инструментов, например, фишинг, вирусы, шпионское ПО, программы-вымогатели и социальная инженерия - чаще всего с целью кражи личных данных или финансовых средств. Эти преступления делятся на две категории:

1) преступления, связанные с несанкционированным доступом к данным и системам в преступных целях

2) преступления, связанные с мошенничеством, фальсификацией, утечкой средств, получением незаконного контента или диффамацией через онлайн-сервисы.

Особую распространенность данное течение приобрело в 21 веке. Термин «компьютерная преступность» впервые появился в США, еще в начале 60-х годов. Тогда были совершены первые преступления с использованием вычислительных машин [13].

Киберпреступность является одним из видов транснациональной преступности, исполнители и жертвы которой могут находиться в любой точке мира, где есть подключение к Интернету. Кроме того, общественная опасность компьютерных преступлений заключается в том, что они становятся способом для совершения многих других умышленных преступлений (например, кражи или мошенничества), облегчения их совершения и уничтожения следов преступной деятельности.

Данные преступления характеризуются анонимностью, максимальной скрытностью преступника. Как известно, в информационном пространстве довольно тяжело вычислить лицо, которое совершило противоправное деяние. Но сложность вычисления и формирование своеобразной «подушки безопасности» для преступника обеспечивают специальные средства и программы (анонимайзеры, использование интернет-кафе и т.д.).

Нестандартность киберпреступления также выступает отличительной чертой данного вида преступлений. Довольно сложно, а порой и невозможно предугадать дальнейшие действия киберпреступника и развитие событий. Также стоит отметить сложность мошеннических схем в виртуальном пространстве.

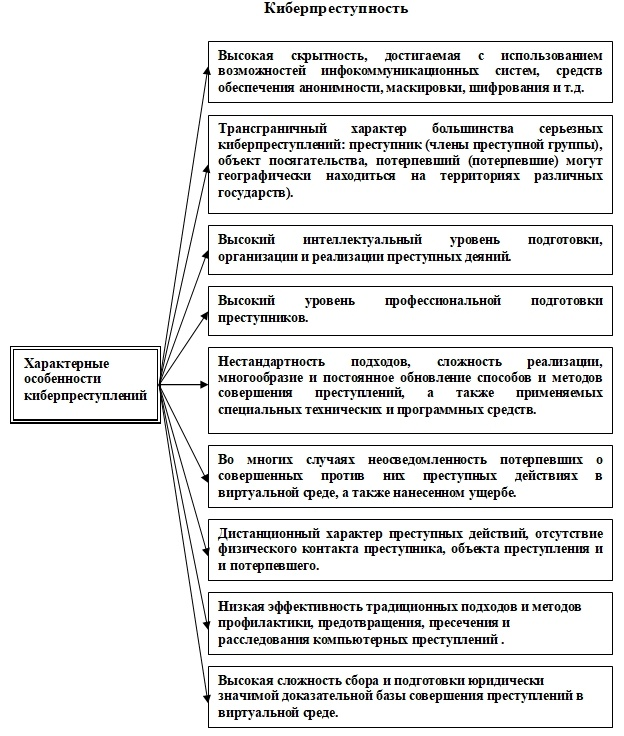


Рисунок 1 – Характерные особенности киберпреступлений. [4]

В этой связи следователям, ведущим расследования киберпреступлений, зачастую требуется трансграничный доступ к данным и обмен ими. Эта задача может быть выполнена в случае, если запрашиваемые данные сохраняются поставщиками услуг и принимаются меры, позволяющие правоохранительным органам оперативно взаимодействовать и сотрудничать с другими странами [19].

Основными правовыми проблемами при расследовании киберпреступлений и судебном преследовании киберпреступников являются: разные правовые системы, существующие в разных странах; различия в национальных законодательствах о киберпреступности; различия в нормах доказательственного права и уголовного судопроизводства (например, в процедурах получения доступа к цифровым доказательствам правоохранительными органами; например, на основании законного распоряжения, такого как ордер на обыск, или без него); различия в охвате и географической применимости региональных и многосторонних договоров о борьбе с киберпреступностью; и различия в подходах к защите данных и соблюдению прав человека [11].

Киберпреступления в современном мире являются довольно популярным вектором развития преступного мира. Данные противоправные деяния направлены практически на все сферы общественной жизни, а разновидность и масштабы данного вида преступлений постоянно растет. Стоит отметить, что четкого разделения на конкретные виды киберпреступлений нет. Из самых актуальных и повсеместных видов киберпреступлений можно выделить следующие.

Преступления, которые направлены против компьютерных систем и баз данных. Огромный перечень киберпреступлений можно отнести к данному виду — это и хакерские атаки, заражение интернет вирусами и вредоносными программами и т.д. В качестве примера можно отметить постоянные взломы баз данных мобильных операторов с дальнейшим использованием полученной информации в различных целях (получении паспортных данных, рекламные рассылки, последующее использование в мошеннических целях и т.д.)

Преступления, связанные с получением экономической выгоды, например, фишинг – самый распространенный вид мошенничества в интернете. Главная цель данного вида компьютерной угрозы - завладеть логином и паролем виртуальной учетной записи пользователя, и как следствие воспользоваться его личными данными в преступных целях (данные банковских карт, электронные кошельки и т.д.).

Большинство фишинговых кампаний предполагают массовую рассылку электронных писем как можно большему количеству пользователей, но также существует адресный фишинг, который отличается направленным характером. Этим способом злоумышленники атакуют конкретное лицо или организацию, часто применяя специально подобранный контент, который, как им представляется, окажет на жертву наибольшее воздействие. Клоновый фишинг предполагает, что злоумышленники копируют (клонируют) ранее доставленное законное сообщение, которое содержит ссылку или вложение. Затем мошенник меняет ссылки или прилагаемые файлы на вредоносные объекты, выдаваемые за настоящие. Ничего не подозревающие пользователи нажимают на ссылку или открывают вложение, чего часто бывает достаточно для хакеров, чтобы перехватить контроль над компьютером [12].

Одной из наиболее опасных угроз для физических лиц остается мошенничество с банковскими картами, или кардинг. В России объем рынка кардинга за анализируемый период оценивается в 663,4 млн долл. Большая часть скомпрометированных карт продается в специализированных «кардшопах». Ежемесячно в них загружается в среднем 686 тыс. текстовых данных карт. [7]

Преступления против свобод и неприкосновенности личности, к которым можно отнести, например, кибербуллинг. Основные жертвы данных преступлений – это несовершеннолетние. Кибербуллинг, или интернет-травля – это осознанные и целенаправленные оскорбления, угрозы, компроматы в виртуальном пространстве, которые длятся в течение продолжительного периода времени. Данная травля осуществляется посредством электронных писем, социальных сетей, видеопорталов и т.д. Данное преступное деяние можно трактовать как вмешательство в личное пространство и ущемление свобод и достоинств личности. Как показывает статистика, большинство жертв кибербуллинга – это подростки в возрасте от 12 до 17 лет.

Кибертерроризм. Данное понятие возникло вследствие очень сильной интеграции виртуального пространства с 158 государством и основными сферами жизни общества. Под данным термином понимают преступные действия, направленные на дезорганизацию электронной, информационной системы общества, в следствие которых может быть причинён большой вред человеку, обществу и государству. Основная особенность данного вида киберпреступления – масштабность. Логично предположить, что главная цель данного противоправного деяния – нанести как можно больший вред человеку, чтобы показать авторитет или, как правило, воздействовать на решения органов власти. [3]



Рисунок 2 – Классификация киберпреступлений [8]

Говоря о видах киберпреступлений, хотелось бы отдельно отметить ряд возможных интернет-угроз, которые тесно связаны и в определенном смысле раскрывают данное понятие. Большинство киберпреступлений направлено против виртуальных данных пользователей, а получить доступ к виртуальной среде возможно только посредством сети Интернет.

Итак, среди основных угроз можно выделить:

Спам – так называемая вредоносная реклама. Данная «рекламная информация» либо уже содержит шпионское ПО, либо переводит пользователей на сайт с вредоносной программой.

Фишинг – данное понятие раскрыто выше, однако хотелось бы отметить явное отличие фишинговых атак от спамов. Спамы, как правило, рассылаются огромной группе пользователей, а фишинг – имеет определенную целевую аудиторию, на основании общего, которым и рассылается вредоносные сообщения.

Повышенное внимание направлено на социальные сети и мобильные устройства − область, в которой пользователи менее информированы о киберугрозах. Хакерские атаки стали более сложными и профессиональными, направленными не только на отдельных пользователей, но и промышленные системы. Согласно исследованию компании Juniper Research, при сохранении текущего уровня кибератак общие убытки мировой экономики от их осуществления составили 2,1 триллиона долл. до 2019 г. [18]

Достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса. Рост киберпреступности связан преимущественно не с крупными предприятиями, а именно с предприятиями относительно небольших размеров. Такие предприятия в силу малого бюджета, отсутствия квалифицированных кадров, пробелов в познаниях сотрудников не могут на должном уровне обеспечить качественную информационную безопасность. Тем более, что потеря данных или же их компрометация не влияют существенным образом на их функционирование, положение на рынке, уровень доверия потребителей, наконец, размер получаемой прибыли.

## **1.2 Киберпреступления в экономической сфере**

Произошла определенная переориентация направленности киберпреступности на получение преимущественно финансового результата. В отличие от распространения вирусов, направленных на создание бот-сетей (распространение ботнетов – сетей инфицированных компьютеров), осуществляющих атаки независимо от пользователей, причиняющих ущерб большому количеству пользователей, целевые атаки хакеров ориентированы на конкретное предприятие или конкретного пользователя [17].

Такие действия связаны с предварительным изучением хакерами своего объекта нападения. Сторона нападения совершает атаку в неожиданный момент, после подборки необходимых инструментов, и действует почти бесследно. Компьютерный шпионаж, операции с компьютерными системами не только сложно зафиксировать и доказать как противоправное действие, но и точно персонифицировать нарушителя и его географическое местонахождение.

К ключевым рискам в кредитно-финансовой сфере эксперты Банка России относят: финансовые потери клиентов (потребителей финансовых услуг), которые подрывают доверие к современным финансовым технологиям; финансовые потери отдельных финансовых организаций, которые могут отрицательно воздействовать на их финансовое положение; нарушение надежности операционной деятельности и непрерывности предоставления финансовых услуг, что может нанести ущерб репутации финансовых организаций и способствовать усилению социальной напряженности в обществе; возникновение системного кризиса из-за значимых для финансового рынка инцидентов информационной безопасности [6].

Финансовые угрозы — вредоносное ПО, атакующее пользователей онлайн-банкинга, электронных кошельков, криптовалют или инфраструктуру финансовых организаций. Как правило, их атаки сопровождаются спамом и фишингом: злоумышленники создают поддельные веб-страницы и электронные письма, якобы связанные с финансовой сферой, чтобы украсть личные данные пользователей.

Интернет-банкинг по-прежнему остается одним из лидеров в перечне киберпреступлений. Банковские учреждения, независимо от времени и технических достижений, являются привлекательной целью для быстрого получения богатства. Электронные технологии, с одной стороны, снизили себестоимость оказываемых услуг, с другой стороны, расширение применения данных технологий увеличило возможности киберпреступников в совершении незаконных финансовых операций, что повысило риски обеспечения финансовой безопасности в банках.

Преступники обогащаются за счет кибершантажа, вымогательства, снятия денежных средств со счетов клиентов банка. Незаконное получение реквизитов банковских карт осуществляется злоумышленниками при осуществлении владельца денежных средств различных финансовых операций с помощью электронного банкинга, с SIM карт мобильных телефонов. Дистанционное банковское обслуживание требует комплексной защиты от фишинга для того, чтобы предотвратить изъятие конфиденциальной информации, хищение паролей [16].

Распространению киберпреступности в банковской сфере способствует использование банками устаревших технологий, не способных противостоять преступникам. Непростая экономическая ситуация в стране не подталкивает к значительному инвестированию банков в замену оборудования, установления современного высококачественного программного обеспечения. Банки вынуждены соизмерять степень риска и стоимость мероприятий по повышению уровня экономической безопасности. В свою очередь, отсутствует законодательный механизм ответственности производителей программного обеспечения перед своими клиентами. Предлагаемые продукты ПО в ряде случаев имеют слабую устойчивость к хакерским атакам и не соответствуют требованиям по безопасности.

Атаки на финансовые организации обычно осуществляют хорошо организованные преступные группы, в состав которых входят организаторы, принимающие стратегические решения, квалифицированные программисты и инсайдеры кредитно-финансовой сферы (из числа действующих либо бывших сотрудников) [17].

Хакеры используют слабые места в программном обеспечении пользующихся популярностью серверов, в первую очередь, социальных сетей, различных государственных служб, учреждений. Социальные сети особенно привлекательны для преступной деятельности в силу популярности у большого числа людей, безосновательного доверия к ним в плане безопасности. Доступ к таким сетям дает возможность, при распространении вредоносных программ, получить в свое пользование огромные объемы конфиденциальной информации, среди которой можно найти данные для последующего онлайн мошенничества, шантажа, перепродажи информации заинтересованным лицам.

Комплекс мер, считают эксперты, может помочь финансовым организациям снизить риск кибератак. Это достаточно простые, но полезные и обязательные к исполнению действия, касающиеся использования (и своевременного обновления) антивирусного и офисного программного обеспечения, операционных систем, браузеров, приложений, учетных записей, а также контроля доступа пользователей к критичным ИТ-системам, проведения тренингов с сотрудниками организации и представителями клиентов и др. Если организация не в состоянии самостоятельно справиться с кибератакой, то эксперты рекомендуют привлекать структуры, компетентные в вопросах информационной безопасности [11].

Для эффективного противодействия виртуальным преступникам также необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты. Система кибербезопасности включает в себя многообразные компоненты, в т.ч. повышение уровня цифровой грамотности населения, содействие в продвижении индивидуальных способов защиты личной информации, механизмы по противодействию и профилактике киберугроз. Кроме значительного экономического ущерба, кибератаки приводят к изменениям в геополитических отношениях и снижению уровня доверия к сети Интернет и в конечном счете могут спровоцировать финансовый кризис.

# **2. Анализ борьбы с киберпреступностью в современном мире**

## **2.1 Особенности и проблемы борьбы с киберпреступностью в России**

Расследованиями киберпреступлений по всему миру занимается ряд международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий. Они не только осуществляют сбор первичных данных об имевших место инцидентах информационной безопасности, но и проводят их анализ и делают прогнозы относительно потенциальных киберугроз.

В последние годы задача обеспечения информационной безопасности финансовых организаций и развития устойчивой и защищенной цифровой инфраструктуры в России является одним из стратегических приоритетов Банка России. В своем выступлении в Совете Федерации глава Банка России Э. Набиуллина подтвердила намерение и дальше «усиливать надзор, стимулировать банки тщательно подходить к вопросам кибербезопасности». «Киберустойчивость — это не просто поставить на компьютер антивирусную программу, нужно писать требования киберустойчивости ко всем бизнес-процессам. Именно это критически важно для следующего динамичного развития технологий», - добавила она.

К сожалению, российские банки и другие финансовые организации пока еще не научились управлять киберрисками: в ходе проверок банков на предмет киберустойчивости, которые проводил Банк России в 2019 г., было выявлено более 730 нарушений. Около 80% связаны с недостаточным уровнем информационной защиты в финансовых организациях. Хотя пока обнаруженные проблемы не являются критическими, указала Э. Набиуллина на Международном конгрессе по кибербезопасности, в любой момент они могут стать таковыми, если их не решать [9].

Крупнейшим частным игроком на рынке расследований киберпреступлений в России является Group-IВ, созданная в 2003 г. Она принимала участие в расследовании первых в России DDoS-атак, хищений средств с помощью вирусов для мобильных телефонов и целевых атак на банки. Сейчас ее деятельность вышла за пределы нашей страны. Компания имеет опыт расследования киберпреступлений по всему миру и сотрудничает с Интерполом и Европолом, а также с российскими провайдерами, специализирующимися на разработке программного обеспечения для финансовой сферы, защите информационных систем и т.д. Group-IВ регулярно публикует результаты своих расследований [15].

К основным причинам динамичного роста киберпреступности в России большинство исследователей относят:

1. Непроработанность российского уголовного и уголовно-процессуального законодательства: многогранность, запутанность норм, лояльные санкции, неотражение всего спектра современных преступлений в киберпространстве. Строгие санкции за киберпреступления предусмотрены законодательством США: тюремное заключение сроком до 20 лет предусмотрено повторно совершившему преступление, повлекшее тяжкие последствия, а лишение свободы сроком до 30 лет без права досрочного освобождения – для проникших в компьютерные инфраструктурные сети США (телесети, энергосети, сети водоснабжения и др.) [10]. Максимальный же срок лишения свободы по санкциям статей гл. 28 УК РФ – 7 лет.

2. Недостаточный уровень образования сотрудников правоохранительных органов (дознавателей, следователей, экспертов и др.), участвующих в расследовании киберпреступлений. Следует отметить, что IT-преступления – самые сложные в расследовании, требующие от сотрудников наличия специальных ресурсов, опыта, знаний. Очередь на проведение компьютерных экспертиз в государственных экспертных учреждениях превышает полгода, хороших специалистов в правоохранительной сфере в этой части единицы. На практике получается, что расследовать IT-преступления поручают сотрудникам с юридическим образованием, хотя, в большинстве передовых стран специалисты по киберпреступлениям имеют в качестве основного высшее техническое образование и в качестве дополнительного – юридическое.

3. Совершенствование киберпреступности как индустрии: вход в данный сегмент свободный, научиться взламывать сайты, электронные почтовые переписки, создавать и распространять вирусные программы легко научиться, изучив информацию в свободном доступе сети Интернет.

4. Низкий уровень грамотности, информированности и защищенности населения: минимальные, базовые знания о компьютерной и цифровой безопасности (гигиене), правовой нигилизм. Правовой нигилизм представляет собой негативное отношение к закону, праву и правовым формам организации общественных правоотношений. Уровень правового нигилизма выступает в качестве своеобразного показателя здоровья государства и общества. Формы выражения правового нигилизма — усиление настроений социальной пассивности; развитие социальных болезней, наркомании и алкоголизма; повышение уровня преступности; моральная деградация; увеличение количества суицидов). [2]



Рисунок 3 – Статистика киберпреступлений в России [4]

Борьбе с киберпреступлениями препятствует и неопределенность в правовом статусе криптовалюты. Так, в июле 2020 года Петроградский районный суд Санкт-Петербурга, вынося приговор по делу злоумышленников, которые под видом сотрудников ФСБ принудили предпринимателя перечислить им 5 млн рублей, 99 биткойнов и более мелкие суммы в криптовалюте на общую сумму 50 млн рублей, признал, что потерпевший перевел цифровые средства под действием угроз, но не посчитал это материальным ущербом, ссылаясь на "отсутствие правового статуса" криптовалюты.

При этом в мае 2018 года в решении по другому делу арбитражный суд фактически разрешил взыскание криптовалюты с должников, а в 2019 году Верховный суд России признал, что взятка в криптовалюте может считаться преступлением. Поэтому, по мнению Генпрокуратуры, требуется скорейшая выработка единых подходов к регулированию оборота цифровой валюты на законодательном уровне. [5]

## **2.2 Перспективы усиления кибербезопасности в России**

Для России одной из причин появления главы 28 УК РФ стало вхождение в мировое информационное сообщество, уже хорошо знакомое с компьютерными преступлениями. За рубежом к таким преступлениям относят не только традиционные преступления против собственности, например кражи и мошенничества, совершаемые с использованием средств и возможностей компьютерной техники, но и целый ряд других, новых для уголовного законодательства деяний, состоящих в злоупотреблениях такой техникой (распространение вредоносных программ, компьютерный шпионаж и др.).

Необходимо отметить, что в Российской Федерации, как и в других государствах, при разработке комплекса мер по противодействию киберпреступности основное внимание уделяется формированию правовых основ этой деятельности, а также проблемам предупреждения, пресечения, расследования преступлений, связанных с использованием информационно-коммуникационных технологий, устранением причин и условий, способствующих их совершению.

За последние годы Банк России, опираясь на мировой опыт, предпринял ряд важных шагов, нацеленных на повышение информационной безопасности финансовой сферы. Так, были разработаны и введены общие требования к информационной инфраструктуре банков, их программному обеспечению, системе хранения персональных данных, методам идентификации, криптографической защите данных и т.д.

Банком России принят комплекс документов, описывающий единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства - Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ (СТО БР ИББС). Он касается безопасности финансовых (банковских) операций, аутсорсинга, аудита, сбора и анализа данных при реагировании на кибератаки, оценки соответствия информационной безопасности организаций банковской системы требованиям и др.

Внедрение Стандарта должно способствовать повышению доверия к банковской системе России и стабильности ее функционирования, использованию адекватных мер по защите от реальных угроз информационной безопасности, предотвращению и снижению ущерба от кибератак, так как одной из стратегических задач Банка России является также защита потребителей финансовых услуг от мошенничества и хищений средств.

В начале марта 2020 г. Банк России сообщил о том, что начинает штрафовать банки за отсутствие систем распознавания мошеннических операций. Речь идет о технологиях, позволяющих отслеживать нетипичные для клиентов операции, которые потенциально может совершать мошенник.

Что же касается достижения прямой пропорциональности роста киберпреступности уровню ее раскрываемости, эффективного уровня безопасности общества и государства в области IT-технологий наиболее правильными будут следующие шаги:

− выделение дополнительного финансирования для обучения высококвалифицированных кадров для противодействия киберпреступности в правоохранительной системе, увеличение штатной численности оперативных сотрудников, дознавателей, следователей, технических специалистов, экспертов в области IT-технологий за счет сокращения штата управленческого аппарата системы МВД России;

− обязательное повышение компьютерной грамотности населения (начиная от дошкольных и школьных учебных заведений до групп населения пенсионного возраста): обучение правилам безопасности работы с цифровыми устройствами и в Интернет-сети с представлением показательных алгоритмов негативных ситуаций;

− изменение подхода бизнес-структур к информационной безопасности посредством обучения и правовой регламентации ответственности в локальных нормативных правовых актах организаций;

− пересмотр санкций уголовных норм об ответственности за киберпреступления с целью их ужесточения по примеру зарубежных стран (например, США).

Развитие механизма страхования организаций в случае кибератак в том числе может способствовать стабилизации ситуации и контролю над киберпреступлениями. Но на данный момент такой вид страхования – редкость для отечественного рынка. Например, программы страхования от кибер-угроз предлагают «АльфаСтрахование», «Сбербанк Страхование», «Согаз», «Альянс» и ещё нескольких крупных игроков рынка [14].

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.

Из этого можно сделать вывод, что необходимым условием обеспечения информационной безопасности является наличие квалифицированных кадров, в связи с чем Банк России планирует содействовать сотрудничеству между вузами и финансовыми организациями. Развитие различных форм такого сотрудничества позволит модернизировать учебный процесс с учетом современных требований в области информационных технологий и информационной безопасности и в конечном счете готовить специалистов, способных своевременно и эффективно реагировать на преступные действия злоумышленников. В связи с трансграничным характером киберугроз Банк России считает необходимым и дальше развивать международное сотрудничество в области кибербезопасности [9].

В частности, намечено расширять участие экспертов Банка России в деятельности ряда международных организаций. Кроме того, Банк России считает необходимым взаимодействовать с центральными банками иностранных государств, в том числе и с регуляторами стран Евразийского экономического союза, а также с международными сообществами и национальными группами по реагированию на киберинциденты.

# **ЗАКЛЮЧЕНИЕ**

Киберпреступность прошла фазу становления, «детства» и перешла на принципиально новый уровень, включающий вымогательство, промышленный шпионаж, таргетированные атаки. Изменился и сам хакер: из любителя превратился в профессионала, являющегося частью криминального бизнеса. Киберпреступники наносят значительный ущерб как отдельным гражданам, организациям, предприятиям, так и всей национальной экономике при минимальном для себя риске.

Борьба с киберпреступностью становится одной из глобальных проблем вследствие все большего усовершенствования и расширения спектра информационных технологий, глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей. Злоумышленники идут на несколько шагов вперед, увеличивая отрыв от систем безопасности компаний. Решение же проблемы киберпреступности состоит не в подстраивании компаний под существующие тенденции, а в активной разработке информационной безопасности стратегии предприятий на опережение.

Для реализации данной стратегии 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.

Совершенно очевидным стал факт невозможности противостояния экономическим преступлениям, в частности киберпреступности, исключительно на национальном уровне, без активного взаимодействия с аналогичными международными организациями, координирующими и оказывающими помощь в борьбе и противодействии преступным действиям.

Несовершенство законодательства приводит к отсутствию на национальном уровне механизма регистрации жалоб населения на кибермошенничество. Для эффективного противодействия виртуальным преступникам необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты.

Наконец, пользователям необходимо научиться быть менее беспечными, самим позаботиться о своей безопасности. Интегративный и комплексный подходы в применении правоохранительными органами профилактических мер могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным.

Предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Головинов, О.Н., Погорелов, А.В. (2016). Киберпреступность в современной экономике: состояние и тенденции развития. 2016.
2. Жвавый П. С. К вопросу о преодолении правового нигилизма в современной России / П. С. Жвавый, Н. М. Добрынин // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2017. Том 3. № 4. С. 182-198.
3. Айков, Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх. –М.: Мир, 2018г. – 95 с.
4. Николюк М. С. Влияние пандемии на угрозу со стороны киберпреступности в России и мире. 2020.
5. Рогоза А.А., Сабиров В.Д., Лаптева А.В. Меры по борьбе с киберпреступностью в России, 2020. С. 68-72.
6. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019­-2021 годов. – М.: ЦБ РФ, 2019. – 26 с.
7. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году / Банк России, ФинЦЕРТ. – 2019. – 86 с.
8. Киберпреступность: история развития, проблемы практики расследования URL: https://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/ (дата обращения 08.05.2021)
9. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 77-96.
10. Зарубежное законодательство на русском языке URL: http://www.worldbiz.ru. (дата обращения 03.05.2021)
11. Борисова Е.С., Белоусов А.Л. Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Актуальные проблемы экономики и права. – 2019, № 3. – С. 1330-1342.
12. Николюк М. С. Влияние пандемии на угрозу со стороны киберпреступности в России и мире. Год: 2020. С: 185-192.
13. Волков К. В. Киберпреступность. Виды и особенности ее влияния. 2019. С. 249-255.
14. Просветова А.А., Дубкова Е.В. Кибер-страхование как способ обеспечения информационной безопасности // Международный журнал гуманитарных и естественных наук. 2020. №4-3.
15. Лобач Д. В., Смирнова Е. А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2019. – № 4. – С. 23–32.
16. Витлякова С. С. Киберпреступность как угроза национальной безопасности (национальным интересам). 2019. С. 91-97.
17. Кленков А.С. Преступления в сфере компьютерной информации. Основные подходы к определению понятий // Юридический факт. 2018. С. 86-90.
18. Гундерич Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018.
19. Комлев Ю.Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник КЮИ МВД России. 2020.
20. Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. С. 44–47.