МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Факультет экономический
Кафедра теоретической экономики

КУРСОВАЯ РАБОТА
по дисциплине «Электронный бизнес»

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, ВИДЫ И СПОСОБЫ БОРЬБЫ С НЕЙ

Работу выполнила _____ П.С. Титова
(подпись, дата)
Направление подготовки 38.03.05 – Бизнес-информатика курс 3
Направленность (профиль) Электронный бизнес

Научный руководитель
канд. экон. наук, доцент _____С.М. Геворкян
(подпись, дата)

Нормоконтролер
канд. экон. наук, доцент _____С.М. Геворкян
(подпись, дата)

Краснодар
2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования заключается в том, что за последние десятилетия число киберпреступлений в мире увеличилось в огромное количество раз, мотивы и цели киберпреступников менялись с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Этому свидетельствуют огромные финансовые потери юридических лиц и структур, а также участившиеся случаи киберпреступлений и против физических лиц.

Эту стремительно возрастающую по своим масштабам проблему необходимо как можно быстрее начать эффективно решать, потому что уровень киберпреступности и сложности преступлений растет, а раскрываемость дел и эффективность работы против преступников в киберпространстве падает. Данная тема *актуальна* на сегодняшний день, потому что расходы на предотвращение и раскрытие киберпреступных дел растет, все большее количество юридических и физических лиц пытается обезопасить себя заранее, но преступнике в киберпространстве не стагнируют, а усложняют методы и виды преступлений, потому данная сфера нуждается в постоянном контроле и поиске решений.

Целью работы является исследование киберпреступности, ее понятия, видов и способов борьбы с ней.

Цель определяет следующие *задачи*:

– определение понятия и видов киберпреступности,

– рассмотрение развития и мотивов киберпреступности,

– изучение экономических киберпреступлений,

– изучение состояния киберпреступности на сегодняшний день,

– рассмотрение методов борьбы с киберпреступностью в Российской Федерации и рассмотрение вариантов мирового сотрудничества по борьбе с киберпреступностью.

Объектом курсовой работы является киберпреступность как явление.

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

Информационную базу исследования научной работы составили: нормативно-правые акты, официальные данные, предоставленные Генеральной прокуратурой Российской Федерации, периодические издания и литература, а также труды и работы отечественных авторов.

В данной работе будем использовать общенаучные методы исследования, такие как описание, анализ, обобщение, системно-структурный анализ.

В первой главе будет рассмотрена теоретическая основа изучения вопроса о явлении киберпреступности, а вторая глава будет основываться на современной статистике, а также методах, используемых в борьбе с киберпреступностью сегодня.

Во второй главе будут рассмотрены: состояние киберпреступности на сегодняшний день, а также способы борьбы с ней, использующиеся в современном мире.

Структура работы. Работа изложена на 30 страницах, содержит 10 рисунков, 4 таблицы, состоит из введения, в котором отражается актуальность работы, объект, предмет цели и задачи работы, двух глав, раскрывающих сущность работы, а также заключения и списка использованной литературы.

1 Теоретические аспекты изучения явления киберпреступности

1.1 Понятие и сущность киберпреступности

Понятие «киберпреступности» на сегодняшний получило большое распространение в связи с информационно-телекоммуникационным прорывом, произошедшим в XXI в. Киберпреступность – совокупность преступлений, совершаемых в «киберпространстве» с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных. К «киберпреступлению» относится любое преступление, совершенное с применением различных способов и средств создания, обработки, передачи компьютерной информации [4].

Термин «киберпреступность» также часто употребляется вместе с термином «компьютерная преступность», причем часто синонимично. Стоит отметить, что термин «киберпреступность» более расширенный, чем «компьютерная преступность», так как более точно отражает природу такого явления, как преступность в информационном пространстве.

Таким образом «киберпреступность» – это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. В то же время термин «компьютерная преступность» относится только преступлениям, совершаемым против компьютеров или компьютерных данных [13].

Большинство преступлений, которые совершаются в глобальных компьютерных сетях, характеризуются следующими особенностями [13]:

1 Повышенная скрытность совершения преступления.

2 Трансграничных характер сетевых преступлений, при котором преступник, объект преступного посягательства и потерпевший могут находиться на территориях разных государств.

3 Особая подготовленность преступников, интеллектуальных характер преступной деятельности.

4 Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно.

5 Неосведомленность потерпевших о том, то они подверглись преступному воздействию.

6 Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.

7 Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.

Сегодня киберпреступность содержит в себе обширный диапазон противоправных действий – от неразрешенного вторжения в компьютерные сети, краж индивидуальной данных до финансового шпионажа и отмывания наличных средств. Как отмечают некоторые авторы, в последние годы интернет-ресурсы используются во всех циклах торговли людьми и запрещенными предметами, а также в последующей легализации преступных доходов [6].

Субъектами преступлений, активно использующими высокие технологии, наряду с лицами, выполняющими профессиональные функции в организациях и на предприятиях, становятся практически любые лица. При этом преследуемые ими цели, используемые методы и располагаемые ими возможности практически не отличаются от тех, которые присущи преступникам по роду занятости. Помимо объединения киберпреступников по группам, можно объединить по определенным группы и жертв киберпреступности, которые представлены в таблице 1. Таким образом, в таблице 1 рассмотрена классификация киберпреступников, а также, то, каким образом можно разделить на группы жертв киберпреступлений, но стоит отметить, что данная таблица делит жертв киберпреступности на группы, как отдельных граждан, другая классификация по объекту киберпреступления будет рассмотрена в таблице 2.

Таблица 1 – Групповые элементы киберпреступности и их основные типы (составлена автором [4])

Основные типы групп	Подтипы группы
Группы как преступники	Группировки, использующие информационные технологии для преступлений
	Традиционно организованные кибер-преступные группы
	Идеалогически и политически мотивированные кибер группы
	Группы, которые используют технологии для мобилизации и действий
Группы как жертвы	Раса
	Возраст
	Инвалидность
	Религия
	Пол
	Сексуальная ориентация

Киберпреступники используют свой арсенал информационного оружия, представляющий собой совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения.

К основным видам информационного оружия относят следующие [4]:

1 Бэкдор – данный инструмент предполагает скрытый метод в системе, который позволяет получить доступ к защищенной области.

2 Компьютерные вирусы – специальные программы, которые внедряются в программное обеспечение компьютеров, уничтожают, искажают или дезорганизуют его функционирование. Они способны передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п. Кроме того, “вирусы” способны самостоятельно размножаться.

3 «Логические бомбы» – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры инфраструктуры, чтобы по сигналу или в установленное время привести их в действие.

4 Программное вредоносное обеспечение – программы или утилиты, которые после установки выполняет незаявленные функции в фоновом режиме.

5 Нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения.

6 Анализаторы трафика (sniffer) – программы или устройства, которые контролируют данные, передаваемые по сети. Традиционно используемые для законных функций сетевого управления, они могут применяться и во время кибератак с целью кражи информации.

7 DDos-атаки – предназначены для нарушения доступа к сети, как правило, при помощи выполнения миллионов запросов каждую секунду в результате чего доступ к сети затрудняется или нарушается.

8 Киберпреступления, совершаемые с помощью e-mail – это метод отправки электронной почты с подменой источника, используется для того, чтобы заставить получателя предоставить конфиденциальную информацию.

9 Keylogger – представляет собой программное или аппаратное средство, предназначенное для контроля нажатия клавиш на клавиатуре компьютера, для получения пароля, пин-кода или другой информации.

В таблице 1 была рассмотрена классификация отдельных граждан, как жертв киберпреступности, также можно рассматривать, как объекты киберпреступность еще бизнес-структуры и государство – это основные объекты киберпреступлений, которые наносят неоценимый ущерб, как отдльным объектам, так и экономике в целом. По отношению к каждому из этих объектов могут быть совершены определенные виды киберугроз. Объекты и виды угроз представлены в таблице 2, а по отношению к

представленным в таблице 2 объектам могут быть совершены те виды атак, которые были рассмотрены выше.

Таблица 2 – Объекты и виды киберугроз (составлена автором [4])

Объект угроз	Виды угроз
Граждане	Воздействие на личность путем сбора персональных данных и атак на персональные компьютеры и мобильные устройства граждан
	Утечка и обнародование частной информации
	Мошенничество
	Распространение опасного контента
Бизнес	Воздействие на системы интернет-банкинга
	Воздействие на информационную инфраструктуру
	Блокирование систем онлайн-торговли, геоинформационных систем
	Хакерские атаки на сайты компаний
Государство	Атаки на ключевые государственные системы управления (электронное правительство, сайты государственных структур)
	Экономическая блокада (масштабное отключение платежных систем, систем бронирования)
	Аппаратные атаки на персональные компьютеры и критически важную инфраструктуру государственных предприятий

Виды киберпреступности можно классифицировать также и в виде четырех основных блоков, представленных на рисунке 1.

Рисунок 1 – Основные виды киберпреступности (составлен автором [12])

Рассмотрим каждый из блоков подробнее [7]:

1 Финансовая сфера является одной из самых незащищенных от киберпреступности: с развитием современных сфер коммуникации подавляющая часть денежных потоков стала носить безналичный характер, что существенно упростило преступникам совершать хищения со счетов банков и со счетов пластиковых карт обычных граждан.

2 Касаясь проблемы взлома, хищения баз данных, а также хакерских атак и распространения вирусов, следует отметить, что проблемами предотвращения данных видов угроз является невозможность прогнозирования потенциальных проблем, использование идентичного ПО в различных устройствах, что увеличивает эффективность эксплуатации технических уязвимостей, а также нехватка кадров в области киберзащиты.

3 Незаконное вторжение в частную жизнь получает наибольшее распространение с каждым годом: люди по всему миру пользуются современными гаджетами, а они в свою очередь могут рассказать преступнику, как местоположения пользователя, так и более личную и конфиденциальную информацию. Таким видом преступления пользуются не только вымогатели, но отделы маркетинга компаний, которые отслеживая личную информацию потенциального потребителя, строят анализ его предпочтений, таким образом выстраивая целевую рекламу и занося информацию о нем в свои базы данных.

4 Незаконное присвоение интеллектуальной собственности также является распространенным видом киберпреступности, так как с развитием IT технологий (как следствие и развития киберпреступности), создатели интеллектуальной собственности, которая подвергается опасности со стороны киберпреступлений, как правило, не могут воспользоваться экономическими плодами своей собственной работы, тем самым подрывая стимулы к осуществлению необходимых инвестиций в развитие своего продукта, а также создатель интеллектуальной собственности будет находиться в невыгодном положении по отношению к тому, кто просто скопировал его наработки, так как создатель вкладывал в разработку идеи финансы и время.

Таблица 3 – Новые концепции киберпреступности (составлена автором [5])

Киберпреступность	
Кибертерроризм	Угроза кибертерроризма может исходить от террористических и экстремистских организаций, отличается большой масштабностью, интенсивностью и огромными последствиями.
Сетецентрическая война	В тактике и искусстве войны за последнее время произошли принципиальные перемены, требующие от правительств государств пересмотра прежних военных доктрин, переоценки области военного искусства, сетецентрическая война и кибер война – принципиально новые виды ведения войн против государств, которые требуют особого подхода и противодействия.
Кибервойна	

В связи со стремительным развитием информационных технологий, киберпреступность расширилась и включает в себя на сегодня новые серьезные угрозы, которые представлены и описаны в таблице 3.

Переходя к развитию киберпреступности, можно сделать вывод: преступления в Сети наиболее новая и динамично развивающая сфера деятельности для злоумышленников. Формы киберпреступности видоизменяются и распространяются на все новые достижения научно-технического прогресса. 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.

1.2 Развитие и мотивы киберпреступности

Говоря о киберпреступности, необходимо понимать, что данное явление является следствием мирового распространения IT-технологий, если же сравнивать киберпреступность с другими видами преступной деятельности, то киберпреступность растет гораздо большими темпами. Это связано со следующими факторами [8]:

1 Постоянное увеличение числа пользователей компьютеров и сети Интернет.

2 Постоянное повышение уровня профессионализма преступников в киберпространстве.

3 Совершенствование, развитие IT-технологий.

То есть все, что связано с развитием IT технологий, является почвой для совершения киберпреступлений.

Развитие и совершенствование информационных и технических средств не единственная вещь, которая влияет на трансформацию и развитие киберпреступности.

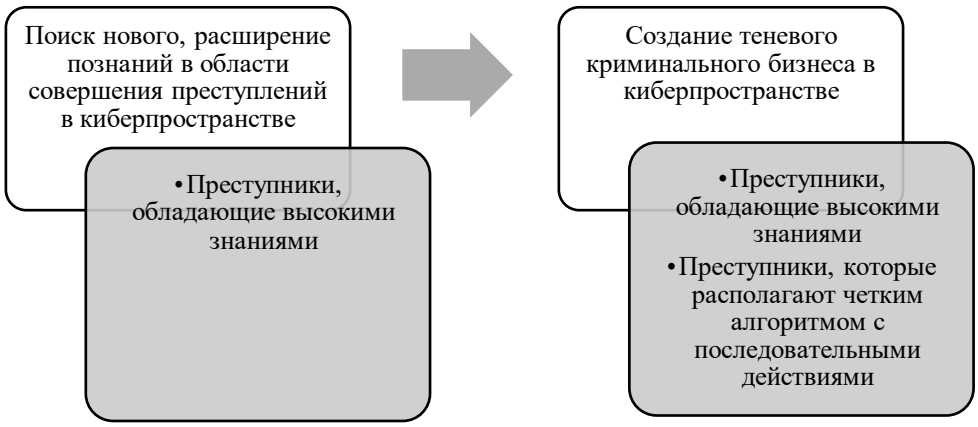

Рисунок 2 – Изменения в мотивации совершения киберпреступных действий (составлен автором [11])

На рисунке 2 представлено изменение мотивации киберпреступников, а также расслоение киберпреступников на две группы в трансформированной стадии мотивации киберпреступников.

Основные причины трансформации киберпреступности в теневой бизнес представлены на рисунке 3.

Рисунок 3 – Причины развития киберпреступности как теневого бизнеса (составлен автором [3])

Говоря о незначительном риске наказуемости подразумевается то, что киберпреступность глобальна и не имеет геополитических разграничений, это значит, что органам власти трудно тяжелее найти киберпреступника, а международные расследования и кооперация требуют больших финансовых средств. Растущая лояльность общества к киберпреступникам обуславливается тем, что киберпреступник часто рассматривается обществом за свободу слова, бесплатное программное обеспечение, интернет блага, таким образом часто владельцы бизнеса задумываются о ведении теневого бизнеса через интернет, а также обеспечения его защиты через теневые киберструктуры, в таком случае угрозой уже будут считаться государственные структуры. И, наконец, третья причина развития киберпреступности как теневого бизнеса подразумевает простоту совершения киберпреступлений: в сети Интернет можно найти множество материала, алгоритмов, объяснений совершения киберпреступлений [3].

Группа преступников, которая обладает высокими знаниями в области совершаемого киберпреступления, является наиболее опасной и может обладать следующими качествами [5]:

1 Киберпреступные действия зачастую находятся под юрисдикцией разных государств и являются трансграничными.

2 Киберпреступник имеет возможность объединять средства совершения киберпреступления (например, компьютеры) в единый механизм в автоматизированном режиме.

3 Преступник обладает такими личными качествами, как высокие профессиональные и интеллектуальные данные.

4 Киберпреступления могут быть совершены анонимно.

5 Отсутствие знания о совершенном преступлении жертвы киберпреступления или получения данного знания с временной задержкой.

6 Отсутствие у преступника необходимости вступать в прямой контакт с жертвой киберпреступления.

Таким образом, высокая опасность киберпреступности объясняется прежде всего возрастающей ролью системы общественных отношений, которым она угрожает, ее глобальным и организованным характером, наличием у хакеров и киберпреступников высокой степени знаний в области совершаемых киберпреступлений.

Подводя итог, можно сказать, что киберпреступность уже прошла фазу становления и перешла на новый уровень, а с каждым днем она развивается. 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.

1.3 Экономические киберпреступления

Основными факторами, оказывающими воздействие на совершение киберпреступлений экономического характера, являются:

– экономически кризис,
– повышение цен на товары первой необходимости,
– снижение уровня жизни,
– повышение уровня безработицы.

Основными источниками преступлений, совершаемых в кибер пространстве являются:

– незаконная предпринимательская деятельность,
– незаконная банковская деятельность,
– организация, проведение азартных игр.

Интернет, помимо площадки незаконной деятельности, являет собой место для легализации денег, полученных преступным путем. Всемирная сеть и образованное ею киберпространство создали единственную среду и

уникальные условия для осуществления преступной деятельности (легализация денежных средств, полученных преступным путём, получение быстрого и стабильного дохода). Некоторые из таких способов иллюстрированы на рисунке 4. Легализация денежных средств в киберпространстве создаёт трудности в правоприменительной практике, и это, в свою очередь, приводит к необходимости совершенствования законодательства.

В совокупность способов легализации денежных средств, полученных в результате совершения киберпреступления входят: использование социальных сетей, сайты-аукционы, сайты-объявления, помимо данных средств злоумышленник может открывать собственные сайты разной направленности, а также использовать уже существующие интернет-банки, криптовалюту биткоин (рисунок 4).

Таким образом, для легализации денег используются привычные операции, которые может совершать любой человек.

Рисунок 4 – Основные способы легализации денежных средств в киберпространстве (составлен автором [10])

Одним из распространённых способов легализации денежных средств является продажа несуществующего имущества через сайты-объявления. Преступник создаёт несколько аккаунтов на сайте, регистрируясь под разными именами с разных адресов, и выставляет на сайте различные товары, главное, при этом фактическое наличие товаров отсутствует. Далее в качестве покупателя использует денежные средства, полученные преступным путём. Метод проиллюстрирован на рисунке 5. Во-первых, правонарушитель переводит деньги в электронную валюту на заранее созданные ложные аккаунты электронных денежных систем. Во-вторых, переводит деньги с этих аккаунтов на электронные кошельки якобы различных покупателей. В-третьих, злоумышленник от имени каждого «ложного покупателя» покупает несуществующие товары, которые он же и выставил на продажу в качестве продавца. В результате осуществления этой схемы полученные деньги переводятся на действительный банковский счет. В качестве подтверждения легальности полученного дохода может быть предоставлена выписка из истории покупок сайта или иные документы, свидетельствующие о правомерном характере дохода.

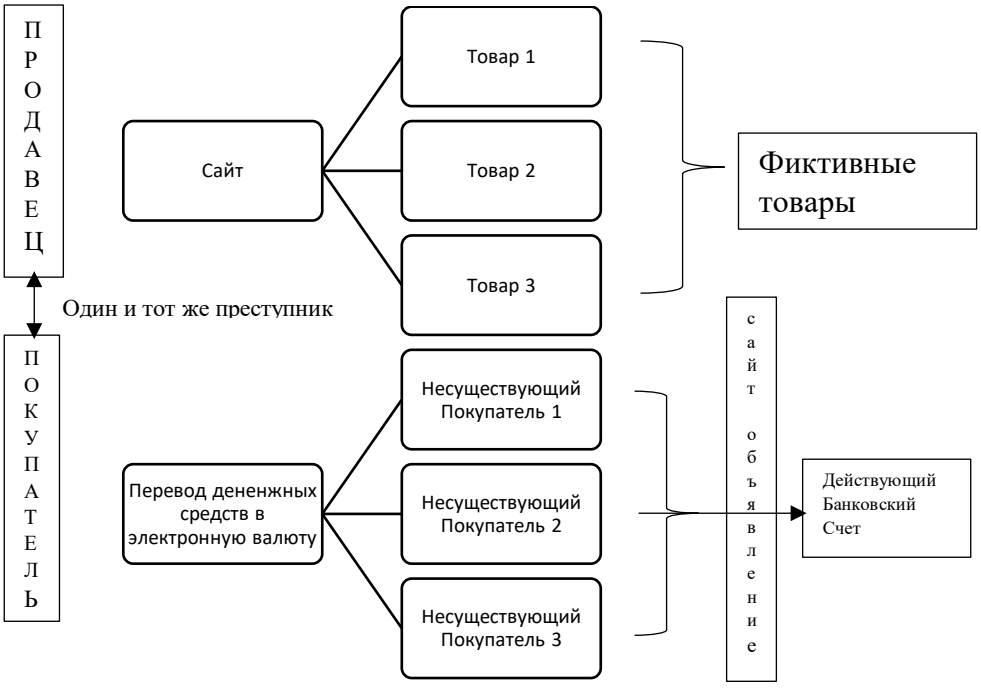

Рисунок 5 – Схема продажи несуществующего имущества (составлен автором [10])

С появлением новых технологий наблюдается появление новых, более сложных видов преступности. Это свидетельствует о том, что преступники достаточно оперативно используют результаты научно-технического прогресса в своих целях. Данная тенденция представляет серьёзную угрозу всем общественным отношениям, складывающимся в киберпространстве, поскольку на данном этапе развития киберпространство и общество уже неразрывны. Главными причинами и условиями существования экономической киберпреступности являются анонимность пользователей киберпространства и анонимность информационных сетей, техническое несовершенство, а также низкий уровень информационной безопасности людей. Правоохранительным органам становится известна лишь малая часть совершаемых экономических киберпреступлений.

2 Место киберпреступности в современном мире, способы борьбы

2.1 Состояние киберпреступности на сегодняшний день

На сегодняшний день необходимо видеть полную картину угроз кибератак в мире и отдельно в Российской Федерации, чтобы понимать, какие меры необходимо принимать для предупреждения и сокращения киберпреступлений. На рисунке 6 показана статистика частоты успешных кибератак по годам. Множество экспертов по безопасности IT технологий на основе этих данных предполагают, что число успешных кибератак в 2019 году возрастет по сравнению с 2018 годом [16].

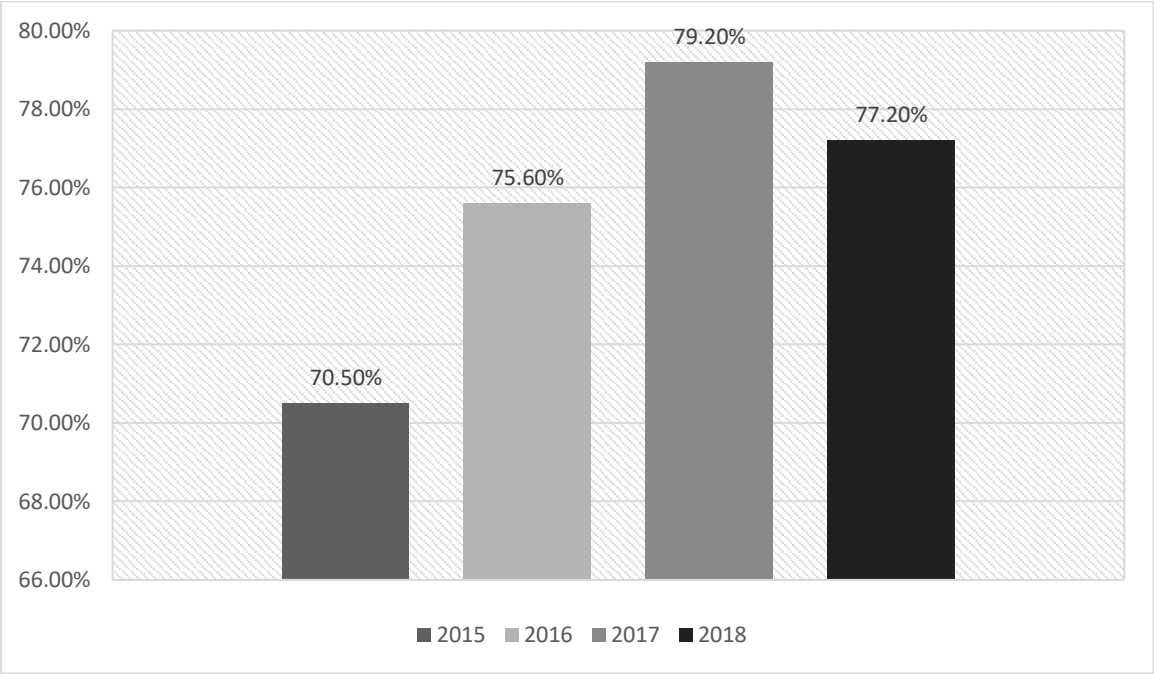

Рисунок 6 – Частота успешных кибератак по годам в мире (составлен автором [16])

Цели и мотивы киберпреступлений преступлений, совершаемых в 2019 году, можно увидеть на рисунке 7. Хорошо видно, что большинство преступлений совершались с целью получения финансовой выгоды, а также получение данных, но и эти данные в дальнейшем могут использоваться злоумышленниками, как средство получения прибыли, например, в качестве предмета вымогательства, шантажа.

Рисунок 7 – Мотивы и цели киберпреступников на 2018 год (составлен автором [16])

Жертвами кибератак в 2018 году стали 23% частных лиц, остальная доля – структуры и юридические лица, представленные на рисунке 8.

Рисунок 8 – Категории жертв киберпреступников среди юридических лиц на 2018 год (составлен автором [16])

Как уже было сказано, киберпреступность имеет глобальный характер, так, к примеру, киберпреступление против определенной компании в определенной стране может быть совершенно не на территории страны. Поэтому наиболее легким и верным в вычислении является не показатель количества совершенных киберпреступлений, а индекс киберзащищенности страны. Фрагмент «Глобального индекса кибербезопасности», ежегодно состовляемый экспертами ООН, за 2018 год представлен в таблице 4.

Таблица 4 – Фрагмент глобального рейтинга стран по индексу кибербезопасности (составлена автором [17])

Место	Страна	Индекс кибербезопасности
1	Великобритания	0.931
2	Соединенные штаты Америки	0.926
3	Франция	0.918

4	Литва	0.908
5	Эстония	0.905
…		
26	Россия	0.836

При составлении рейтинга, представленного в таблице 3 эксперты-составители учитывают пять основных критериев [17]:

1 Юридическая составляющая: наличие правовых систем и структур, занимающихся вопросами кибербезопасности и киберпреступлений.

2 Техническая составляющая: технические возможности в области кибербезопасности.

3 Составляющая организационной подготовленности: существование институтов координации политики и стратегий развития кибербезопасности на государственном уровне.

4 Составляющая образовательного и исследовательского потенциала: наличие научно-исследовательских, образовательных и подготовительных программ, а также сертифицированных специалистов и госучреждений, способствующих наращиванию потенциала в сфере информационной безопасности.

5 Составляющая готовности к сотрудничеству: наличие партнерств, механизмов сотрудничества и систем обмена информацией.

Положение России в рейтинге по кибербезопасности можно обосновать огромным ростом киберпреступлений, зарегистрированных в Российской Федерации. Согласно отчету Генеральной прокуратуры Российской Федерации от 14 августа 2018 года, в 2017 году количество преступлений выросло на 7,7% в сравнении с предыдущим годом, а в первой половине 2018 года количество преступлений выросло еще на 3,4%. При этом расследованные преступления на 19,6% уменьшились, на 30,5% выросло число нераскрытых преступлений – раскрываемость киберпреступлений

составляет 41,3%. Отрицательную динамику 2017-2018 годов в количестве числа преступлений можно проследить на рисунке 9 [2].

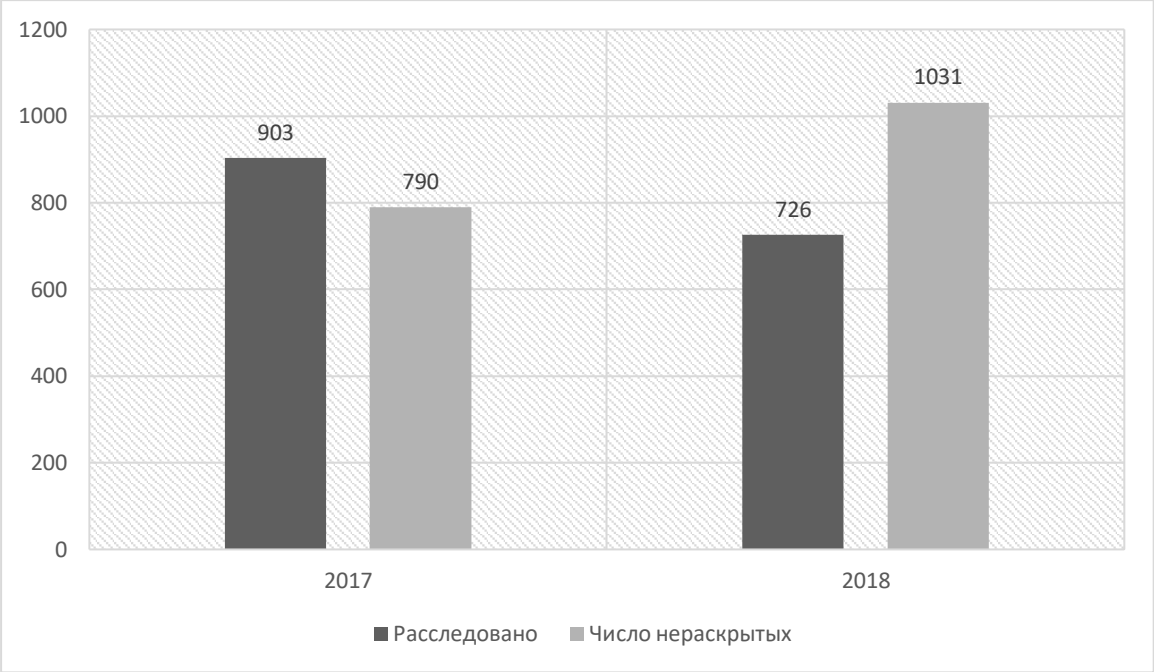

Рисунок 9 – Расследованные и нераскрытые киберпреступления в РФ за 2017-2018 года (составлен автором [2])

Киберпреступность сегодня наносит огромный ущерб как частным, так и государственным предприятиям, а также увеличивает расходы на IT-безопасность. Мировые расходы на продукты и услуги в области кибербезопансости в 2018 году (расчеты не охватывают различные категории кибербезопансости, включая Интернет вещей, Интернет промышленность) превышают расходы по сравнению с 2017 годом на 12,4%, а в 2019 году прогнозируется рост на 8,7% по сравнению с 2018 годом и достижения отметки расходов в 124 миллиарда долларов США, в целом ожидается рост рынка кибербезопасности к 2021 до 12-15% от общего рынка к 2021 году [20].

Киберпреступность сегодня стоит миру почти 600 миллиардов долларов или 0,8% от мирового ВВП, согласно новому отчету Центра стратегических международных исследований (CSIS) и McAfee. Европа и Центральная Азия потеряли 170 миллиардов долларов. В России на 2018 год

ярким примером масштабного киберпреступления является получение одной группировкой 1.2 миллиарда логинов и пароль от электронной почты пользователей [22].

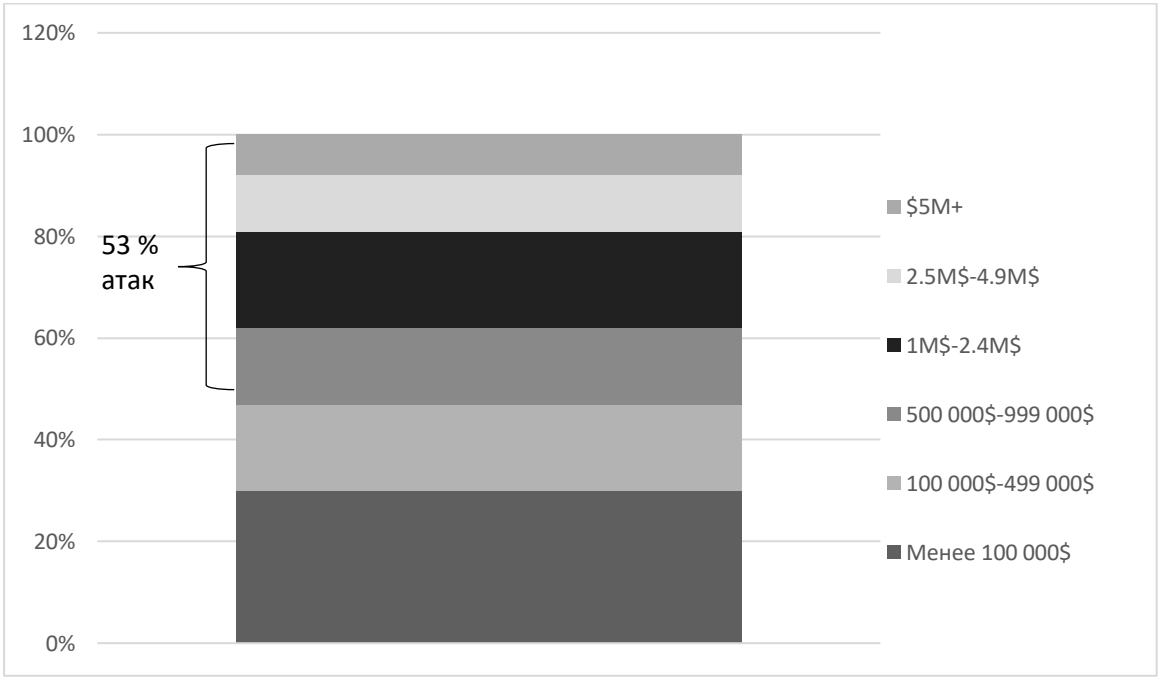

Рисунок 10 – Убытки от произошедших кибератак в 2018 году опрошенных 3600 респондентов в 26 странах мира (составлен автором [15])

Серьезность кибератак, страх перед их растущим числом и растущим числом нераскрытых преступлений основан на финансовом ущербе не только влияющим на количество ВВП страны и мирового ВВП, но и ущерба отдельных компаний и структур, а также физических лиц. Киберпреступления наносят реальный экономический ущерб организациям, структурам, восстановление которого может занимать месяцы и годы. По данным респондентов, опрошенных в ходе исследования Cisco, более половины (53%) всех атак привели к финансовому ущербу на сумму более 500 000 долларов США, включая, помимо прочего, потерю доходов, клиентов, возможностей и расходов из собственного кармана. Убытки от произошедших атак срели респондентов, проанализированных компанией Cisco, показаны на рисунке 10 [15].

Подводя итог, необходимо сказать, что достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса (МСБ), рост киберпреступности связан преимущественно не с крупными предприятиями, а именно с предприятиями МСБ. Такие предприятия в силу малого бюджета, отсутствия квалифицированных кадров, пробелов в познаниях сотрудников не могут на должном уровне обеспечить качественную информационную безопасность. Также 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, преступники обогащаются за счет кибершантажа, вымогательства, снятия денежных средств со счетов клиентов банка. 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 получить в свое пользование огромные объемы конфиденциальной информации, среди которой можно найти данные для последующего онлайн мошенничества, шантажа, перепродажи информации заинтересованным лицам.

2.3 Способы борьбы с киберпреступностью в Российской Федерации и международное сотрудничество

В уголовном законодательстве зарубежных государств криминализация киберпреступности не только включает деяния, непосредственно посягающие на информационную безопасность (консолидированные с учетом тождества родового объекта посягательства), но и охватывает иные общественно опасные посягательства, сопряженные с использованием информационно-телекоммуникационных сетей (в которых информационная

сфера является факультативным объектом преступления). В настоящее время вектор «растворения» таких норм в структуре уголовных законов зарубежных стран направлен на [22]:

1 Введение ответственности за хищение в сфере компьютерных технологий в специальной уголовно-правовой норме.

2 Установление признака использования информационных технологий в качестве криминообразующего признака хищения.

3 Признание компьютерной информации предметом преступного посягательства либо криминализации использования компьютерных технологий одним из способов, средством или квалифицирующим признаком совершения различных видов преступлений.

4 Выравнивание видов киберпреступлений.

В России на сегодняшний день действует Глава 28 УК РФ, которая так или иначе связана с киберпреступной деятельностью, она носит название «Преступления в сфере компьютерной информации». Включает в себя [9]:

1 Статью 272. Неправомерный доступ к компьютерной информации.

2 Статью 273. Создание, использование и распространение вредоносных компьютерных программ.

3 Статью 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

4 Статью 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Одно из наиболее серьезных ограничений национального законодательства о компьютерных преступлениях состоит в том, что оно не позволяет эффективно бороться с глобальным явлением киберпреступности. Европейская конвенция о киберпреступности, разработанная с целью создания международной структуры для борьбы с киберпреступлениями, была принята Комитетом министров Совета Европы в ноябре 2001 года [19].

Конвенция охватывает широкий круг вопросов, в том числе все аспекты киберпреступности, включая незаконный доступ к компьютерным системам и перехват данных, воздействие на данные, воздействие на работу системы, противозаконное использование устройств, подлог и мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, и правонарушения, связанные с авторским правома и смежными правами. При подготовке конвенции также преследовались цели формирования общей правоохранительной системы для борьбы с киберпреступностью и создания условий для обмена информацией между всеми странами, подписавшими конвенцию. Россия не входит в число стран-участников конценции.

Эффективно противодействовать киберпреступности можно только объединив усилия. Потому в 2018 году был проведен Первый Международный конгресс по кибербезопасности, который состоялся в Москве 5-6 июня. В нем приняли участие представители 681 организаций из более чем 50 стран, включая Интерпол, Всемирный экономический форум, SWIFT, ICANN, и более 45 российских и зарубежных правительственных агентств, и министерств. Повестка дня включала в себя обсуждение новейших угроз в цифровом мире и ключевых направлений глобального развития кибербезопасности.

Конгресс пришел к нескольким важным выводам:

1 Потери мировой экономики и России от киберпреступности беспрецедентны и продолжают расти.

2 Кибербезопасность отстает от технологических разработок на 2-5 лет.

3 Существует острая нехватка квалифицированных специалистов по кибербезопасности.

4 Киберпреступники действуют безнаказанно.

5 Эффективное международное сотрудничество необходимо для успешного противодействия киберпреступности [18].

Таким образом, высокая социальная опасность киберпреступности объясняется ее транснациональным и организованным характером, поэтому ни одно государство сегодня не способно активно противодействовать этой угрозе самостоятельно, в связи с чем неотложной является потребность активизации международного сотрудничества. Эффективная борьба с киберпреступностью требует коллективных усилий. Для этого необходимо вести постоянную разъяснительную работу среди населения. Требуется длительный и, что немаловажно, упорный воспитательный процесс для того, чтобы люди осознавали необходимость мер предосторожности. Для того чтобы эффективно противостоять киберпреступности, масштабы которой столь разительно выросли за последние годы, государственным структурам и коммерческим компаниям необходимо рассматривать информационную безопасность в качестве одного из ключевых компонентов своей деятельности. Наиболее приоритетными должны стать вопросы ответственности, соблюдения российского законодательства в области информационной безопасности и повышения уровня культуры безопасности граждан.

ЗАКЛЮЧЕНИЕ

Исходя из поставленных нами задач, подведем итоги:

1) Понятие «киберпреступности» на сегодняшний получило большое распространение в связи с информационно-телекоммуникационным прорывом, произошедшим в XXI в. На сегодняшний день существует несколько подходов к делению киберпреступности на виды.

2) Развитие киберпреступности идет в ногу с развитием информационно-технических средств, а мотивы киберпреступников также видоизменяются с развитием киберпреступности.

3) Существует ряд факторов, влияющих на совершение экономических преступлений, а совершение таких преступлений подразделяется на некоторые виды.

4) Киберпреступность на сегодня является большой проблемой и стремительно развивается с каждым годом во всех странах мира.

5) Существуют подходы к определению законов, связанных с киберпреступностью зарубежом, в Российской Федерации принят закон по борьбе с киберпреступность, а также огромное место в борьбе с киберпреступностью занимают мировые объединения.

Таким образом, киберпреступность является актуальной проблемой, которая затрагивает различные слои и структуры, развивается с каждым годом и становится более сложной в плане разрешения и уменьшения ее прогрессии, наказуемости киберпреступников. Она наносит огромные ущербы экономике, финансовым активам компаний, физическим лицам, поэтому в мире существуют различные объединения и обсуждения на тему киберпреступности, должны формироваться новые решения проблемы киберпреступности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Актуальные киберугрозы – 2018. Тренды и прогнозы. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/#id3 (дата обращения 9.05.2019)

2 Генеральная прокуратура Российской Федерации, о преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий. – URL: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (дата обращения 8.05.2019).

3 Глотина И.М. Киберпреступность как теневой бизнес // Экономические науки. – 2016. – №6 (388). – 54 с.

4 Глотина И.М. Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. – 2014. – №8. – 12 с.

5 Головинов О. Киберпреступность в современной экономике: состояние и тенедеции развития // Вопросы инновационной экономики – 2016. – Т. 6. – №1– 79 с.

6 Дикарев В.Г. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. – 2016. – № 8. – 15 с.

7 Карцхия А.А. Кибербезопасность и интеллектуальная собственность // Вопросы кибербезопасности – 2014. – №1 (2). – 63 с.

8 Морозов Н.А. Борьба с компьютерной преступностью в Японии // Общество и право. – 2014. – № 2 (48). – 141 с.

9 О преступлениях в сфере компьютерной информации: федер. Закон от13.06.1996 №63-ФЗ (ред. От 23.04.2019) – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/#dst101786:

10 Парфенов Н.П. Технология защиты персональных данных // Наука, техника и образование. – 2016. – № 4 (22). – 15-16 с.

11 Рогозин В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения. – 2015. – № 1 (7). – 58 с.

12 Сальникова Л. С. Репутационный менеджмент. Современные подходы и технологии: учеб. Для академического бакалавриата. – Москва: Издательство Юрайт, 2019 – 42-43 с.

13 Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – 104-106 с.

14 Скляров С.В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. – 2016. – Т. 10. – № 2. – 328 с.

15 Annual Cybersecurity report Cisco 2018. – URL: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf (дата обращения 9.05.2019)

16 Cybercrime and Cybersecurity Statistics & Trends. – URL: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Headline_cyber_crime_statistics_for_2018-2019 (дата обращения: 9.05.2019)

17 Global Cybersecurity Index (GCI) 2018. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (дата обращения 9.05.2019)

18 ICC: About the Congress. – URL: https://icc.moscow/about/ (дата обращения 21.05.2019)

19 Kaspersky: Киберпреступность и закон. – URL: https://securelist.ru/kiberprestupnost-i-zakon-obzor-polo/1315/#7 (дата обращения 21.05.2019)

20 Official Annual Cybercrime Report 2019 report from Cybersecurity Ventures sponsored by Herjavec Group. – URL:

https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (дата обращения: 9.05.2019).

21 The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations Jason R. C. Nurse – URL: https://www.researchgate.net/publication/328763267_The_Group_Element_of_Cybercrime_Types_Dynamics_and_Criminal_Operations (дата обращения 9.05.2019)

22 There's Nowhere to Hide from the Economics of Cybercrime. – URL: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html (дата обращения 9.05.2019).