САНКТ – ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

НАЗЫКОВ Максим Александрович

Выпускная квалификационная работа

**БОРЬБА РОССИЙСКОЙ ФЕДЕРАЦИИ ПРОТИВ КИБЕРПРЕСТУПНОСТИ НА НАЦИОНАЛЬНОМ И МЕЖДУНАРОДНОМ УРОВНЕ.**

**RUSSIAN FEDERATION’S STRUGGLE AGAINST CYBERCRIME AT THE NATIONAL AND INTERNATIONAL LEVEL.**

Направление 41.04.04 – «Международные отношения»

Основная образовательная программа магистратуры «Мировая политика»

Научный руководитель

к.п.н., доцент кафедры мировой политики

БОЛГОВ Р.В

Рецензент

КАБЕРНИК В.В.

Санкт-Петербург

2018

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 5](#_Toc515031144)

[ГЛАВА 1 КИБЕРПРЕСТУПНОСТЬ. ПОНЯТИЕ И СУЩНОСТЬ. ПОЛИТИЧЕСКИ МОТИВИРОВАННЫЕ КИБЕРПРЕСТУПЛЕНИЯ 14](#_Toc515031145)

[1.1 Определения киберпреступности. 15](#_Toc515031146)

[1.2 Цели и объекты киберпреступлений.Классификация и особенности. 17](#_Toc515031147)

[1.3 Динамика и основные показатели на современном этапе. 20](#_Toc515031148)

[1.4 Политически мотивированные киберпреступления, определение и особенные случаи. 24](#_Toc515031149)

[ГЛАВА 2 МЕЖДУНАРОДНАЯ КИБЕРПРЕСТУПНОСТЬ. ОПЫТ МЕЖДУНАРОДНОЙ БОРЬБЫ И УЧАСТИЕ РОССИИ. 29](#_Toc515031150)

[2.1 Международная киберпреступность. 29](#_Toc515031151)

[2.2. Международный опыт борьбы и участие России. 34](#_Toc515031152)

[ГЛАВА 3 БОРЬБА РОССИЙСКОЙ ФЕДЕРАЦИИ С КИБЕРПРЕСТУПНОСТЬЮ НА НАЦИОНАЛЬНОМ УРОВНЕ. 45](#_Toc515031153)

[3.1 Документы, принятые на территории Российской Федерации. 45](#_Toc515031154)

[3.2 Органы и организации, занимающиеся вопросами киберпреступности на территории России. 49](#_Toc515031155)

[ЗАКЛЮЧЕНИЕ. 56](#_Toc515031156)

[ПРИЛОЖЕНИЕ 1 70](#_Toc515031157)

[ПРИЛОЖЕНИЕ 2 71](#_Toc515031158)

[ПРИЛОЖЕНИЕ 3. 72](#_Toc515031159)

[ПРИЛОЖЕНИЕ 5 74](#_Toc515031160)

[ПРИЛОЖЕНИЕ 6 75](#_Toc515031161)

[ПРИЛОЖЕНИЕ 7 76](#_Toc515031162)

[ПРИЛОЖЕНИЕ 8 77](#_Toc515031163)

# ВВЕДЕНИЕ

На сегодняшний день, сложно представить жизнь без употребления благ современной цивилизации. Электронная почта, видео-хостинги, интернет банкинг и другие финансовые операции, а так же многие другие возможности стали неизменной частью нашей повседневной жизни.

В действительности же связано это в основном с нарастающей активностью жителей Земли на интернет просторах, так, например, по оценкам Internet World Stats на 31 декабря 2017 года, общее количество пользователей интернет услуг перевалило более чем за 50 процентов населения земного шара.[[1]](#footnote-1)[[2]](#footnote-2)

Использование информационно-коммуникационных технологий в значительной степени облегчает существование как отдельно взятых лиц, так и организаций, бизнеса и государственных структур. Благодаря всеобъемлющему покрытию сетью интернет большей части земной поверхности, доступ во «всемирную паутину» можно получить практически из любой точки мира, скорость передачи информации позволяет моментально обмениваться данными, сообщениями находясь даже за несколько тысяч километров от места назначения передачи, а возможности передачи информации позволяют оперировать огромными массивами данных в режиме онлайн не испытывая особых трудностей.

Не ставя под сомнение объективных плюсов, которые человечество получает в лице информационных технологий, следует отметить, что новые средства коммуникации порождают так же и новые угрозы. На фоне резко растущих и расширяющихся возможностей получения и обмена информации возникают и преступления в пространстве интернет, жертвами которых становятся не только рядовые пользователи – граждане, но и юридические лица, организации, бизнес. Но самым опасным являются преступления, совершаемые в киберпространстве для правительств и государств земного шара. О киберпреступлениях в общем смысле, а так же «политически мотивированном» их аспекте и борьбе с ними на территории РФ как внутри государства, так и на международном уровне и пойдет речь в данном диссертационном исследовании.

**Актуальность исследования.**

Актуальность данного исследования, продиктована тем, что несмотря на существующую тенденцию к увеличению числа политически мотивированных киберпреступлений, на фоне не прекращающегося увеличения числа киберпреступлений в общем, в научных трудах, вопросы и обоснования политических киберпреступлений рассмотрены фрагментарно, либо не поднимаются вообще.

Тем не менее вслед за ускоряющимся развитием интернет коммуникации, а так же других видов информационно-коммуникационных средств, усиливается и частота и объем противозаконных деяний совершаемых с использованием данных технологий. Так например, еще в 2012 году, согласно отчету представленному в пресс-релизе компании Symantec более 30 млн. граждан Российской Федерации стали жертвами тех или иных противоправных действий совершенных по отношению к их персональным устройствам, аккаунтам в социальных сетях и т.д Совокупный ущерб нанесенный злоумышленниками за 12 месяцев, согласно отчету составил около двух миллиардов долларов США. Хочется заметить: несмотря на то, что в 2012 году РФ была впервые представлена в отчете Norton Cybercrime Report, результаты были не утешительными, поскольку Россия заняла в представленном рейтинге 1-е место по общему проценту атакованных технических средств (этот процент составил 74%) обогнав Китай с их 66% атакованных технических устройств. [[3]](#footnote-3)

Кроме этого, уже в прошлом, 2017 году, генеральный прокурор РФ Юрий Чайка, в своем выступлении в Бразилии, на встрече руководителей прокурорских служб, отметил, что различного рода противоправные мероприятия и действия, которые совершаются, при посредничестве и использовании сети интернет и различных коммуникационных технологий, причиняют огромный ущерб в материальном плане, а так же посягают на общую национальную безопасность.[[4]](#footnote-4) Кроме этого, согласно выступлению генерального прокурора , совокупный материальный ущерб, от нанесенных кибератак составил более 18 миллионов долларов США, в дополнение к тому, что общее число лишь за период с 2013 до 2016 года число нарушений в пространстве интернет увеличилось в 6 раз.

Помимо вышеперечисленного, аналогичное исследование проведенное компанией Symantec, но уже в 2017 году, зафиксировало, что жертвами киберпреступлений лишь в 20 исследованных странах стали около 1 миллиарда человек по всему миру, а за последние 12 месяцев 44% пользователей были подвергнуты правонарушению с использованием средств информационно-коммуникационных технологий. [[5]](#footnote-5) Что в общем привело к убыткам порядка 172 миллиардов долларов США.

Но помимо этого, киберпространство становится ареной и одновременно целью атак не только с целью финансового ущерба лицам и организациям. В своем заявлении генеральный прокурор РФ Ю.Чайка так же отметил, что зачастую в ходе исследований и мониторинга современных социальных сетей выявляются многочисленные содержательные части (контент в виде текстовых форматов, форматов изображения и видео, аудио ), которые демонстрируют, призывают к совершению или оправдывают различные террористические акты и деяния, а так же открыто призывают к экстремизму.[[6]](#footnote-6) Очевидно, что призывы имеют виду нарушение законодательства, как на просторах интернета, так и в сфере «оффлайн».

Кроме этого, нередки случаи нарушения законодательства в сети по политическим мотивам, что в первую очередь ставит под угрозу национальную безопасность отдельно взятых государств, так же и всего международного сообщества в целом. Именно поэтому, на сегодняшний день, на первый план выходят вопросы обеспечения безопасности как персональных данных физических и юридических лиц, так и информационной инфраструктуры государственных органов, государственных корпораций, а так же других общественных и политических ведомств, частной переписки лиц, занимающих важные государственные посты, систем, которые обеспечивают работу структур гражданских и социальных услуг, взаимодействия общества и институтов государства.

В качестве **хронологических рамок** выбран период времени от начала 2000 года до первой половины 2018 года, в вопросах противодействия киберпреступности на территории Российской Федерации, поскольку именно этот этап характеризуется наибольшей активностью развития и внедрения информационных технологий в бизнес структуры, государственную службу и услуги, политические процессы, а так же повседневную жизнь. Так же данный период отличается подавляющим количеством принятых документов, по вопросам кибербезопасности и контролю процессов в сфере интернет. Так первые документы, в том числе «Окинавская Хартия» были приняты в начале указанного временного отрезка, то же касается и первой Российской «Доктрины информационной безопасности», которая датируется 9-ым сентября 2000 года.[[7]](#footnote-7)

**Степень разработанности проблемы.**

Хочется отметить, что за последнее время те или иные аспекты противодействия киберпреступности стали освещаться значительно лучше, чем несколько лет тому назад. Очевидно, что острота проблемы сказывается на данной тенденции. Тем не менее, большинство работ не носят всеобъемлющего характера и посвящаются в основном отдельным правовым или криминологическим аспектам проблемы киберпреступности, а так же направлены на рекомендации по оптимизации уголовной ответственности за преступные деяния в сфере ИКТ. Кроме этого, в исследовательскй литературе редко встречается освещение политического мотива совершения киберпреступления на международной и национальной аренах. Исключение составляют работы А.Л. Осипенко «Борьба с преступностью в глобальных компьютерных сетях: Международный опыт»[[8]](#footnote-8), и работа Волеводза А.Г. «Противодействие компьютерным преступлениям: правовые основы международного сотрудничества»[[9]](#footnote-9), содержащие обширный исследовательский материал по данному вопросу. На тему глобального влияния и проблематики киберпреступности, до сегодняшнего дня в отечественной теории отмечены в большей степени научные статьи.

Среди авторов занимающихся разработкой данной проблемы выделяются работы Булай Ю.Г и Р.И., которые изучали способы профилактики, а так же противодействию киберпреступности и международным киберугрозам.[[10]](#footnote-10) Болгова Р.В., который поднимал вопрос об акторности различных сообществ в интернете, в том числе и киберпреступных группировок. Кроме этого автор опирался на исследования Каберника В.В., который в своей работе «Проблемы классификации кибероружия», описал виды кибероружия и провел основные отличия данного оружия от видов информационного воздействия.[[11]](#footnote-11) Журавленко Н. И. и Шведовой Л.Е., которые в своей работе «Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере»[[12]](#footnote-12), в виду исследования современных тенденций киберпреступности и исследования международного опыта сотрудничества, определили перспективные направления сотрудничества на международной арене, по данному вопросу. Кроме этого, автор, в ходе исследования учитывает наработки сделанные Валько Д.В, Евдокимовой К.Н., Тропиной Т.Л. и Номоконовым В.А., Осипенко А.Л., Введенской О.Ю, а так же некоторых дргугих исследователей отмеченных в ходе диссертационного исследования, изучавших основные тенденции развития регулировки в сфере информационного общества, видов совершения противонарушений в сфере информационной среды и др.

Кроме этого по теме компьютерной преступности и ответственности за совершение компьютерных преступлений выполнено несколько диссертационных исследований: Тропина Татьяна Львовна. «Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы»[[13]](#footnote-13), а так же другие диссертационные исследования проведенные Хисамовой З.И.,Сафоновым О.М., безусловно отражают проблематику Уголовно-процессуального аспекта киберпреступности, но, к сожалению не отражают тенденцию к политической мотивировке данных преступлений.

Работы исследователей ученых: Марка Бреннера и Сьюзан Гудман,[[14]](#footnote-14) Фила Вильямса[[15]](#footnote-15), Дороти Деннинг[[16]](#footnote-16), Джеймса Льюиса[[17]](#footnote-17), Барри Колина[[18]](#footnote-18), Кемерон Браун[[19]](#footnote-19), Дэборы Шиндер[[20]](#footnote-20), посвященные киберпреступности, дают неплохое представление об этом явлении, но, к сожалению, эти исследования практически никогда не охватывают Россию и российское законодательство, в то время, как Российская Федерация достаточно давно является активным участником международных усилий по противодействию киберпреступности. Тем не менее, они дают хорошие теоретические основы для изучения киберпреступности в глобальном аспекте.

Данное исследование призвано, учитывая уже имеющиеся наработки в данной проблеме, уточнить особенности международного толкования и восприятия киберпреступности и противодействия ей, выявить основные тенденции по борьбе с киберпреступностью на территории Российской Федерации, как на национальном так и международном уровнях, отразить наиболее успешные стороны реализации стратегий и выявить причины основных отстающих положений, попытаться сформировать рекомендации для дальнейшего изучения и внедрения на практике наиболее успешных из имеющихся практик по противодействию киберпреступности из международного опыта.

Цели и задачи исследования.

**Цель данной диссертационной работы** состоит в определении особенностей Российского подхода к борьбе с киберпреступностью, в том числе политически мотивированной и мер противодействия ей, со стороны Российской Федерации, на международном и национальном уровнях.

Для достижения цели диссертационного исследования необходимо в ходе изучения выполнить **ряд задач**, а именно:

- Сформулировать собственное определение киберпреступности и смежных понятий на основе уже существующих разработок;

- Определить основные виды и цели киберпреступлений на территории РФ и международном уровне, а так же основные отличительные характеристики данных видов противонарушений;

- Дать определение «политически мотивированным» киберпреступлениям и отразить особенности данного вида правонарушений;

- Проанализировать основополагающие конвенции, соглашения и нормативно-правовые акты в соответствии с выбранной тематикой принятые в РФ, а так же на международном уровне с участием РФ;

- Определить состав и историю основных органов в системе силовых ведомств РФ, а так же частных организаций, курирующих вопросы кибербезопасности;

- Изучить основные меры и методы борьбы с киберпреступностью применяемые на территории РФ, а так же основные меры по противодействию на международном уровне с участием России;

- Сформулировать выводы на основе статистических данных и изученных документов, относительно тенденций законодательных и процессуальных мер РФ по противодействую киберпреступности на международном и национальном уровнях.

**Объектом** данного диссертационного исследования является феномен киберпреступлений, совершаемых на национальном и международном уровне.

**Предметом** данного исследования является совокупность документов и мер, предпринимаемых для противодействия киберпреступности на территории Российской Федерации, а так же на международном уровне с участием России.

**Основными методами**, которые были использованы в данном диссертационном исследовании являются:

Сравнительно исторический метод, использованный при изучении основных этапов развития и формирования общего представления, о состоянии киберпреступности и мер противодействия ей.

Сравнительно – правовой для анализа существующих соглашений и договоров, нормативно-правовых актов, регулирующих вопросы кибербезопасности в РФ и странах зарубежья, а так же системный метод, который позволяет проанализировать структуру основных органов, занимающихся вопросами предупреждения киберпреступлений и их взаимодействия в процессе противодействия правонарушениям.

Статистический, в частности метод статистического сравнения, который используется при изучении массовых явлении, прослеживания динамики развития и увеличения числа кибератак, с целью выявить основные тенденции развития и заметить основные причины .

В ходе рассуждения и формулировки выводов, автор придерживался неореалистической парадигмы теории международных отношений, исходя из тенденции к фрагментации международных усилий в сторону национальных или, иногда, региональных инициатив, которые являются яркими примерами эффективных противодейственных мер, по сравнению с международными усилиями, в то же время применяя национальные и региональные меры, государства при этом стремятся к сохранению статуса-кво и незыблемости суверенитета, в связи с чем, зачастую меры и документы угрожающие самостоятельности государства и его исключительной роли в самостоятельном принятии решений, по данному вопросу, отклоняются, как в случае с отказом РФ от подписания Конвенции Совета Европы от 2001 года.

**Теоретическую базу** для исследования составляют научные статьи, а так же работы отечественных и зарубежных исследователей по данной тематике, отраженные выше, и частично, в ходе диссертационного исследования которые дают представления об отдельных аспектах и специфике киберпреступности на современном этапе, аналитические записки исследовательских групп и организаций и журнаолов, таких как «Международная жизнь», РБК др.

**Эмпирическую базу** составят статистические данные полученные на основе исследований различных ведомств и организаций, изучающих вопросы развития и распространения киберпреступности на территории РФ и за рубежом, такими данными обладают отчеты компании «Symantec»[[21]](#footnote-21), «IBM security»[[22]](#footnote-22), «The Accenture Index»[[23]](#footnote-23) среди отечественных исследований, проведенных по этому направлению отмечается бюллетень составленный «Лабораторией Касперского»[[24]](#footnote-24), затрагивающий вопросы количества и качества, а так же основных показателей произошедших правонарушений в области компьютерной безопасности за определенные периоды времени.[[25]](#footnote-25) Кроме этого, в эмпирическую базу входят доклады подготовленные Международным Союзом Электросвязи в 2017 году[[26]](#footnote-26) и исследования Евроазиатской Группа экспертов[[27]](#footnote-27), отражающих основные тенденции и направления борьбы с киберпреступностью в разных государствах и региональных объединениях, а так же оперативная информация полученная из записей Федеральной службы государственной статистики РФ.

Кроме этого в данном исследовании, затруднительно будет обойтись без периодических сообщений СМИ, комментариев должностных лиц отечественных органов власти, которые позволят с большей точностью описать происходящие события «из первых рук».

**Источниковую базу** для исследования составили:

Основополагающие документы по вопросам предупреждения киберпреступности в международной сфере:

-Окинавская хартия информационного общества 2000 года[[28]](#footnote-28);

- Европейская конвенция по киберпреступлениям от 2001 года[[29]](#footnote-29);

- Резолюция ООН по предупреждению преступности и уголовному правосудию[[30]](#footnote-30);

- Стратегия национальной безопасности Российской Федерации[[31]](#footnote-31);

- Доктрина информационной безопасности Российской Федерации[[32]](#footnote-32);

- Конвенция об обеспечении международной информационной безопасности (концепция)[[33]](#footnote-33);

- Другие нормативно-правовые акты регулирующие вопросы противодействие киберпреступности на территории РФ, как Уголовный Кодекс РФ( в частности его статьи которые содержат составы преступлений в сфере компьютерной информации);

- Соглашения по информационной безопасности с участием Российской Федераций по вопросам противодействия киберпреступности на национальном и международном уровнях.

**Практическая значимость** данного исследования заключается в том, что выводы, сделанные в результате изучения тенденций развития киберпреступности и мер борьбы с ней на международном и национальном уровнях могут быть использованы:

- ходе дальнейшего изучения международных, а так же юридических аспектов киберпреступности, для совершенствования мер противодействия данным видам правонарушения в рамках существующих законодательных и декларативных норм;

- в виду, отмеченной автором тенденции, к отставанию развития законодательных инициатив по регулировке информацинного обмена от скорости информационного развития, при разработке новых национальных и международных норм, по противодействию киберпреступлениям.

**Научная новизна**

Особенностью данного диссертационного исследования является рассмотрение специфики политически мотивированных киберпреступлений, как одного из отдельных видов правонарушений. Поскольку в отечественной и зарубежной литературе изученной по данной тематике, вопросы политической подоплеки совершения правонарушений в области информационных технологий рассмотрены фрагментарно, либо не поднимаются вообще. Таким образом в данном диссертационном исследовании:

1) Формулируется собственное определение «киберпреступления» и смежных понятий, в частности «политически мотивированное киберпреступление», отражающие основные характерные черты данных правонарушений и удовлетворяющие основным целям исследования;

2) Изучается статистика видов информационных правонарушений за последние годы, в динамике, а так же основные тенденции к изменению векторов противонарушений в сфере информационной среды. Кроме этого изучены некоторые виды противонарушений, совершенные по политическим мотивам, в частности в составе организованных групп;

3) Исследуется тенденция развития правовых норм международного сообщества, по противодействию киберпреступности, на международном уровне с участием Российской Федерации, и национального законодательства Российской Федерации в данной сфере, в том числе и органов в структуре ведомств РФ и частных организаций, курирующих вопросы противодействия киберпреступности.

# ГЛАВА 1 КИБЕРПРЕСТУПНОСТЬ. ПОНЯТИЕ И СУЩНОСТЬ. ПОЛИТИЧЕСКИ МОТИВИРОВАННЫЕ КИБЕРПРЕСТУПЛЕНИЯ

Современное развитое общество, всецело основано на использовании информационно-коммуникационных технологий(далее ИКТ), компьютерных сетей, облачных хранилищ данных, а так же многих других преимуществ XXI века.

Для всецелого понимания сущности и особенностей рассуждения в данном диссертационном исследовании, автор считает необходимым дать определение «информационно-коммуникационных технологий».

Так глоссарий по информационному обществу, составленный М.Р. Когаловским, отмечает, что под Информационно-коммуникационными технологиями следует понимать совокупности методов, различных производственных процессов, программное обеспечение или лингвистические средства, объединяемые для того, чтобы накапливать, хранить, обрабатывать и передавать информацию различного рода, в первую очередь в интересах пользователей.[[34]](#footnote-34)

Кроме этого, в Законодательстве Российской Федерации так же имеется определение информационных технологий, под ними в Федеральном законе под номером 149-ФЗ понимаются процессы, а так же методы поиска, сбора, хранения и обработки информации, для дальнейшего предоставления и распространения. Более того, в данном определении подразумеваются и методы, используемые для осуществления всех этих процессов. [[35]](#footnote-35)

Как уже отмечалось во введении к данному диссертационному исследованию, по данным Internet World Stats[[36]](#footnote-36), более половины населения земного шара на сегодняшний день являются в той или иной степени активными пользователями сети интернет. Ежедневная работа органов государственного аппарата, транспортных, энергетических систем, органов здравоохранения и банковских структур затруднительно представить без надежной и постоянной работы высоких технологий и средств ИКТ.

Поскольку примером успешной реализации целей развития информационно-коммуникационных технологий является развитие всемирной сети Интернет[[37]](#footnote-37), автор считает необходимым уточнить определение, сделав его подходящим под тему и задачи диссертационного исследования.

ИКТ – средства, способы и методы накопления и обмена и распространения информации, с целью ее использования, затрагивающие использование сети Интернет, устройств объединенных в единое информационное пространство, с целью получения и обработки максимального количества информации.

Поскольку, как уже было отмечено, средства и способы ИКТ в ходе прогресса проникают во все сферы жизни человечества, включая финансовую, образовательную, государственную и даже частную жизнь граждан нередкими становятся случаи нарушения прав и свобод людей, организаций и даже целых государств, с применением высоких технологий, высокотехнологичных устройств и других воплощений ИКТ.

Объединение устройств и баз данных в единые пространства и сети, позволило пользователям получать доступ, обрабатывать и передавать информацию из любой точки планеты, осуществлять управление собственными активами, капиталами компании или фонда, заключать сделки договора без личного контакта.[[38]](#footnote-38) Но именно эти преимущества и позволили стать «всемирной паутине» стать одновременно и местом совершения преступлений и целью противоправных действий злоумышленников.

## 1.1 Определения киберпреступности.

Для того, чтобы наиболее четко проследить основные тенденции, методы и способы борьбы Российской Федерации с киберпреступностью, необходимо уточнить само понятие «киберпреступление», а так же сопоставить его с другими смежными феноменами, такими как «киберпреступность» и «преступление с использованием компьютера», разграничить особенности и отметить основные тенденции развития.

В отечественной и зарубежной литературе подходы к определению понятия киберпреступления разнятся, ввиду отличительной черты данного вида правонарушений, а именно в том, является ли компьютер целью правонарушения или же средством для совершения преступных деяний.[[39]](#footnote-39)

**Определение киберпреступлений.**

Энциклопедия «Britannica» киберпреступлением, которое, так же может быть названо компьютерным преступлением определяет использование компьютера, как инструмент для совершения противоправных действий, как кража, распространение порнографии или нарушение прав интеллектуальной собственности. Кроме этого, согласно определению, киберпреступления включают в себя нарушение частной жизни и кражу личных данных.[[40]](#footnote-40)

Данное определение, как видится автору, в значительной степени подходит под феномен «преступления с использованием компьютера», поскольку отмечает роль технических устройств лишь как инструмента совершения преступлений.

Отечественный исследователь Карпова Д.Н., в своей научной статье, посвященной изучению проблем киберпреступности[[41]](#footnote-41), так же отмечает, что характерной особенностью данного вида правонарушений является компьютер, а так же любые другие технические устройства, имеющие доступ к сети Интернет, в качестве основного инструмента совершения преступления. Кроме этого, определение предложенное Карповой, содержит обобщение целей для совершения киберпреступлений, среди них исследователем выделяются экономические, политические цели, а так же нанесение морального идеологического, культурного и других видов вреда пользователям, которые могут быть как обычными гражданами, так организациями или государственными органами.

Как мы можем заметить, данное определение уже содержит уточняющие формулировки, которые затрагивают цели злоумышленников, а так же определяют как средство нанесения вреда не только персональные компьютеры (далее ПК), но и другие технические устройства, в качестве инструментов. Но наиболее важной деталью данного определения является наличие формулировки о том, что связь устройств с помощью Интернета – наиболее распространенная особенность совершения данных правонарушений. Поскольку, согласно отчету «Global Cybersecurity Index 2017»,представленный Международным Союзом Электросвязи, к 2020 году более 12 млрд. устройств будут соединены между собой, посредством сети интернет, данное определение указывает на нарастающую тенденцию в изменении пространства используемого для совершения преступлений в информационной среде. [[42]](#footnote-42)

Конвенция Совета Европы « О преступности в киберпространстве», определяет киберпреступления, как действия, совершаемые против конфиденциальности, целостности, а так же доступности компьютерных систем, сетей и информации, и злоупотребления данными системами сетями и данными в преступных целях. [[43]](#footnote-43)

Таким образом, исходя из изученных материалов, автор считает необходимым предложить собственное определение понятия «киберпреступление», которое бы удовлетворяло целям исследования и отражало наиболее актуальные тенденции развития данного феномена на современном этапе:

**Киберпреступление** – действие, совершаемое посредством использования персонального компьютера, мобильного устройства или других технических средств, связанных между собой сетью интернет, нарушающее права человека, а так же законодательно установленные нормы, с целью извлечения экономических, политических, культурных и других выгод; нарушения стабильности, конфиденциальности и доступности информационных сетей.

Данное определение на наш взгляд соответствует целям исследования и отражает особенности, а именно политические аспекты данных правонарушений, которые рассматриваются в ходе данного диссертационного исследования.

Исходя из выведенного определения, следует и определение киберпреступности в целом, которую следует понимать как «совокупность преступных действий, совершаемых посредством технологических средств, нарушающих законодательно установленные нормы, с целью извлечения политических, экономических и других видов выгод и посягающих на функционирование, стабильность и конфиденциальность информационных систем.

Кроме этого, вероятно, полезным для общего осознания исследуемой проблемы будет предложение определения «кибербезопасности» - феномена, как совокупности условий, при которых угрозы киберпреступлений минимизированы или отсутствуют, а так же «кибербезопасности» - процесса, понимаемого исследователем, как совокупности усилий и мер, предпринимаемых, для предотвращения преступлений, совершаемых в информационном пространстве и/или с использованием технологических средств.

## 1.2 Цели и объекты киберпреступлений.Классификация и особенности.

Согласно определению, предложенному в диссертационном исследовании, злоумышленниками в сфере высоких технологий преследуется ряд целей, для удобства понимания необходимо подробнее описать виды целей, при совершении киберпреступлений.

Согласно данным исследований проведенным Карповой, чаще всего правонарушения данного характера, совершаются для получения экономических выгод, нанесения финансового ущерба, кражи денежных средств и других активов, завладение конфиденциальной или потенциально важной информации.[[44]](#footnote-44) Следующим видом целей киберпреступлений являются политические, совершаемые ради нанесения существенного ущерба различным государственным органам и службам, использующим технические устройства и технологии в работе, для того чтобы спровоцировать сбои в работе и стабильности систем, скомпрометировать отдельных представителей государственной власти, подорвать доверие граждан к правительству и государству. Кроме этого, зачастую злоумышленники используют сеть и информационные системы для того, чтобы добиться идеологических целей, а именно, распространить антиобщественные или потенциально радикальные идеи, завербовать пользователей в ряды террористических или противогосударственных, так же националистических группировок. Другим видом целей является социально-психологические, среди них – нанесение морального, психологического вреда индивидам, запугивание или угрозы личного характера, посягательство на личную или конфиденциальную информацию граждан. Другой классификацией целей «киберзлоумышленников», является предложенная в Концепции Совета Европы, принятая в Будапеште в 2001 году[[45]](#footnote-45), согласно ей преступниками движут следующие цели:

1) Преступления, которые совершаются против целостности, конфеденциальности, а так же доступности компьютерных данных и систем, в которую входят:

* противозаконный доступ, путем обмана взлома, с применением других путей;
* противозаконный перехват процессов обмена информации и компьютерных данных;
* внедрение в данные, для умышленного повреждения, изменения, извлечения и сокрытие данных без получения прав у правообладателя;
* умышленное вмешательство в работу, путем взлома, создания помех и удаленных атак;
* производство и распространение устройств ,механизмов и способов, используемых при совершении киберпреступлений.

2)Противозаконные действия, связанные с персональными компьютерами, включая подделку и мошенничество различного рода;

3)Противозаконные действия с содержанием информации, включая распространение запрещенных материалов, порнографии(включая детскую), националистических идей и ксенофобии;

4)Нарушение авторских, а так же смешных прав, использование материалов различных форматов, включая аудио, видео, изображения, данные, книги, другой цифровой продукции без получения права, на использование. [[46]](#footnote-46)

Объектами киберпреступлений на сегодняшний день являются граждане различных стран, организации бизнеса и благотворительные фонды, институты и органы, а так же представители власти, которые используют сеть интернет в повседневной жизни, для осуществления коммерческой или культурной деятельности, осуществление политических процессов и способов отправления государственной власти, соответственно.

Среди особенностей, отличающих данный вид противоправных действий, исследователи и экспертные группы отмечают следующие:[[47]](#footnote-47)

- высокую вероятность сокрытия данных, удаления или редактирования данных, зачастую хранящихся на локальных копиях и серверах;

- сложности при получении данных от поставщиков интернет-услуг, связанные с законодательством и, в частности, договорах о неразглашении данных в каждой стране;

- сложности при обнаружении конкретных данных необходимых для определения вины или регистрации правонарушения, а так же с дешифровкой и распознанием данных;

- трудности при выполнении экстерриториальных расследований, вызванные особенностями национальных подходов к проведению следствия;

- вопросы неприкосновенности частной жизни или вопросы, представляющие государственную тайну, при проведении следствия;

- сложности в процессе сбора и анализа доказательств, определения состава преступлений, авторизации или проверки источников информации изучаемых в процессе расследования;[[48]](#footnote-48)

Все эти отличительные особенности киберпреступлений, позволяют выделить данный вид правонарушений в отдельный вид противоправных деяний. Кроме этого, перечисленные особенности отражают современные тенденции политики международного сообщества и отдельных стран, в частности РФ, направленную на единое отражение киберпреступлений на уровне национальных законодательств, что позволит улучшить меры, направленные на предотвращение нарушения прав граждан, организаций и государства.

## 1.3 Динамика и основные показатели на современном этапе.

Перед тем, как изучить основные статистические показатели, отражающие состояние киберпреступлений, необходимо заметить, что общее число правонарушений, происходящих в Российской Федерации, а так же во всем мире ежегодно растет, показывая значительный рост в каждый изучаемый период и в количественном и в качественном понимании. Нужно сказать, что по оценкам исследователей, еще в 2012 году около половины всех пользователей сети Интернет подвергались нарушениям в киберпространстве, в общем счете, за тот период злоумышленниками был нанесен экономический ущерб вред в размере 500 миллионов долларов США. Более того, согласно исследованию, представленному в работе Бондаря В.В., 20% компаний малого и среднего бизнеса так или иначе пострадали от преступных действий в информационной среде.[[49]](#footnote-49)

Так же, согласно данным, озвученным во время панельной сессии, состоявшейся в г.Сочи в 2016 году, по теме «Киберпреступность – одна из ключевых угроз роста мировой экономики. Готова ли Россия к новым вызовам?», было отмечено, что по итогам 2015 года, в общем счете, киберпреступники нанесли ущерб мировой экономике в размере 400 миллиардов долларов США. Как утверждают эксперты к концу 2018 года, общее число правонарушений в информационной среде может вырасти в 4 раза, тогда как совокупный ущерб Российской экономике, сможет составить порядка 2 триллионов рублей. Из интервью, которое было сделано с модератором данной панельной сессии, заместителем председателя «Сбербанка», Станиславом Кузнецовым, следует информация о том, что ни один другой элемент криминальной активности не демонстрирует подобных темпов роста: их число ежемесячно увеличивается на 3-4%. [[50]](#footnote-50)

В связи с широким распространением информационных систем и услуг связанных с доступом в сеть интернет, киберпреступность за последние 10-15 лет стала одной из самых обсуждаемых и исследуемых проблем. Следует заметить, что далеко не все страны, на данный момент, разработали и приняли законодательство, всецело отвечающее вызовам современной киберпреступности, так например, согласно типологическому исследованию, приведенному Евразийской Группы, законодательство подавляющего числа стран-участниц исследования отсутствует само определение «киберпресупности».

Так по данным отчета IBM Security Group, который был представлен по итогам 2016 года, можно сделать вывод о том, что территориально большинство киберпреступлений и нарушений прав в области информационных технологий за прошедший период были совершены в отношении стран Северной Америки, стран Европы, а так же ряда Скандинавских стран.[[51]](#footnote-51) Что подтверждает одно из замечаний автора диссертационного исследования о том, что в «зону риска» попадают страны и регионы наиболее широко использующие информационные технологии, внедряющие их в различные сферы общественных и экономических отношений.[[52]](#footnote-52)[[53]](#footnote-53)

Кроме этого, данный отчет отражал основные отрасли общественных, государственных и экономических отношений, которые в наибольшей степени пострадали от киберпреступности.

По схеме, представленной в Приложении 1, можно сделать вывод о том, что качество кибератак за период с 2014 по 2015 годы изменилось, так на первое место вышла сфера здравоохранения, а на второе сфера производства. Для целей данного диссертационного исследования, особо заметным становится тот факт, что в 2015 году в рейтинге сфер, затронутых киберпресупниками, появляется сфера государственных органов и отношений, что позволяет выдвинуть предположение об изменении основных тенденции в развитии и целях киберпресупности, а так же о методах совершения данных противоправных действий, что не может не отразиться на ведении внутренней и внешней политики государств в условиях новых вызовов. [[54]](#footnote-54)

Среди стран-источников киберпреступлений на 2015 год, Исследовательская Лаборатория Касперского, выделяет лидирующими Соединенные Штаты Америки, Германию и Нидерланды, что можно увидеть на диаграмме представленной в Приложении 2.[[55]](#footnote-55) Сразу же после перечисленных стран, следует Российская Федерация, что позволяет сделать вывод об усиливающемся характере киберпреступлений на территории нашей страны.

Кроме этого, исследование подготовленное группой NTT, говорит о том, лидером по количеству атак совершенных с территории конкретного государства является США, у России же, согласно данному исследованию всего 1% атак, от общего числа совершенных.[[56]](#footnote-56)[[57]](#footnote-57)

Среди атакованных стран по данным этого исследования лидирующее положение занимает Российская Федерация, в которой общий процент атакованных пользователей превышает 40% от общего числа корпоративных клиентов.[[58]](#footnote-58) Кроме этого, в отчете отмечается заметную положительную динамику на 2015 год по сравнению с 2014 годом, так общее число кибератак на корпоративных клиентов, с использованием вирусных программных средств выросло более чем в два раза, что можно увидеть на диаграмме в Приложении 3.[[59]](#footnote-59) [[60]](#footnote-60)

Что же касается наиболее «свежих» данных, то исследование, проведенное компанией «Norton by Symantec» в 2017, отмечает, что более 44% процентов пользователей по всему миру столкнулись с правонарушениями и информационной и электронной среде. Всего эта цифра была около 1 миллиарда человек , среди 20 исследуемых стран. Совокупный ущерб по всему миру составил около 172 миллиардов долларов США или около 140 долларов США на человека, подвергшегося правонарушению в информационной среде, за один день. [[61]](#footnote-61)[[62]](#footnote-62)

Среди наиболее распространенных правонарушений по данным исследования стали: внедрение вирусного программного обеспечения (далее –ПО) на мобильное или стационарное устройство в 53% случаев правонарушения; попытка или кража с дебетовой или кредитной карты в 38% случаев; взлом паролей, а так же аккаунтов на сайтах или в социальных сетях; совершение заведомо ложного платежа; предоставление в результате мошеннических действий личной и/или финансовой информации.

Кроме этого, отчет представленный компанией IBM, по проведенному исследованию в рамках проекта X-Force , опубликованный в марте 2018 года, утверждает, что в целом картина киберпреступлений в изученных странах (их было около 100) не изменилась по сравнению с предыдущими годами, за исключением небольших нюансов, которые отражаются в основном в способах нападений для извлечения прибыли, так например наиболее популярными стали шифровальшики, которые за период 2017 года стоили компаниям порядка 8 миллиардов долларов.[[63]](#footnote-63)

Кроме этого, исследование отразило три основных тенденции изменившихся за один год, проведенного исследования:

- все целевые сферы для кибер-атак испытали снижение активности в количестве атак и количестве попыток незаконного получения доступа, на 18 и 22 процента, соответственно в 2017 году по сравнению с предыдущим годом;

- способ атаки через «внедрение вредоносного ПО», самого активного способа атак в 2017 году практически удвоился в количественном отношении по сравнению с предыдущим годом;

- финансовый сектор по прежнему остается наиболее подверженной отраслью для совершения атак по всему миру, уже второй год подряд.

Так же в отчете были отражены основные отрасли, которые, как и финансовый сектор были целевыми для угроз и атак на протяжении всего 2017 года[[64]](#footnote-64), и основные способы совершения кибератак, которые можно увидеть в Приложении 8, на рисунке 13.

Кроме этого отчет содержит описание наиболее опасных программ, вредоносного ПО, которые нанесли наиболее серьезный вред функционированию информационных систем, бизнес структур, критически-важной инфраструктуры, сводную схему о которых можно увидеть в Приложении, на рисунке 14.

Так в отчете фигурирует вредоносная платформа вымогатель - «Bad Rabbit», которая в середине прошлого года атаковала множество технических устройств, включая несколько Российских и зарубежных СМИ. Его распространение началось с территории Украины, где пострадали часть информационных систем метрополитена, аэропортов, «Укрэнерго» и даже часть компьютеров правительства Украины.[[65]](#footnote-65) И вирусное программное обеспечение NotPetya(или ExPetr), которое специалисты Лаборатории Касперского связывают с «плохим кроликом», поскольку часть кода обнаруженного экспертами, уже была обнаружена ими, во время предыдущих атак вирусного ПО - “NotPetya”.[[66]](#footnote-66)

Так же, в исследовании отражен вредоносный вымогатель WannaCry, кибер-вымогатель, который называется различными экспертами самой масштабной в истории человечества, поразила различные страны, общее число которых превысило 150, различные системы, банковские, медицинские, транспортные, государственные и другие учреждения. Из интервью «Первого канала» с экспертом по кибербезопасности Ильей Скачковым, можно сделать вывод о том, что если подобный вирус заражает информационную сеть , например больницы, а у IT-сотрудников нет резервной копии, то под угрозу попадет вся история и все данные пациентов, включая карточки, назначения и так далее. [[67]](#footnote-67)Данные угрозы можно легко экстраполировать и на все оставшиеся социальные сферы: образование, транспорт, налогообложение, охрана порядка и так далее, таким образом, что вопрос о вероятном ущербе не является риторическим.

Таким образом, следует отметить, что данная сфера преступлений имеет весьма обширную географию на земном шаре, и не ограничивается рамками отдельно взятой страны, что в еще большей степени усложняет процесс контроля и предупреждения распространения киберпреступности за пределы стран, регионов, материков.

Кроме этого, следует заметить, что на сегодня стала заметна смена основных приоритетов и целей киберпреступности, если раньше в большинстве своем злоумышленники атаковали лишь финансовый сектор, преследуя исключительно финансовые интсересы, то на сегодня наблюдается заметный сдвиг в сторону атак на критическую инфраструктуру государственных органов, информационных сетей здравоохранения и транспорта, средств массовой информации и других общественно-важных отраслей.[[68]](#footnote-68) Данные атаки и проблемы, могут стать причиной подрыва доверия граждан к государству, отсутствия стабильности и бесперебойной работы общественно-значимых институтов, а так же большие потери и расшатывание привычных основ государственности.

## 1.4 Политически мотивированные киберпреступления, определение и особенные случаи.

Следует отметить, что далеко не все случаи нарушения законодательства в области информационных технологий или с применением технических устройств нового поколения носят своей целью обогащение. Да, с определенной долей вероятности, можно предположить, что многие преступники в информационной сфере используют свои исключительные навыки, для приобретения средств к существованию, но зачастую, взломы, раскрытие конфиденциальных данных связанно с попыткой информационных активистов: повлиять на общественное мнение, изменить ход политических процессов, донести сообщение до масс или распространить определенную идею. В качестве примера, автор диссертационного исследования предлагает ознакомиться лишь с незначительным числом ярких случаев таких событий произошедших в информационной среде, посредством совершения киберпреступлений.

Одним из ярких примеров, такого рода преступлений, является атака, совершенная на дипломатические и политические информационные сети различных стран мира в 2009 году, тогда, в первую очередь под атаку попали несколько компьютеров расположенных в представительстве тибетского правительства и лично Далай Ламы, операция была проведена посредством нескольких устройств расположенных на территории США и КНР. Как утверждают специалисты целью атак злоумышленников стало получение доступа к секретной информации, шпионаж и получение доступа к видеокамерам и аудиомикрофонам представительств стран и негосударственных органов по всему миру. Операция получила название «Далай Лама под колпаком». [[69]](#footnote-69)

Так же, еще одним запомнившимся случаем, стала кибер-атака совершенная с использованием вирусной платформы «Stuxnet» по неофициальным данным разработанный группой специалистов из Соединенных Штатов Америки и Израиля, созданный специально для саботирования Иранской ядерной программы. [[70]](#footnote-70)Отличительной особенностью данного вредоносного ПО было то, что он мог навредить не только информационной и сетевой инфраструктуре, но и физически повреждать носители перегружая внутренние механические процессы технологических устройств и в первую очередь жестких носителей, которые и были основными целями данного вируса. Кроме этого, данный вирус смог вывести из строя более 1 тысячи обогатительных центрифуг на атомном объекте в г.Натанз.[[71]](#footnote-71)

Кроме этого, в том же 2014 году, неизвестными специалистами была осуществлена массовая атака информационных сетей и серверов, обслуживающих государственные органы Германии. Во время данной атаке был получен доступ к 14 парламентским серверам Бундестага, которые содержали себе пароли и коды доступа ко всем правительственным базам данных. О том, какая информация была похищена из информационных сетей, вопрос остается открытым, но среди подозреваемых сотрудники спецслужб Германии в первую очередь указывают российских хакеров, которые, по их мнению, пытались получить доступ к перепискам представителей власти ФРГ.[[72]](#footnote-72)

Еще одним ярким примером является кибератака, совершенная на информационные сети представительства Демократической Партии Соединенных Штатов Америки в 2016 году, тогда, в связи с вмешательством в работу систем и серверов Национального Комитета, на сайте «Wikileaks», были опубликованы личные письма, а так же другой цифровой контент, предназначенный для внутреннего пользования представителей партии. Данная информация, как утверждается исследователями,[[73]](#footnote-73) могла стать причиной подрыва доверия среди избирателей к кандидату от Демократической Партии США, и прямым образом повлиять на итоги голосования.

Более того, на ход данных выборов, как отражают исследователи и средства массовой информации могла повлиять так же и интернет-пропагангда, с размещением ложных новостей и расследований.[[74]](#footnote-74)

Представленный в диссертационном исследовании список лишь частично отражает общую тенденцию учащения случаев проникновения, получения незаконного доступа, взлома и использования информационных сетей правительств, представительств государств, организаций, фондов и тд. с целью изменения политической ситуации, донесения определенной позиции, влияния на политические процессы.

Поскольку в современной литературе редко встречается стандартизированное определение «политических киберпреступлений», для удовлетворения целям исследования, автор считает необходимым предложить собственное определение, выведенное на основе уже существующих определений «политического преступления», взятого из существующих исследований, и «киберпреступление» предложенного ранее в диссертационном исследовании.

Поскольку политические преступления обычно заносятся в ряд с другими уголовно-наказуемыми преступлениями, в законодательствах многих стран оно редко отражено отдельно. Данное определение, в необходимом понимании, можно широко найти лишь в исследовательской или политической среде.[[75]](#footnote-75) Обычно под политическими понимаются правонарушения, которые прямо или косвенно затрагивают сферу общественно-политических отношений, конституционный строй, представителей власти или политических процессов. По мнению Краковского К.П., политические преступления направлены на подрыв, ослабление, изменение общественного строя, отдельных общественных институтов или формы правления, совершаемое из политических побуждений. [[76]](#footnote-76)

Таким образом, для диссертационного исследования можно предложить определение, которое будет определять «политическое киберпреступление». **Политическое киберпреступление** - действие, совершаемое посредством использования персонального компьютера, мобильного устройства или других технических средств, связанных между собой сетью интернет, нарушающее права человека, а так же законодательно установленные нормы, совершаемое из политических побуждений и направленное на подрыв, ослабление или изменение текущего общественного строя, институтов власти и других элементов политического процесса.

Данное определение, с точки зрения автора диссертационного исследования, удовлетворяет цели исследования и поможет в дальнейшем изучении вопросов киберпреступности, совершаемой на международном и национальном уровне, а так же практик и мер по борьбе с данным явлением на территории Росскийской Федерации.

**Выводы по первой главе.**

Таким образом, исходя из изученного материала, можно сделать выводы о том, что феномен киберпреступлений, не является новым для современной науки, хотя, при этом, и требует дальнейшего изучения, особенно в вопросах точности и определении самого понятия. Была сделана попытка определения некоторых смежных понятий, таких как ИКТ, «киберпреступность», «кибербезопасность». Кроме этого автором диссертационного исследования был предложен собственный вариант определения киберпреступления, которое отмечает отличительную особенность данных правонарушений, а именно использование технических средств, в качестве инструментов совершения преступлений, одновременно с определением технических средств и информационных систем как объектов данных преступлений, а так же описывает причины и мотивы данных преступлений.

Так же отмечены основные характеристики, отличающие данный вид правонарушений от других уголовно-наказуемых деяний, а именно: большая вероятность сокрытия данных, сложности при проведении следствия, ввиду ограниченности информации, невозможности унификации национальных законодательств и подходов к следствию в данной области, сложности в процессе сбора данных, определения состава преступлении и др. Более того, автором отмечена тенденция к увеличению влияния такого аспекта, как трансграничность данных правонарушений.

Кроме этого, в первой главе отражается основная динамика и статистика за последние годы, и на основе изученных данных сделаны выводы об основных странах и отраслях общественно-экономических отношений подвергшихся за последние годы кибератакам. Среди основных стран пострадавших автором отмечаются страны Северной Америки в частности США, Канада, страны Европейского Союза, а так же Российская Федерация. Так же, автором сделано предположение о том, что данная география распространения напрямую связана с уровнем технологического развития государства, и интенсивности использования информационных систем в бизнес-структурах, общественных институтов, и личной жизни граждан, на территории перечисленных стран. Отмечен заметный переход, за последние периоды, от исключительно финансовых структур в сторону общественных и информационных структур, как целей киберпреступлений.

В ходе исследования так же был представлен ряд «громких» случаев киберпреступлений затрагивающих политические процессы в различных странах, в частности США, Иране, Германии, Российской Федерации, для подтверждения тезиса о том, что зачастую киберпреступления являются «политически мотивированными». Более того, автором исследования был предложен собственный вариант определения «политических киберпреступлений» на основе изученных данных и уже существующих смежных понятий. Таким образом, по мнению автора «политические киберпреступления» - это, совершаемые с помощью технических средств, связанных между собой интернетом и из политических побуждений, противоправные деяния, направленные на технические средства и информационные системы государственных органов и СМИ, с целью подрыва, ослабления или изменения существующего политического режима, государственных институтов или политических процессов.

# ГЛАВА 2 МЕЖДУНАРОДНАЯ КИБЕРПРЕСТУПНОСТЬ. ОПЫТ МЕЖДУНАРОДНОЙ БОРЬБЫ И УЧАСТИЕ РОССИИ.

## 2.1 Международная киберпреступность.

Поскольку многими исследователями отмечается, что на сегодняшний день на международную арену выходят многие участники, среди которых, помимо бизнес-структур, международных социальных сетей, образовательных учреждений и другие, в частности, киберпреступность, которая, используя такую особенность информационных технологий, как стремление к трансграничности, активно воспринимает передовые технологии для достижения своих целей. [[77]](#footnote-77) Так например в целях обхода цензуры на политическую информацию, во время беспорядков в Иране после президентских выборов в 2009 году, кибер-движение Anonimous Iran, запустили проект , который помимо паралича онлайн-присутствия государственной вещательной компании, так же вывел из строя личный сайт выбранного на тот момент президента М. Ахмадинижада,[[78]](#footnote-78)[[79]](#footnote-79) сообщают исследователи и информационный ресурс «ИноПресса», со ссылкой на репортеров из TheTimes.

Данный случай говорит о том, что преступая законодательно установленные нормы, специалисты из международного хакерского движения, преследовали политические интересы, для того, чтобы «подогреть» разгоравшиеся в стране протестные настроения, как утверждает один из участников «Анонимуса», с того момента, они начали тратить свое время и энергию на те страны, которые лучше всего могут воспользоваться их «помощью». [[80]](#footnote-80)

Однако такой случай далеко не единственный, кроме этого, такие международные группировки пользователей, которые зачастую удовлетворяя свои цели, преступают законодательно-зафиксированные нормы «во имя общего блага». Поэтому, в рамках данного исследования, прежде чем перечислить основные меры, направленные международным сообществом на противодействие нарушениям в информационной среде, автор считает нужным отметить наиболее ярких представителей, из числа международных преступных группировок, действующих и существующих в пределах информационных систем, действующих, весьма вероятно, из политических взглядов.

1)Первой из рассмотренных группировок автором диссертационного исследования выбрана хакерская группа «Анонимный интернационал» или как она была названа для простоты освещения сообществом «Шалтай Болтай, поскольку все сообщения и «сливы» информации, публиковавшиеся в сети участниками данного объединения, публиковались от имени сказочного персонажа. Существует данная группировка приблизительно с 2013 года, в список ее целей попали видные деятели политики, чиновники, общественные деятели и представители СМИ Российской Федерации, в том числе взломанные аккаунты Дмитрия Медведева (бывшего Президента РФ, премьер-министра на сегодняшний день), Аркадия Дворковича ( заместитель председателя правительства РФ), Дмитрия Киселева( телеведущего одного из федеральных каналов) и многие другие.[[81]](#footnote-81) Примечателен тот факт, что задержанные силами ФСБ РФ, предполагаемые участники данной группировки, это специалисты из области информационных технологий из различных ведомств и компании на территории России, в том числе Центра информационной безопасности ФСБ и Лаборатории Касперского[[82]](#footnote-82). Данные лица, к слову, в ходе следствия обвинялись в том, что сотрудничали с Центральным Разведывательным Управлением США. В их основную деятельность входили взломы и публикация личных переписок высокопоставленных чиновников и общественных деятелей, крупных организации и СМИ.

2)Следующей группировкой, совершавшей политические атаки, для исследования выбрана хакерская группа под названием «LulzSec» или «TheLulz Boat» , изначальным девизом которой было «смеемся над вашей защитой(кибер) с 2011 года». Несмотря на свою сравнительно небольшую историю( участники были задержаны в июне 2011 года) , группировка созданная изначально «ради смеха» отличилась серией громких преступлений против информационных сетей не только компаний, которые считались самыми защищенными на тот момент, но и официальными сайтами Сената Соединенных Штатов Америки, сайта Центрального Разведывательного управления США, сайта компании Sony (11 миллионов учетных записей) и социальной сети для Американских военнослужащих ( на которой они взломали 170 тысяч личных страниц) а так же различные компрометирующие данные о чиновниках и представителях военной элиты США.[[83]](#footnote-83) Участники хакерской группировки выкладывали всю открытую конфиденциальную информацию в сеть, а так же открыто поддерживали основателя «WikiLeaks» Д.Ассанжа. В одном из интервью, участник проекта «ЛулзСек», хакер под псевдонимом Водоворот, который называл себя «капитаном судна лулз», уточнил что группировка изначально насчитывала 6 специалистов, которые изначально действовали ради смеха, но после, перешли на «политически мотивированные атаки» .[[84]](#footnote-84)

3)Еще одной группой хакеров, совершающих преступления исходя из своих политических взглядов является «Сирийская Электронная Армия» (Syrian Electronic Army). Появление данной группировки связывают с началом гражданской войны в Сирии в 2011 году. Группа специалистов, которая поддерживает президента страны Башара Асада по заявлениям экспертов причастна ко многим громким политическим случаем в информационном пространстве среди которых: взлом сайтов новостных агентств «Нью-Йорк Таймс» и «Хаффлингтон Пост» и других значимых СМИ в 2014 году[[85]](#footnote-85), аккаунтов бывшего Президента США Б.Обамы, и бывшего президента Франции - Николя Саркози. Кроме этого группировка причастна к взлому сайта корпуса морской пехоты США[[86]](#footnote-86), на котором она разместила сообщения о том, что Сирийская Армия не должна быть врагом США, напротив – она должна стать их союзниками, и блокировки сайта армии США и размещении сообщений, о связи военных ведомств Америки с подготовкой бойцов оппозиционной армии.[[87]](#footnote-87) Это делается по словам самих представителей группировки на их официальных обращениях, для того, чтобы преподносить информацию о конфликте в Сирии, с правительственной точки зрения, в противовес той, которая преподносится западными политиками и СМИ.

4)Такими же методами и средствами совершения преступлений в информационной среде пользуется организация FancyBearz, целями которых становятся государственные представители различных стран, включая США и Германию, а так же Международный Олимпийский Комитет, и анти -допинг агентство - WADA. Впервые по словам экспертов данная организация проявила себя в середине 2000-х годов, и самыми громкими делами с участием данной группы хакеров стали: взлом переписки Ричарда Макларена, на основе доклада которого из состава сборной России на олимпиаде были исключены спортсмены принимавшие допинг, в которой специалисты из FancyBearz обличали политическую подоплеку происходящего и разглашали инструкции по «изгнанию Российской команды из игр».[[88]](#footnote-88)На основании разглашенной информации и ее посыла эксперты из анти-допинг агентства посчитали, что к взломам причастны Российские хакеры. Кроме этого данной группе специалистов приписывают взлом систем Национального Комитета Демократической Партии США, и получение компрометирующего материала на кандидата в президенты от Демократической партии, что могло повлиять на исход избирательной компании в США в 2016 году.[[89]](#footnote-89) Более того, данная группировка обвиняется так же, во взломах правительственных информационных систем Германии, в получении доступа к серверам партии ХДС и личной переписке канцлера Германии Ангелы Меркель. Немецкие специалисты ведомственных служб считают отказались подтвердить связь данных атак с российскими хакерами, однако, замечается, что данные хакеры уже известна своими атаками на внутренние сети бундестага и, вероятно, связаны с Главным Разведывательным Управлением ВС Российской Федерации.[[90]](#footnote-90)

5)Следует отметить, что даже среди такого рода акторов, отмечаются наиболее активные в проявлении своей позиции и наиболее серьезные в действиях и методах сообщества, примером таковых является группа хакеров известная как Анонимный (Anonimous) – международная группировка насчитывающая многочисленный состав участников по всему миру. Специалисты данной группировки преступников действуют довольно давно, приблизительно с 2003 года, и их целями становятся правительственные сети, религиозные и корпоративные веб-страницы, аккаунты чиновников и общественных деятелей. Данная группа использует все методы совершения киберпреступления для продвижения политических идей и распрастранения свободы слова, защиты прав человека, свободы обращения информации. Девизом данной организации является сочетание предложений: «Нас много, мы не забываем, мы не прощаем, ожидайте нас»[[91]](#footnote-91) ( пер. автора диссертационного исследования). Неоднозначность поведения данной группировки позволила сложиться массе слухов и легенд вокруг их истинных целей, однако факты говорят о том, что данное движение своей целью видит свободу слова и информации, раскрытие корпоративной лжи и неравенства, а так же достижения политической правды, что делает данную группировку скорее «идеей движения» по всему миру, особенно, с учетом призывов к участию, которые «хактивисты» оставляют после ряда атак.

Самыми громкими делами в рамках деятельности группы «Неизвестных», помимо случая отраженного вначале данной главы, стали: взлом информационных сетей компании Booz Allen Hamilton, сотрудничающей с министерством обороны, разведывательными службами и крупными производителями вооружений, а так же систем безопасности информационных структур для правительства США. Пираты выложили на своем сайте, PirateBay файл содержащий более 90 тысяч электронных адресов, паролей, личной информацией, с целью обозначить слабости в системах защиты фирмы, которая занимается разработкой программного обеспечения для предотвращения киберпреступлений и атак.[[92]](#footnote-92) Кроме этого случая, «Неизвестные» отметились весьма неоднозначным действием, когда в ноябре 2015 года подвергла атаки аккаунтов Исламского Государства (запрещенной в РФ организации) в различных социальных сетях. В ответ на теракты совершенные в Париже ранее, «Неизвестные» объявили кибер-войну боевикам ИГ, заявив при этом, что их возможности по сдерживанию Исламского Государства в Интернете намного выше, чем у любого государства мира, и они направят все усилия по сдерживанию активности террористов в сети.[[93]](#footnote-93) Так же СМИ говорят о причастности группы «Неизвестные» к взлому около 500 сайтов на территории КНР, включая правительственные ресурсы, с призывом к гражданам Китая, присоединяться к сопротивлению против строгости режима и контроля жизни граждан. Кроме этого на взломанных страницах, «хактивисты» размещали информацию о том, как обходить цензуру в интернет сети.[[94]](#footnote-94) Так же активисты данной группировки, на основе изученной информации, могут быть причастны к операциям, которые в информационной среде получили названия «Возмездие» (Operation Payback) в 2010 году, когда в ответ на заморозку платежными системами переводов платежей сайта WikiLeaks, хакерские атаки обрушились на платежные системы Visa и MasterCard, а так же операции «Захвати Уолл-Стрит» (Occupy Wall Street) в 2011 году, по атакам на сайт Нью-Йоркской биржи в борьбе против социального и экономического неравенства в мире.[[95]](#footnote-95)

Помимо перечисленных акций следует отметить, что данное движение имеет страницы в различных социальных сетях, где в различные периоды публикуются их заявления в отношении каких-либо событий или личностей. Так например на их странице содержатся видео-рассуждения на тему прошедших выборов в США, содержащие информацию, вероятно, добытую нелегальным путем, порочащую честь и достоинство Президента США Д.Трампа[[96]](#footnote-96), с обвинениями в ложности заявлений, предположении о будущем Соединенных Штатов Америки во время президентского срока и видео-расследование обстоятельств смерти Аарона Шварца интернет-активиста и борца за свободное распространение информации, к которым привели многочисленные нарушения конституции со стороны представителей власти, с обвинениями в «доведении до самоубийства», в дополнение к этому, активисты взломали сайт Комиссии по исполнению наказаний США, разместив там угрожающее сообщение для сотрудников.[[97]](#footnote-97)

Для более наглядного и схематичного представления деятельности крупных киберпреступных группировок, автор диссертационного исследования рекомендует ознакомиться с Приложением 5 рис.12.[[98]](#footnote-98)

## 2.2. Международный опыт борьбы и участие России.

Поскольку киберпреступность, сама по себе, не представляет нового явления, а так же достаточно долго исследуется в академической среде, специальными государственными ведомствами и международными организациями регионального и глобального масштаба, следует сказать, что на практике применяемость и эффективность данных норм не приносит ощутимых плодов, исходя из статистики, приведенной в первой части исследования. Более того, согласно отчету представленному «Accenture Security», к 2030 году совокупные потери, в результате киберпреступлений могут составить порядка 90 триллионов долларов США.[[99]](#footnote-99) В этой связи встает вопрос о том, какие же нормы применяются на международном и региональном уровне в вопросах противодействия киберпреступности.

Следует сказать, что одним из первых документов, принятых в 21 столетии, который очерчивал основные тенденции и отмечал основные стремления стран - участниц, подписавших данный договор в области информационного общества, стала Окинавская Хартия Глобального информационного обещства, принятая странами – участницами «большой восьмерки» 22 июля 2000 года. Она отметила важность и необходимость развития глобальных информационных систем для жизнедеятельности и взаимодействия правительства, а так же гражданского общества.

Помимо этого, в данном документе отмечалась важность стимулирования развития информационных технологий для содействия людям и обществу в получении знаний и идей. Более того, данный документ содержал положения о необходимости ликвидации цифрового неравенства в странах мира, а так же создания условий для здоровой и честной конкуренции в области развития информационных технологий. Но, что самое важное, данный документ так же, содержит положения о необходимости поддержания постоянного, быстрого, надежного и безопасного доступа к информационным технологиям. Кроме этого, подразумевается так же и защита прав интеллектуальной собственности и, что немаловажно, в документе говорится о том, что усилия международного сообщества, должны сопровождаться согласованными действиями по созданию свободного и безопасного от преступности киберпространства(ст.8,9).[[100]](#footnote-100) Следует заметить, что РФ в 2000 году, являясь членом клуба «большой восьмерки» подписала данную Хартию, приняв на себя все обязательства, изложенные в данном документе, таким образом, очертив для себя основные принципы развития информационного общества.[[101]](#footnote-101)

Кроме этого, правовую основу борьбы с киберпреступлениями так же составляют и документы принятый Организацией Объединенных Наций, так, например, Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 года, в некоторых статьях(ст.27,28,29) упоминает необходимость для стран-участниц ООН сотрудничество при разработке программ для подготовки кадров, при сборе и анализе данных и в другом сотрудничестве, создания , в силу возможности, кооперации для улучшения показателей в борьбе с организованной преступностью, использующей компьютеры, различные виды телекоммуникации и другие способы с привлечением современных технологий.[[102]](#footnote-102)

Одним из наиболее важных этапов в развитии международного подхода к вопросам борьбы с киберпреступностью, является Конвенция Совета Европы «О киберпреступности», принятая в Будапеште в ноябре 2001 года. Данный документ являлся одним из первых международных актов, регионального, а затем и глобального уровня, регламентировавших многосторонние меры по противодействию киберпреступности, а так же способствовала стандартизации европейских уголовных и других видов законодательств в данной отрасли.[[103]](#footnote-103) Кроме этого, данная конвенция положила начало процессуальному взаимодействию специализированных институтов стран, подписавших данный документ. Более того, данная концепция, как было упомянуто ранее, имела не только региональное значение, но и значение выходящие за пределы Европейского региона, так данную конвенцию подписали Япония, США, Автралия, Канада и ряд других стран[[104]](#footnote-104) Следует так же сказать, что по соятоянию на конец 2016 года, участниками данной конвенции, а значит полностью принимающими ее условия и принципы являются 50 стран мира, так же, 5 государств подписали документ, но не ратифицировали его.[[105]](#footnote-105) Согласно исследованию, проведенному, Нарутто и Якимовой, положения некоторых статей, указанных в данной конвенции являются прямым нарушением Российской конституции, и, кроме этого, противоречат законодательству, поскольку ряд действий, предусмотренных конвенцией может быть совершен без предварительного согласия и уведомления стороны, на которой действия предполагаются к совершению. Такое положение вещей прямым образом создает угрозу национальной безопасности России.[[106]](#footnote-106) Российская Федерация, таким образом, отказалась от подписания вышеупомянутой концепции в 2008 году, с распоряжением Президента РФ, о том, что документ о подписании данной конвенции утрачивает свою силу. [[107]](#footnote-107)

Поскольку, в рамках диссертационного исследования, в соответствии с целью поставленной для достижение, необходимо рассмотрения опыта международного сотрудничества, рассмотрим некоторые положительные аспекты, нашедшие свое отражение в Конвенции Совета Европы от 2001 года:

1)в рамках данной конвенции, была поставлена цель ее принятия и соблюдения, а именно выработка всеобъемлющей и гармоничной политики уголовного права, касающейся вопросов преступлений в сфере информационных технологий, которая бы защищала общество от киберпреступности, как на внутригосударственном, так и региональном уровне;

2) так же в конвенции классифицируются основные виды правонаршуений в киберпространстве, а дополнительные протоколы, принятые в г. Страсбург в 2003 году, дополняют классификацию некоторыми видами правонарушений, в частности дискриминацию, распространение расистских взглядов, ксенофобию и оправдание геноцида и расизма в киберпространстве.

3)особое внимание в рамках данной конвенции уделяется сфере международного сотрудничества.[[108]](#footnote-108)

Последняя из названных особенностей, видится автору диссертационного исследования особенно продуктивной, поскольку тот факт, что взаимная кооперация является одним из наиболее перспективных направлений развития политики, направленной на пресечение и наказание киберпреступлений, учитывая, названные в первой части исследования тенденции к трансграничности киберпреступности.

В дальнейшем страны-участницы данной конвенции, и, в частности Европейского Союза упрочили и углубили свое взаимодействие в рамках принятой концепции, принятием ряда директив, касающихся: противодействия сексуальной эксплуатации детей в информационной среде и распрастранению детской порнографии в сети; атак на информационные сети; сохранения безопасности сетей и информационных систем. Кроме, принятия указанных директив в рамках конвенции были созданы межгосударственные агентства и органы, катализирующие национальные усилия в борьбе с киберпреступностью, которые не подменяют собой национальные институты правоохранительных органов, но служат для координации и своевременного предоставления технической, экспертной и информационной помощи при проведении расследования.[[109]](#footnote-109)

Поскольку Российская Федерация отказалась от подписания данной конвенции, остается лишь предполагать, какие позитивные черты и тенденции данной конвенции могли бы служить на благо защищенности граждан от киберпреступников. Но тем не менее, в рамках региональных организаций данная конвенция хоть и является одним из основополагающих соглашений в области противодействия киберпреступности, она не единственная из документов, регламентирующих вопросы пресечения правонарушений в информационной среде.

Следует отметить, так же, что в рамках Содружества Независимых Государств действует соглашение[[110]](#footnote-110) « о сотрудничестве...в борьбе с преступлениями в сфере компьютерной информации», которое как и Европейская Конвенция призвано гармонизировать усилия стран-участниц в противодействии правонарушениям, совершаемым в информационной среде. Данное соглашение было принято в рамках СНГ 1 июня 2001 году, его подписали 10 государств-участников, а Россия является участником данного соглашения с 2008 года. [[111]](#footnote-111) По структуре и содержанию данное соглашение напоминает конвенцию Совета Европы, однако, меры перечисленные в нем, являются более узкими, по сравнению с конвенциональными, более того в нем есть ряд положений которые перекликаются с информацией и положениями изложенными в конвенции:

1) в нем дана классификация основных преступных деяний, в сфере информационных технологий, как уголовно наказуемых деяний, отмечены основные, среди которых- неправомерный доступ к информации, в случае если это влечет изменение информации в том или ином виде;создание или использование вредоносных программ; нарушение баз данных защищенных авторским правом, а так же нарушение правил эксплуатации технических средств, которые привели к изменению охраняемой информации или нанесли вред или имело тяжкие последствия.

2)Определены основные компетентные органы и сферы их сотрудничества, а так же порядок взаимодействия данных компетентных органов.

Следует отметить, что ряд стран, в том числе Азербайджан, и Украина приняли соглашение с оговорками, а Грузия и Туркменистан отказались от подписания.[[112]](#footnote-112)

Так же, следует упомянуть, что в 2013 году, СНГ была принята так же концепция, касающаяся вопросов взаимодействия участников Содружества, в борьбе с преступлениями, которые совершаются в информационной среде, которую одобрили 9 стран. В данной концепции, развивая положения концепции СНГ о борьбе с преступностью от 1999 года, определяется целью расширение и укрепление стран-участниц в борьбе с преступлениями с применением информационных технологий, определяет основные цели, основные задачи, формы и систему обеспечения данного сотрудничества. Кроме этого, данная концепция, так же очерчивает основные направления сотрудничества стран СНГ в данной сфере.[[113]](#footnote-113)

Хочется сказать, что Организация Объединенных Наций, как ведущая международная организация универсального типа, за последние годы активно принимает участие в процессах взаимодействия со странами и другими региональными организациями в вопросах обеспечения повестки дня и взаимодействия в сфере кибербезопасности. Так, например, в 2011 году, по итогам 12 конгресса ООН по предупреждению преступности и уголовному правосудию, была принята Резолюция, решением которой, была создана межправительственная группа экспертов, работа которой была направлена на всестороннее исследование проблем киберпреступности в мире, а так же изучение мер, принимаемых странами-участниками ООН по противодействию.[[114]](#footnote-114) Итогом работы данной группы экспертов стал доклад по Всестороннему исследованию проблем киберпреступности подготовленный и выпущенный в феврале 2013 года.[[115]](#footnote-115) Как отмечают, специалисты данного исследования, большая часть стран, не считают необходимым введение дополнительных форм в свои уголовные кодексы, относительно киберпространства и киберпреступности, поскольку эффективное сотрудничество уже возможно, на основе существующих соглашений и механизмов взаимодействия.[[116]](#footnote-116) К слову, так же считают и специалисты, Евроазиатской группы. Согласно их типовому исследованию по киберпреступности. Эксперты отмечают, что все существующие соглашения, в частности региональные, такие как соглашения и концепции, ЕС и Совета Европы, Стран СНГ, Африканских межправительственных организаций, Лиги арабских государств и ООН, так или иначе, дополняют друг друга, особенно в вопросах положений уже описанных в Конвенции Совета Европы от 2001 года.[[117]](#footnote-117) Кроме этого, под эгидой Управления ООН по наркотикам и преступности, в 2015 году была подготовлена и одобрена Дохинская декларация[[118]](#footnote-118), всецело описывающая направления борьбы с преступностью, в том числе по противодействию киберпреступности.

Следует отметить также, что при ООН, как специализированное учреждение действует Международный Союз Электросвязи, который был основан еще в 1865 году, как Международный телеграфный союз, но стал специализированным учреждением ООН в 1947 году. В состав данного союза входят, а так же являются участниками 193 государства мира, а так же около 800 организаций по всему миру, включая другие организации регионального значения, академические заведения, бизнес-структуры. Штаб данного учреждения находится в Женеве, помимо него по миру действует 12 региональных представительств( в Российской Федерации оно находится в г. Москва).[[119]](#footnote-119) Поскольку данный Союз входит в состав ООН, как специализированное учреждение, в круг его основных направлений, помимо разработки технических стандартов информационного вещания и присоединения к обмену информацией, а так же улучшения доступа к ИКТ по всему миру, входят так же и вопросы исследования нарушений в информационной среде. В этой связи МСЭ еще в 2007 году, запустил программу «Глобальная Программа по Кибербезопасности» (ITU Global Cybersecurity Agenda), направленную на поддержание безопасности и открытости в информационном обществе 21 столетия. Данная программа работает на основе 5 основных принципов:

- законодательных мер;

- технических и прикладных инициатив;

- организационной структуризации;

- наращивании потенциала в информационной среде;

- международном сотрудничестве в данной сфере.[[120]](#footnote-120)

Кроме этого Союз ежегодно собирает индексы различных исследовательских групп, организаций по регионам, бизнес-структур по странам, организациям и другим основаниям, для более детального изучения и представления, а так же анализа в динамике основных тенденций и изменений в вопросах кибербезопасности, количестве атак, угроз и уязвимостией, полученных в результате очетов данных организаций, исследовательских групп и т.д. [[121]](#footnote-121) Так же, в результате исследования проведенного МСЭ в 2017 году, был представлен отчет «Global Cybersecurity Index (GCI) 2017», который отразил основные меры и направления работы исследованных государств, по противодействию киберпреступности в нормативных мерах, стратегических решениях согласно пяти принципам Глобальной Программы по Киберпреступности, обозначенной выше, в диссертационном исследований:

- В вопросах законодательства Союз исследовал: наличие на территории государства или региональной организации правовых мер, основанных на существовании и функционировании институтов и рамок, по вопросам киберпреступности и кибербезопасности;

- в соответствии с принципом технических и прикладных инициатив Союз исследовал наличие в стране или организации мер по развитию технических институтов и рамок, занимающихся вопросами кибербезопасности;

- в соответствии с принципами организационной структуризаии Союз исследовал наличие в стране или организации мер направленных на развитие политики или стратегии, координирующей вопросы кибербезопасности на национальном уровне;

- в соответствии с принципом наращивания потенциала Союз исследовал наличие мер основанных на существовании научных и исследовательских разработок, образовательных и квалификационных программ, сертифицированных организаций и агентств, занимающихся улучшением информационного потенциала страны;

- в соответствии с принципом взаимодействия Союз исследовал наличие мер, основанных на существовании кооперационных, партнерских взаимоотношений и инструментов обмена информацией на национальном и региональном уровнях.[[122]](#footnote-122)

В ходе изучения данного отчета, составленного МСЭ, было выявлено, что по пяти основным показателям, страны разделились на три группы, первая из которых это страны, кибербезопасность в которых находится на стадии запуска ( сюда вошли 96 стран, индекс которых наименее низок и набирает до 50 пунктов, относительно лучших показателей), следует отметить, что основное число данных групп, занимают страны Африки, Ближнего Востока и часть стран Средней Азии, которые лишь начали разрабатывать вопросы кибербезопасности. [[123]](#footnote-123)

Вторая группа стран (всего их 77), индекс данных стран согласно отчету составляет от 50 до 89 пунктов, по расчетам специалистов МСЭ, их уровень кибербезопасности находится на «зрелом» этапе. Данные страны разработали комплексные соглашения и рамки на национальном уровне, а так же включились в инициативы и программы по кибербезопасности на международном уровне.[[124]](#footnote-124)

Третья группа лидирующих стран[[125]](#footnote-125), наименьшее число от общего количества – 21 страна, рейтинг которых составил выше 90 пунктов, по данным исследования специалистов МСЭ, которые демонстрируют высокий уровень показателей по всем направлениям, отмеченным в Глобальной Программе по Кибербезопасности. К слову, в рейтинг 21 ой лучшей страны входит и Российская Федерация, а СНГ является 2[[126]](#footnote-126) объединением в рейтинге по уровню выполнения необходимых принципов Глобальной Программы. [[127]](#footnote-127)

В соответствии с отчетом, в общем рейтинге Российская Федерация значится на 11 месте, кроме этого в 10 лучших стран вошли – Сингапур(одна из ведущих стран, согласно данному отчету),Малайзия, Оман, Эстония, Мавритания, Австралия, Грузия, Франция и Канада. [[128]](#footnote-128)Худшей страной, по исполнению основных положений Глобальной Программы, была признана Экваториальная Гвинея.

Российская Федерация был отмечена как вторая лучшая страна в составе СНГ, благодаря лучшему развитию информационного потенциала, отмеченному в различных направлениях от высоких стандартов в исследовательской и научной деятельности по данному направлению, а так же высокой осведомленности по данным вопросам среди граждан, а так же среди отечественной информационной индустрии. Кроме этого, специалистами МСЭ, Российская Федерация была обозначена как яркий прмер стратегического подхода к вопросам кибербезопасности, благодаря официально принятым документам среди которых: Национально Стратегии Безопасности от 2000 года, и Концепции Внешней политики РФ от 2013 года, Доктрину Информационной Безопасности РФ от 2000, в соответствии с которыми, каждый государственный орган проводит ежегодную проверку и анализ работы информационных систем и сетей. [[129]](#footnote-129)

**Выводы по второй главе.**

Таким образом, на основе изученных и представленных материалов, следует сделать вывод о том, за последние годы преступность в информационной среде заметно усилила активность. Участились случаи совершения киберпреступлений по политическим мотивам и убеждениям, помимо привычных экономических мотивов. Согласно замечаниям исследователей, на сегодняшний день, множественные акторы активно выходят на мировую арену, принимая на себя передовые технологии, в том числе и киберпреступность. Заметно, так же стало и учащение случаев, когда совершение киберпреступлений по политическим соображениям, проводилось не отдельно взятыми правонарушителями, а в составе организованных групп, причем целями становились как Средства Массовой Информации, так и отдельные видные деятели политики, в частности президенты стран, общественные организации, военные и судебные ведомства различных стран. В рамках диссертационного исследования были представлены некоторые случаи совершения киберпреступлений в составе организованных групп ( Amonimous,FancyBearz, LulzSec, Syrian Electronic Army, Анонимный интернационал), получившие наиболее широкую огласку в связи с масштабностью и уроном нанесенным в ходе данных правонарушений. Данные преступления, по сути своей пытаются дескридитировать власть в глазах общественности, открыть какие-либо тайные факты, неизвестные страницы из различных политических процессов, для того, чтобы подорвать доверие граждан к государственности.

В особенности автор диссертационного исследования хочет отметить тот факт, что зачастую такие международные киберпреступные группировки обвиняются в связях с государственными и военными структурами, что, с учетом особенностей данных видов преступлений (таких как сложность расследования, сбора доказательств и стремления к трансграничности), делает их, с высокой вероятностью, инструментом удобным для ведения «теневой» нелегальной политики со стороны одного государства против другого.

Кроме этого во второй главе были рассмотрены основополагающие документы и положения Европейского Союза, Организации Объединенных Наций и Стран СНГ, касающихся и очерчивающих направления противодействия киберпреступности. Более того, были рассмотрены некоторые виды исследований, проведенных, в том числе и ООН и специализированными учреждениями при данной организации, которые изучают основные методы и способы борьбы различных стран и региональных объединений против киберпреступности. Автором диссертационного исследования, в результате изучения данных отчетов, делается вывод о том, что опыт международной борьбы с киберпреступности хоть и является обширным, тем не менее, согласно статистике, не достаточным для того, чтобы успевать за развитием методов и способов ведения киберпреступлений. Роль ООН в данном вопросе остается координирующей и очерчивающей общие рамки, тогда как основная работа и реальные примеры взаимодействия все же проявляются на региональных уровнях, примером тому является обширное подписание и исполнение Конвенции Совета Европы от 2001 года, в которой РФ не участвует с 2008 года. В исследовании сделанном Международным Союзом Связи отмечается так же, что Содружество Независимых государств, которые в свое время приняли похожие соглашения, так же являются примером активной борбы с киберпреступностью на региональном уровне. То же касается и Российской Федерации, которая отмечается исследователями из МСЭ, как один из лидирующих игроков в процессах противодействии киберпреступности, в соответсвии с Глобальной Программой по Кибербезопасности от 2007 года.

Однако, не умаляя, положительной динамики развития данной сферы, хочется отметить так же и ряд негативных тенденций, затрудняющих скорое развитие и всеобъемлющий подход к вопросам борьбы с киберпреступностью на международном уровне:

- ускоряющаяся тенденция к фрагментации международных подходов в рамках отдельно взятых региональных объединений, которые принимают и реализуют собственные специфические подходы к данной проблеме;

- противоречия между национальными государствами по вопросам основных законодательных инициатив и принципов многостороннего сотрудничества, которые, как например в случае с отказом РФ от подписания Конвенции Совета Европы от 2001 года, могут поставить под удар национальных суверенитет страны;

- наличие правового отставания от процессов развития информационных технологий, когда, юридические нормы не успевают урегулировать поведение с использованием конкретных технологий, а в ближайшем времени появляются уже другие, поведение в которых так же требует регулировки.

Между тем, государства и международное сообщество активно стремится к преодолению противоречий и проблем, возникающих в процессе борьбы с киберпреступностью, используя при этом инструменты и учреждения ООН, Европейского Союза, Содружества Независимых Государств, Африканских и Арабских объединений, создающих и улучшающих национальные и региональные нормы в данной сфере.

# ГЛАВА 3 БОРЬБА РОССИЙСКОЙ ФЕДЕРАЦИИ С КИБЕРПРЕСТУПНОСТЬЮ НА НАЦИОНАЛЬНОМ УРОВНЕ.

Переходя, к исследованию вопросов о законодательном закреплении борьбы с киберпреступностью на территории РФ, хочется отметить, что по данным, одного из крупных медиа-мониторинговых центров на территории Российской Федерации, аудитория интернет-пользователей в России к марту 2017 года составляла 87 миллионов человек. При этом значимую часть из этой цифры и наиболее быструю динамику демонстрирует распространение аудитории, использующей мобильные технические устройства для получения доступа в сеть Интернет.[[130]](#footnote-130)

Кроме этого, по данным Российской Федеральной Службы Статистики «Росстат», число активных пользователей подвижной телефонной связи, с доступом в интернет на 2017 год составил порядка 125 миллионов человек, а число активных абонентов фиксированного доступа к сети интернет составило порядка 31 миллиона человек.[[131]](#footnote-131)

Поскольку аудитория пользователей услуг связи, в том числе и сети Интернет, на территории Российской Федерации, растет из года в год, и расширяется не только в количественном, но и возрастном измерении, в рамках диссертационного исследования существует необходимость уточнения документов и мер, направленных на защиту стабильности, конфиденциальности и безопасности использования всех положительных направлений развития информационного общества на территории нашего государства.

## 3.1 Документы, принятые на территории Российской Федерации.

Традиционно, основным документом принятым Российской Федерацией в сфере информационных технологий является «Стратегия информационного общества Российской Федерации», последняя ее версия очерчивающая основные приоритеты России вплоть до 2030 года от 9 мая 2017 года[[132]](#footnote-132) официально отменила предыдущую ее редакцию от 2008 года, которая с того момента была признана утратившей силу. В данном документе:

-утверждена основная стратегия информационного развития Российской Федерации вплоть до 2030 года;

-были определены цели, а так же задачи и способы по реализации внутренней, а так же внешней политики России в сфере применения и развития ИКТ;

- было так же отмечено, что информационные технологии, в том числе социальные сети, Средства Массовой Информации стали постоянной частью жизни для большего числа граждан Российской Федерации;

- в качестве приоритетов для развития информационного общества РФ были выделены: приоритет формирования информационного общества, с учетом потребностей получения достоверной и качественной информации, а так же обеспечение конкурентноспособности Российских информационных технологий на международном рынке. Кроме этого данный документ приоритетной целью ставит исключение возможности создания анонимности и безнаказанности правонарушений в информационной среде, на основе создания механизмов партнерства и выработки системы доверия к использованию сети Интернет на международном уровне, а так же создания возможности сохранить конфиденциальность и безопасность при использовании информационных технологий.

Еще одним основополагающим документом РФ в области информационной безопасности является «Доктрина информационной безопасности РФ [[133]](#footnote-133) от 5 декабря 2016 года, которая является собранием официальных государственных взглядов на задачи, принципы и основные цели, а так же направления Российской Федерации в вопросах достижения информационной безопасности государства. Под «информационной безопасностью» данный документ подразумевает полную защищенность интересов Российской Федерации и информационной среде, которая достигается гармоничный совокупностью интересов личности, а так же государства и общества.

Интересы личности в этом контексте достигаются через реализацию констиутуционных прав граждан РФ на полный, стабильный и безопасный доступ к информации, и ее использование в легальных формах, а так же на защиту этой информации со стороны государства.

Интересы всего общества достигаются соблюдением интересов личности и создания правового государства в информационном обществе.

Интересы государства же достигаются через соблюдение интересов личности на соблюдение его конституционных прав и свобод, а так же на создание для гармоничного развития Российской информационной структуры, в целях обеспечения суверенитета и целостности РФ и конституционного строя, создания равноправного и взаимо-выгодного международного сотрудничества. [[134]](#footnote-134)

Данной доктриной выделено 4(четыре) основных составляющих национальных интересов РФ в информационной среде, соответственно угрозы национальным интересам России в данных сферах признаются принятой доктриной угрозами в информационной безопасности РФ:

1) Соблюдений прав и свобод человека и гражданина, зафиксированных в конституции, в вопросах получения гражданами информации, а так же обладания ей;

2)Информационное обеспечение национальной политики России, а именно, открытого и достоверного донесения до международного сообщества информации о государственной политике Российской Федерации, а так же ее официальной позиции по основным событиям международной и российской действительности. Кроме этого, данный интерес РФ связан с открытым доступом граждан России к государственным информационным ресурсам;

3)Еще одним интересом РФ в информационной среде является развитие современных технологий в информационной сфере, Российской информационной индустрии. Кроме этого, ставится потребность в накоплении и сохранности, а так же эффективном использовании информации, жизненно необходимой для науки, технологического перевооружения и т.д.

Главным направлением для исследования в соответствии с целями текущего диссертационного исследования является следующий пункт:

4)Интерес в защите информационных систем и ресурсов от несанкционированного проникновения, а так же обеспечение защиты информационных систем и систем ИКТ, уже существующих и еще создаваемых на территории России.

Данный интерес , согласно доктрине, подразумевается реализовывать путем повышения безопасности информационных систем первичных связей, а так же систем информации федеральных органов и всех остальных систем информации, включая банковские , военные, хозяйственные сферы деятельности, финансово-кредитных систем. Кроме этого данный интерес должен быть реализован путем интенсификации развития средств защиты и аппаратного ПО, по защите информационных, а так же развития контроля за соблюдением эффективности данного ПО. Так же, достижение этого интереса осуществляется, посредством защиты государственной тайны и обеспечения международного сотрудничества с сфере использования информационных ресурсов и противоборства информационным угрозам.

Кроме вышеуказанных документов, еще одним всеобъемлющим актом, принятым Российской Федерацией на национальном уровне, является Стратегия национальной Безопасности РФ от 31 декабря 2015 года[[135]](#footnote-135), которая отменила действующий до этого документ о стратегии национально безопасности РФ от 2009 года. Данный документ так же содержит положения о том, что одной из угроз национальной безопасности для России, является деятельность группировок различного рода, в том числе и экстремистских, по уничтожению и нарушению работы критически важной инфраструктуры государства, в том числе и информационной. Кроме этого действия, с использованием информационных технологий для распространения радикальных идей, ксенофобии и нарушение ущерба гражданскому и политическому миру и стабильности внутри общества.( гл. IV п. 43.) В этой связи одними из ключевых направлений в целях обеспечения безопасности признаются: совершенствование систем выявления, анализа и противодействия угрозам в информационной среде, а так же предприятие мер по повышению защищенности граждан РФ и общества от разлагающего воздействия в информационной среде. (гл. IV п.47)

Более того, положения касающиеся противодействия киберпреступности содержатся и в Концепции внешней политики РФ от 30 ноября 2016 года.[[136]](#footnote-136) В данной концепции говорится о том, что увеличиваются масштабы трансграничных вызовов и угроз, среди которых указана и киберпреступность, стремительно увеличивающая уровень и масштабы.(гл II. п 16,17). Так же среди региональных приоритетов внешней политики РФ, среди прочих, названо наращивание взаимодействие и взаимовыгодный диалог с Европейским Союзом, по основным вопросам внешней политики, включая преступность и киберпреступность.(гл IV п.64)

В основном, согласно исследованию Дмитрика Н., законодательство РФ в информационной безопасности развивается по следующим направлениям:

-закрепление общих положений, касательно доступа к информации, конфеденциальности, а так же защиты информации, основным законом по которым является закон « Об информации, информационных технологиях и защите информации»;

- определение правового статуса для различных видов информации( так ФЗ « О персональных данных» регулирует правововой режим для персональной информации; Гражданский Кодекс РФ и Семейный Кодекс РФ регулируют правовой режим для информации, касающейся семейной тайны, а так же тайны личной жизни; закон «О государственной тайне» РФ регулирует режим для информации содержащей государственную тайну и т.д);

- административное регулирование деятельности направленной на защиту информации;

- определение порядков осуществления оперативных и розыскных мероприятий, а так же борьба с преступлениями в информационной среде, посредством закрепления различных составов преступлений в УК РФ.[[137]](#footnote-137)

Так, например, Уголовный Кодекс Российской Федерации предусматривает наказание за противоправные деяния в сфере компьютерной информации, отраженные в 28 главе кодекса[[138]](#footnote-138):

- 272 статья УК РФ – в случае неправомерного доступа к компьютерной информации;

- 273 статья УК РФ – в случае создания, использования и распространение вредоносных компьютерных программ;

- 274 статья УК РФ – в случае нарушения правил эксплуатации средств хранения и обработки, передачи информации и информационно-коммуникационных сетей;

- 274 статья п.1 УК РФ – в случае неправомерного воздействия на критическую государственную информационную структуру РФ.

Кроме этого, Дмитрик Н., отмечает так же, что составы преступления закрепленные в УК РФ, которые можно отнести к киберпреступности содержат так же: мошенничество в сфере компьютерной информации, хищение чужого имущества или хищение права на чужое имущество путем манипулирования компьютерной информации и вмешательство в процессы функционирования средств хранения и обработки финансовой информации.[[139]](#footnote-139)

## 3.2 Органы и организации, занимающиеся вопросами киберпреступности на территории России.

Одним из центральных органов, занимающихся вопросами пресечения преступлений является Министерство Внутренних Дел РФ, поскольку уголовно-наказуемые преступления входят в сферу компетенции именно данного органа.

Однако в составе МВД существует специальное управление, на сегодняшний день называющееся «Управление «К» МВД РФ», основным направлением работы которого является борьба с киберпреступностью на территории РФ. [[140]](#footnote-140)

Из истории данного подразделения следует то, что еще в 1986 году, для обеспечения безопасности органов внутренних дел, так же для борьбы с различными радиопомехами, выявления и работы со специальными устройствами ( созданными, запрограммированными и приспособленными) для неправомерного получения информации, а так же для предотвращения попыток проникнуть в информационные сети в системе Министерства Внутренних Дел Советского Союза была организована работа службы РЭБ, Управления радиоэлектронной борьбы, или широко известное под именем «Управление-Р».

В то время, в компетенции данного управления входили не оперативно-розыскные, но исключительно оперативные задачи. В связи с действующим на тот момент законодательством преступлений в компьютерной сфере не существовало совсем. В соответствии с законодательством их еще не существовало, но на деле по данным с сайта Министерства Внутренних Дел РФ, они уже совершались на протяжении нескольких лет. [[141]](#footnote-141) Одно из первых преступлений с применением компьютера было зафиксировано Международной Полицией «Интерпол», данное деяние было зафиксировано на территории г. Вильнюс в 1979 году. Тогда, оператор почтовой связи с помощью программно технического комплекса, совершал мошеннические действия с «двойной» бухгалтерией, присваивая себе остатки денег, долгое время оставаясь безнаказанным.

Позже уже в 1997 с принятием упомянутого в диссертационном исследовании 28 раздела Уголовного Кодекса Российской Федерации, данному управлению был назначен статус специализированного органа дознания- оперативно розыскного подразделения.

Однако численность и техническое обеспечение данного подразделения на тот момент, не позволяли в полной мере решать задачи, возросшие с приобретением нового статуса. Более того, данная ситуация усугубилась когда в новую редакцию уголовного кодекса РФ от 1997 года и , в еще действовавший, до 2001 года, старый формат уголовно процессуального кодекса РСФСР от 1964 года, были внесены значительные изменения и поправки.

Данные поправки возложили на Управление Р, дополнительные обязанности по обеспечению функционирования, дейстующей на сетях электросвязи с 1994 года, системы оперативно розыскных мероприятий. Учитывая данную ситуацию и возникшие сложности, в 1998 данное управление было расширено до Управления по борьбе с преступлениями в сфере высоких технологий. Кроме этого, в его составе выделились три отдельных подразделения:

1. Отдел по борьбе с преступлениями в сфере компьютерной информации;

2. Отдел по борьбе с преступлениями в сфере телекоммуникаций;

3. Отдел по борьбе с незаконным оборотом радиоэлектронных (РЭС) и специальных технических средств (СТС).

Более того, в 81(восьмидесяти одном) субъекте РФ, на различных уровнях управления Министерства Внутренних Дел , вскоре были созданы похожие подразделения и отделы по борьбе с преступлениями в сфере высоких технологий. Поначалу, штат данных подразделений составляли сотрудники с техническим образованием, что отрицательно отражалось на процессуальных вопросах и качестве расследования преступлений. Лишь к 2000, когда подразделения укомплектовались сотрудниками с юридическим образованием, ситуация изменилась к лучшему.

Кроме этого в 1999 году согласно Распоряжению Правительства РФ под номером 1701 от 22.10.99 Об усилении борьбы с преступлениями в сфере высоких технологий[[142]](#footnote-142), бюджетные средства, выделенные на содержание правоохранительные органы были перераспределены на противодействие преступности в рамках указанной программы. Данные средства были перенаправлены «на усиление борьбы с преступлениями в сфере компьютерной информации, правонарушениями с использованием ЭВМ, сетей и систем».

Кроме этого в соответствии с указанным распоряжением, также, были проведены различного рода семинары и встречи международного уровня, по вопросам борьбы с компьютерной преступностью, созданы контакты с специальными службами в зарубежных странах, занимающихся данными правонарушениями. В итоге, после проведения всех мероприятий был достигнут качественный перелом в уровне противодействия преступлениям в компьютерных системах, как на территории РФ, так и на международном уровне.

В 2002 году, данное управление было сокращено и переведено в материально техническом и штатном плане в Бюро Специльных и Технических мероприятий, работающее при Министерстве Внутренних Дел РФ. На сегодняшний день, данные подразделения называются «Отделы К (компьютерные престпления)» В их структуре сохранились так же профильные подразделения, отвечающие за конкретную сферу, перечисленные ранее в диссертационном исследовании.

Помимо подразделений «К» в структуре управления МВД РФ по Борьбе с экономическими преступлениями еще в 1997 году в субъектах федерации были созданы Отделы по борьбе с преступлениями в сфере экономики и компьютерной информации. Данные отделы , тоже являются специальными органами дознания, и в соответствии с действующим законодательством, занимаются выявлением, расследованием и пресечением хищений и мошенничества с использованием электронных докмуентов, данных, объектов авторского права, которые хранятся на информационных носителях.[[143]](#footnote-143)

Так же в 1997 году при Следственном Комитете МВД Российской Федерации, были созданы специальные следственные отделы по расследованию преступлений в сфере экономики и компьютерной информации. Следователи этих отделов, тесно взаимодействуют между собой с органами дознания – Отделами ОБЭП и «К».

В феврале 1998 в соответствии с указанием Главного управления кадров, состоялся первый выпуск специалистов подготовленных по программе «Расследование преступлений в сфере компьютерной информации», в рамках государственного стандарта по повышению квалификации в Волгоградской академии Министерства Внутренних Дел Российской Федерации.

Хочется так же отметить основные направления работы Управления «К» при Министерстве Внутренних Дел Российской Федерации[[144]](#footnote-144):

1)Первой целью является борьба с преступлениями в сфере компьютерной информации, которая осуществляется посредством: выявления и пресечения неправомерного использования информации, получения доступа к ней; борьба с изготовлением использованием и распространением вредоносного ПО; пресечение мошенничества в сфере электронных платежных систем; борьба с распространением детской порнографии через Интернет;

2) Второй целью Управления «К» является пресечение преступных действий в информационных сетях включая интернет, которое реализуется через: выявление и пресечение неправомерного доступа к коммерческим, государственным и частным каналам связи; выявление и предупреждение преступлений совершенных с использованием проводной и сотовой связи; противодействие мошенничеству через информационные сети и интернет;

3) Кроме этого, в цели Управления «К» МВД РФ входит противодействие незаконному обороту специальных технических и радиоэлектронных средств, применяющихся при совершении преступлений;

4)Расследование и предотвращение, пресечение фактов нарушения авторских, а так же смежных прав;

5) Обеспечение международного сотрудничества и взаимодействии в этой области.

Помимо законодательства и официальных государственных органов, работающих по направлению противодействия киберпреступности на территории РФ, действуют так же и негосударственные компанию в сферу исследований которых входят вопросы обеспечения кибербезопасности и защищенности информации.

Ярким примером такой организации является Лаборатория Касперского, международная компания, работающая в сфере информационной безопасности еще с конца двадцатого века. Многолетний опыт работы компании и специалистов в сочетании с высоким профессионализмом позволили создать одну из самых перспективных организаций по защите в сфере информационных систем, а так же проводить значительные исследования и инициативы в области кибербезопасности. На сегодняшний технологии разработанные в компании обеспечивают защиту более 400 миллионов человек по всему миру, а так же около 270 тысяч организаций, являющихся корпоративными клиентами Касперского. Уже упоминавшийся в исследовании Глобальный Индекс Кибербезопасности, составленный Международным Союзом Электросвязи[[145]](#footnote-145), в своем отчете приводит пример Информационные Бюллетени Лаборатории Касперского, отражающие индекс безопасности информации на определенном ареале(среди корпоративных и индивидуальных клиентов), как один из немногих, на основании которого можно делать выводы о совокупном потенциале кибербезопасности в мире.

Кроме этого, частично информация, представленная в Упомянутых Бюллетенях, легла в основу текущего диссертационного исследования, в вопросах отражения статистики и динамики киберугроз на международном и национальном уровне.[[146]](#footnote-146)

**Выводы по третьей главе.**

Исходя из материалов и документов национального уровня, исследованных в третьей части, автор диссертационного исследования делает вывод о том, что Российская Федерация имеет ряд всеобъемлющих документов, касающихся обеспечения развития информационного общества, противодействия угрозам данного этапа развития, в том числе и киберпреступности, ряд документов освещенных в ходе диссертационного исследования содержат как основные приоритеты Российской Федерации. Среди отмеченных приоритетов были выделены: обеспечение прав и свобод граждан в условиях информационного общества, необходимость создания стабильного и безопасного доступа к информационным технологиям, противодействие преступлениям, совершаемым в информационной среде, а так же с применением высоких технологий.

Тем не менее, принятые документы, так же, отражают и новые угрозы, исходящие от киберпреступности. Среди данных угроз отмечается: уязвимость критически важной экономической, государственной и общественной инфраструктур, стремление к усилению международной активности экстремистких, террористических и преступных группировок, активно использующих информационные технологии в своих целях, а так же угроза информационных войн, с участием сторонних государств.

Так же было отмечено стремление законодательства Российской Федерации не к принятию новых уголовно-процессуальных норм, по противодействию киберпреступлениям, а определение составов преступлений в соответствии с уже существующими статьями в Уголовном и других кодексах России.

В ходе диссертационного исследования, кроме документов очерчивающих основные направления борьбы с преступлениями в информационном пространстве, были изучены органы в составе государственных институтов, курирующие вопросы противодействия киберпреступлениям.

Особо отмечена роль, Управления «К», при МВД РФ, которое было создано в ответ на возникновение новых вызовов, связанных с технологическим прогрессом, и за время своего существования, укрепилось в системе органов государственной службы Российской Федерации в соответствии со своими целями и задачами: борьбы с преступлениями в информационной среде, пресечение нарушения авторских и смежных прав в киберпространстве, пресчение незаконного оборота технических средств и программного обеспечения, направленного на получение неправомерного доступа к информации, финансовым и государственным системам.

Кроме этого, автором отмечается роль и негосударственных организаций на территории Российской Федерации, занимающихся обеспечением информационной безопасности, примером которых является Лаборатория Касперского. Данная организация, помимо активной разработки средств защиты для индивидуальных и корпоративных клиентов, так же исследует вопросы развития и основных тенденции в иформационных правонарушениях. Данные исследования ложатся не только в основу для составления статистики, но и для составления отчетов крупных учреждений, как например Международный Союз Электросвязи при Организации Объединенных Наций, а так же могут являться источником для академического изучения тенденции, процессов развития и других аспектов кибербезопасности.

# ЗАКЛЮЧЕНИЕ.

Таким образом, исходя из изученного материала, можно сделать выводы о том, что феномен киберпреступлений, не является новым для современной науки, хотя, при этом, и требует дальнейшего изучения, особенно в вопросах точности и определении самого понятия. Была сделана попытка определения некоторых смежных понятий, таких как ИКТ, «киберпреступность», «кибербезопасность». Кроме этого автором диссертационного исследования был предложен собственный вариант определения киберпреступления, которое отмечает отличительную особенность данных правонарушений, а именно использование технических средств, в качестве инструментов совершения преступлений, одновременно с определением технических средств и информационных систем как объектов данных преступлений, а так же описывает причины и мотивы данных преступлений.

Так же отмечены основные характеристики, отличающие данный вид правонарушений от других уголовно-наказуемых деяний, а именно: большая вероятность сокрытия данных, сложности при проведении следствия, ввиду ограниченности информации, невозможности унификации национальных законодательств и подходов к следствию в данной области, сложности в процессе сбора данных, определения состава преступлении и др. Более того, автором отмечена тенденция к увеличению влияния такого аспекта, как трансграничность данных правонарушений.

Кроме этого, в первой главе отражается основная динамика и статистика за последние годы, и на основе изученных данных сделаны выводы об основных странах и отраслях общественно-экономических отношений подвергшихся за последние годы кибератакам. Среди основных стран пострадавших автором отмечаются страны Северной Америки в частности США, Канада, страны Европейского Союза, а так же Российская Федерация. Так же, автором сделано предположение о том, что данная география распространения напрямую связана с уровнем технологического развития государства, и интенсивности использования информационных систем в бизнес-структурах, общественных институтов, и личной жизни граждан, на территории перечисленных стран. Отмечен заметный переход, за последние периоды, от исключительно финансовых структур в сторону общественных и информационных структур, как целей киберпреступлений.

В ходе исследования так же был представлен ряд «громких» случаев киберпреступлений затрагивающих политические процессы в различных странах, в частности США, Иране, Германии, Российской Федерации, для подтверждения тезиса о том, что зачастую киберпреступления являются «политически мотивированными». Более того, автором исследования был предложен собственный вариант определения «политических киберпреступлений» на основе изученных данных и уже существующих смежных понятий. Таким образом, по мнению автора «политические киберпреступления» - это, совершаемые с помощью технических средств, связанных между собой интернетом и из политических побуждений, противоправные деяния, направленные на технические средства и информационные системы государственных органов и СМИ, с целью подрыва, ослабления или изменения существующего политического режима, государственных институтов или политических процессов.

Так же, на основе изученных и представленных материалов, следует сделать вывод о том, за последние годы преступность в информационной среде заметно усилила активность. Участились случаи совершения киберпреступлений по политическим мотивам и убеждениям, помимо привычных экономических мотивов. Согласно замечаниям исследователей, на сегодняшний день, множественные акторы активно выходят на мировую арену, принимая на себя передовые технологии, в том числе и киберпреступность. Заметно, так же стало и учащение случаев, когда совершение киберпреступлений по политическим соображениям, проводилось не отдельно взятыми правонарушителями, а в составе организованных групп, причем целями становились как Средства Массовой Информации, так и отдельные видные деятели политики, в частности президенты стран, общественные организации, военные и судебные ведомства различных стран. В рамках диссертационного исследования были представлены некоторые случаи совершения киберпреступлений в составе организованных групп ( Amonimous,FancyBearz, LulzSec, Syrian Electronic Army, Анонимный интернационал), получившие наиболее широкую огласку в связи с масштабностью и уроном нанесенным в ходе данных правонарушений. Данные преступления, по сути своей пытаются дескридитировать власть в глазах общественности, открыть какие-либо тайные факты, неизвестные страницы из различных политических процессов, для того, чтобы подорвать доверие граждан к государственности.

В особенности автор диссертационного исследования хочет отметить тот факт, что зачастую такие международные киберпреступные группировки обвиняются в связях с государственными и военными структурами, что, с учетом особенностей данных видов преступлений (таких как сложность расследования, сбора доказательств и стремления к трансграничности), делает их, с высокой вероятностью, инструментом удобным для ведения «теневой» нелегальной политики со стороны одного государства против другого.

Кроме этого во второй главе были рассмотрены основополагающие документы и положения Европейского Союза, Организации Объединенных Наций и Стран СНГ, касающихся и очерчивающих направления противодействия киберпреступности. Более того, были рассмотрены некоторые виды исследований, проведенных, в том числе и ООН и специализированными учреждениями при данной организации, которые изучают основные методы и способы борьбы различных стран и региональных объединений против киберпреступности. Автором диссертационного исследования, в результате изучения данных отчетов, делается вывод о том, что опыт международной борьбы с киберпреступности хоть и является обширным, тем не менее, согласно статистике, не достаточным для того, чтобы успевать за развитием методов и способов ведения киберпреступлений. Роль ООН в данном вопросе остается координирующей и очерчивающей общие рамки, тогда как основная работа и реальные примеры взаимодействия все же проявляются на региональных уровнях, примером тому является обширное подписание и исполнение Конвенции Совета Европы от 2001 года, в которой РФ не участвует с 2008 года. В исследовании сделанном Международным Союзом Связи отмечается так же, что Содружество Независимых государств, которые в свое время приняли похожие соглашения, так же являются примером активной борбы с киберпреступностью на региональном уровне. То же касается и Российской Федерации, которая отмечается исследователями из МСЭ, как один из лидирующих игроков в процессах противодействии киберпреступности, в соответсвии с Глобальной Программой по Кибербезопасности от 2007 года.

Однако, не умаляя, положительной динамики развития данной сферы, хочется отметить так же и ряд негативных тенденций, затрудняющих скорое развитие и всеобъемлющий подход к вопросам борьбы с киберпреступностью на международном уровне:

- ускоряющаяся тенденция к фрагментации международных подходов в рамках отдельно взятых региональных объединений, которые принимают и реализуют собственные специфические подходы к данной проблеме;

- противоречия между национальными государствами по вопросам основных законодательных инициатив и принципов многостороннего сотрудничества, которые, как например, в случае с отказом РФ от подписания Конвенции Совета Европы от 2001 года, могут поставить под удар национальных суверенитет страны;

- наличие правового отставания от процессов развития информационных технологий, когда, юридические нормы не успевают урегулировать поведение с использованием конкретных технологий, а в ближайшем времени появляются уже другие, поведение в которых так же требует регулировки.

Между тем, государства и международное сообщество активно стремится к преодолению противоречий и проблем, возникающих в процессе борьбы с киберпреступностью, используя при этом инструменты и учреждения ООН, Европейского Союза, Содружества Независимых Государств, Африканских и Арабских объединений, создающих и улучшающих универсальные, национальные и региональные нормы в данной сфере.

Исходя из материалов и документов национального уровня, исследованных в третьей части, автор диссертационного исследования делает вывод о том, что Российская Федерация имеет ряд всеобъемлющих документов, касающихся обеспечения развития информационного общества, противодействия угрозам на данном этапе развития, в том числе и киберпреступности, ряд документов освещенных в ходе диссертационного исследования содержат как основные приоритеты Российской Федерации. Среди отмеченных приоритетов были выделены: обеспечение прав и свобод граждан в условиях информационного общества, необходимость создания стабильного и безопасного доступа к информационным технологиям, противодействие преступлениям, совершаемым в информационной среде, а так же с применением высоких технологий.

Тем не менее, принятые документы, так же, отражают и новые угрозы, исходящие от киберпреступности. Среди данных угроз отмечается: уязвимость критически важной экономической, государственной и общественной инфраструктур, стремление к усилению международной активности экстремистких, террористических и преступных группировок, активно использующих информационные технологии в своих целях, а так же угроза информационных войн, с участием сторонних государств.

Так же было отмечено стремление законодательства Российской Федерации не к принятию новых уголовно-процессуальных норм, по противодействию киберпреступлениям, а определение составов преступлений в соответствии с уже существующими статьями в Уголовном и других кодексах России.

В ходе диссертационного исследования, кроме документов очерчивающих основные направления борьбы с преступлениями в информационном пространстве, были изучены органы в составе государственных институтов, курирующие вопросы противодействия киберпреступлениям.

Особо отмечена роль, Управления «К», при МВД РФ, которое было создано в ответ на возникновение новых вызовов, связанных с технологическим прогрессом, и за время своего существования, укрепилось в системе органов государственной службы Российской Федерации в соответствии со своими целями и задачами: борьбы с преступлениями в информационной среде, пресечение нарушения авторских и смежных прав в киберпространстве, пресчение незаконного оборота технических средств и программного обеспечения, направленного на получение неправомерного доступа к информации, финансовым и государственным системам.

Кроме этого, автором отмечается роль и негосударственных организаций на территории Российской Федерации, занимающихся обеспечением информационной безопасности, примером которых является Лаборатория Касперского. Данная организация, помимо активной разработки средств защиты для индивидуальных и корпоративных клиентов, так же исследует вопросы развития и основных тенденции в иформационных правонарушениях. Данные исследования ложатся не только в основу для составления статистики, но и для составления отчетов крупных учреждений, как например Международный Союз Электросвязи при Организации Объединенных Наций, а так же могут являться источником для академического изучения тенденции, процессов развития и других аспектов кибербезопасности.

Выводы сделанные в ходе диссертационного исследования, предположительно, могут быть использованы:

- при дальнейшем научном и практическом исследовании международных, а так же юридических аспектов киберпреступности, для совершенствования мер противодействия данным видам правонарушения в рамках существующих законодательных и декларативных норм;

- в виду, отмеченной автором тенденции, к отставанию развития законодательных инициатив по регулировке информацинного обмена от скорости информационного развития, при разработке новых национальных и международных норм, по противодействию киберпреступлениям.

На данном этапе, автор диссертационного исследования считает, цели и задачи, поставленные перед исследованием достигнутыми, однако, поскольку данный вопрос только начинает свое активное развитие в практической и академической среде, необходимо и, так же, планируется дальнейшее исследование данного вопроса, в рамках других форматов научного исследования.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники

1. Bissel K., LaSalle R.M., Richards K., «The Assenture Security Index»/ REDEFINING SECURITY PERFORMANCE AND HOW TO ACHIEVE IT 2017. – 16p;
2. Cyber Security Intelligence Index 2016 // IBM Security. - URL: [http://www-01.ibm.com/common/ssi/cgi-](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&amp;infotype=SA&amp;htmlfid=SEW03133USEN&amp;attachment=SEW03133USEN.PDF) [bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&amp;infotype=SA&amp;htmlfid=SEW03133USEN&amp;attachment=SEW03133USEN.PDF) (дата обращения 24.03.2018);
3. Global Cybersecurity Index 2017// International Telecommunication Union . - Geneva, 2017 –65 p;
4. Global Threat Intelligence Report 2016 // NTT Group. URL <https://www.nttsecurity.com/en-us/gtic-2016-q4-threat-intelligence-report> (дата обращения 25.03.2018)
5. IBM X-Force Threat Intelligence Index 2018 // IBM Security © Copyright IBM Corporation 2018. – New York, USA. March, 2018. -43p.
6. INDEX OF CYBERSECURITY INDICES 2017 // International Telecommunication Union 2017 . Geneva, 2017 17p
7. Kaspersky Security Bulletin 2015// Kaspersky Security Lab. URL: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09065518/KSB_2015_business_threats_ru.pdf> (дата обращения 25.03.2018);
8. KASPERSKY SECURITY BULLETIN: 2017. РАЗВИТИЕ УГРОЗ // Лаборатория касперского 2017/ URL: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09043350/KSB_Review-of-2017_final_RU.pdf> (дата обращения 15.05.2018);
9. Norton Cyber Security Insights Report 2017 Global Results // Norton by Symantec 2018 URL: <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf> (дата обращения: 17.03.2018);
10. World Internet Users and 2018 Population Stats// Internet World Stats / 31.12.2017 URL: <https://www.internetworldstats.com/stats.htm> (дата обращения: 18.03.2018);
11. Доктрина информационной безопасности Российской Федерации // Утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646/ “Об утверждении Доктрины информационной безопасности Российской Федерации” Иформационно-правовой портал Гарант.ру URL: <http://www.garant.ru/products/ipo/prime/doc/71456224/> (дата обращения: 08.05.2018);
12. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 г. URL: <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081580> (дата обращения 25.04.2018) ;
13. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года// Официальный сайт МВД Республики Беларусь URL. <http://mvd.gov.by/main.aspx?guid=4603> (дата обращения 20.03.2018);
14. Конвенция об обеспечении международной информационной безопасности (концепция) от 22.09.2011г// Сайт МИД РФ/ URL: <http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666> (дата обращения: 12.05.2018);
15. Конвенция Организации Объединенных Наций против транснациональной организованной преступности // Принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года/ Официальный сайт Организации Объединенных Наций URL: <http://www.un.org/ru/documents/decl_conv/conventions/orgcrime> статьи 27,28,29 (дата обращения 25.04.2018);
16. Концепция внешней политики Российской Федерации // Утверждена Президентом Российской Федерации В.В.Путиным 30 ноября 2016 г./ Официальный сайт Министерства Иностранных Дел РФ URL: <http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248> (дата обращения: 10.05.2018);
17. Концепция сотрудничества государств – участников Содружества Независимых Государств, в борьбе с преступлениями, совершаемыми с использованием информационных технологий от 25 октября 2013 года.// Интернет – портал «О СНГ» URL: <http://www.e-cis.info/page.php?id=23808> (дата обращения: 26.04.2018);
18. Распоряжение Правительства РФ [Об усилении борьбы с преступлениями в сфере высоких технологий] от 22 октября 1999 года N 1701-р // Электронный Фонд Правовой и Нормативно –Технической Документации «Консорциум кодекс» URL: <http://docs.cntd.ru/document/901745530> (дата обращения: 12.05.2018);
19. Распоряжение Президента РФ№ 144-рп - О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. N 557-рп «О подписании Конвенции о киберпреступности»22.03.2008. URL: <http://www.kremlin.ru/acts/bank/27059> (дата обращения: 26.04.2018);
20. Резолюция принятая Генеральной Ассамблеей ООН // Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию/ A/RES/65/230 1.04.2011. URL: <http://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf> (дата обращения 27.04.2018);
21. Связь 2017 – Оперативная информация //Деятельность в сфере телекоммуникации (по данным Минкомсвязи России) / Официальный сайт Федеральной службы государственной статистики РФ URL: [http://www.gks.ru/wps/wcm/connect/rosstat\_main/rosstat/ru/statistics/science\_and\_innovations/it\_technology/#](http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/) (дата обращения: 08.05.2018);
22. Соглашение «о сотрудничестве государств – участников Содружества Независимых Государств, в борьбе с преступлениями в сфере компьютерной информации» Минск. 2001 год.// Официальный сайт Исполнительного Комитета СНГ. URL: <http://www.cis.minsk.by/page.php?id=866> (дата обращения: 26.04.2018);
23. Стратегия национальной безопасности Российской Федерации// Утвержденная указом Президента РФ № 683 от 31декабря 2015 года/ Иформационно-правовой портал Гарант.ру URL: <http://base.garant.ru/71296054/#friends> (дата обращения: 10.05.2018);
24. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы// Утвержденная Указом Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы”/ Иформационно-правовой портал Гарант.ру URL: <http://www.garant.ru/products/ipo/prime/doc/71570570/> (дата обращения: 08.05.2018);
25. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 23.04.2018, с изм. от 25.04.2018)// Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ/ Официальный сайт компании «КонсультантПлюс» URL: <http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/> (дата обращения: 10.05.2018);
26. ДОХИНСКАЯ ДЕКЛАРАЦИЯ от 12-19 апреля 2015 года.// Тринадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию / УНП ООН. Нью-Йорк .2015 год., - 26 с.;
27. Указ Президента Российской Федерации от 31.12.2015 г. № 683 «О стратегии национальной безопасности»/ URL: <http://www.kremlin.ru/acts/bank/40391> (дата обращения: 12.05.2018);
28. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.07.2016) "Об информации, информационных технологиях и о защите информации"// Официальный сайт компании «КонсультантПлюс» URL <http://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/> (дата обращения: 18.03.2018);
29. Окинавская хартия Глобального информационного общества 21 июля 2000 года// Официальный сайт Президента РФ / URL: <http://www.kremlin.ru/supplement/3170> (дата обращения 25.04.2018);
30. Отчет «Global Cybersecurity Index (GCI) 2017» // Официальный сайт Международного Союза Электросвязи URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI-17Report.pdf> (дата обращения: 20.03.2018);

Литература

1. Brown C., Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice// International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015.- 65p;
2. Collin B., The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge// Crime Research URL: <http://www.crime-research.org/library/Cyberter.htm> (дата обращения: 24.04.2018);
3. Definition of Cybersecurity Gaps and overlaps in standardisation// European Union Agency For Network And Information Security V1.0 DECEMBER 2015. Heraklion, Greece. – 35p;
4. Denning D.E., Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy// Information Warfare Site URL: <http://www.iwar.org.uk/cyberterror/resources/denning.htm> (дата обращения: 23.04.2018);
5. Dennis M.A., Defenition of «Cybercrime»// Encyclopædia Britannica 09.03.2018 Encyclopædia Britannica, inc. URL: <https://www.britannica.com/topic/cybercrime> (дата обращения: 20.03.2018);
6. Lewis J.A., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats//Center for Strategic and International Studies, December 2002. - 12p;
7. Marc D. Goodman AND Susan W. Brenner «THE EMERGING CONSENSUS ON CRIMINAL CONDUCT IN CYBERSPACE» // Archive.org URL: <https://archive.org/details/TheEmergingConsensusOnCriminalConductInCyberspace> (дата обращения: 23.04.2018);
8. Schjølberg S., ITU Global Cybersecurity Agenda (GCA) // REPORT OF THE CHAIRMAN OF HLEG URL: <https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf> (дата обращения: 26.04.2018);
9. Shinder D.L., Tittel E. Scene of the Cybercrime: Computer Forensics Handbook // BookReader URL: <http://bookre.org/reader?file=495251> (дата обращения: 24.04.2018);
10. Williams P., Organized Crime and Cybercrime: Synergies, Trends, and Responses// Crime Research URL: <http://www.crime-research.org/library/Cybercrime.htm> (дата обращения: 23.04.2018);
11. Багдеева В. А. Проблемы международной киберпреступности // Актуальные проблемы российского права. – 2009. – № 3(12). – С. 564-572.;
12. Болгов Р. В., Сообщества пользователей интернет-проектов // Вестник МГИМО. 2013. №1 (28). URL: <https://cyberleninka.ru/article/n/soobschestva-polzovateley-internet-proektov> , (дата обращения: 15.04.2018);
13. Бондарь В.В., Киберпреступность – современное состояние и пути борьбы // Юридические записки. 2013. №2. <URL:https://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby> (дата обращения: 22.03.2018);
14. Валько Д.В., Киберпреступность в России и мире: Сравнительный анализ Управление в Социально- Политических и Правовых системах, №3(10) 2016 С.29-40;
15. Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности. Проект, февраль 2013. ООН -Вена , 2013. – 360 с;
16. Дмитрик Н., Обзор законодательства Российской Федерации в сфере информационной безопасности – Часть 1: Общий обзор // Digital.Report Инфобезопасность. Статья от 04.12.2016 URL: <https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/> (дата обращения: 10.05.2018);
17. Дмитрик Н., Обзор законодательства Российской Федерации в сфере информационной безопасности – Часть 9: Борьба с киберпреступностью // Digital.Report Инфобезопасность. Статья от 04.12.2016 URL: <https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/> (дата обращения: 10.05.2018);
18. Журавленко Н. И., Шведова Л.Е., Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. №3 (53). URL: https://cyberleninka.ru/article/n/problemy-borby-s-kiberprestupnostyu-i-perspektivnye-napravleniya-mezhdunarodnogo-sotrudnichestva-v-etoy-sfere (дата обращения: 23.04.2018);
19. Каберник В. В., Проблемы классификации кибероружия // Вестник МГИМО. 2013. №2 (29). URL: https://cyberleninka.ru/article/n/problemy-klassifikatsii-kiberoruzhiya (дата обращения: 23.04.2018);
20. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. - 2014. - №8. – С. 46-50;
21. Киберпреступность и отмывание денег // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма./ Проект типологического исследования ЕАГ URL:<https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014.pdf> (дата обращения: 20.03.2018);
22. Когаловский М. Р. и др. Глоссарий по информационному обществу / Под общ. ред. Ю. Е. Хохлова. — М.: Институт развития информационного общества, 2009. — 160 с.
23. Краковский К. П. Государственные и политические преступления (к вопросу о понятиях) // Северо-Кавказский юридический вестник. 2009. №1. URL: <https://cyberleninka.ru/article/n/gosudarstvennye-i-politicheskie-prestupleniya-k-voprosu-o-ponyatiyah> (дата обращения: 27.03.2018);
24. Научное сообщество студентов. «Междисциплинарные исследования»: Электронный сборник статей по материалам ХII студенческой международной научно- практической конференции. – Новосибирск: Изд. АНС «СибАК». – 2017. – № 1 (12)/ URL: <http://www.sibac.info/archive/science/1(12).pdf>.(дата обращения: 26.03.2018);
25. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях М.: Норма, 2004.- - С.432;
26. Политические преступления// Большой юридический словарь. — М.: Инфра-М. А. Я. Сухарев, В. Е. Крутских, А.Я. Сухарева. 2003. URL: <http://www.e-reading.club/bookreader.php/135201/Bol%27shoii_yuridicheskiii_slovar%27.pdf> (дата обращения: 26.03.2018);
27. Талипова Л. Р., Международно-правовая регламентация киберпреступности // Гуманитарные, социально-экономические и общественные науки. 2016. №4. URL: <https://cyberleninka.ru/article/n/mezhdunarodno-pravovaya-reglamentatsiya-kiberprestupnosti> (дата обращения: 26.04.2018);
28. Тропина, Т. Л. (Татьяна Львовна). Киберпреступность :Понятие, состояние, уголовно-правовыемеры борьбы// Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08- Уголовное право и криминология ; Уголовно-исполнительное право /Т. Л. Тропина ; Науч. рук. В. А. Номоконов. Владивосток, 2005. -26 с;
29. Чугунов А.В. Ч-83 Развитие информационного общества: теории, концепции и программы: Учебное пособие. — СПб.: Ф-т филологии и ис- кусств СПбГУ, 2007. —98с;
30. Шарапова М. И. ИКТ в образовании // Вестник МГЛУ. 2011. №620. URL: https://cyberleninka.ru/article/n/ikt-v-obrazovanii (дата обращения: 18.03.2018);
31. Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. — 2016. — №28. — С. 720-723. — URL https://moluch.ru/archive/132/37021/ (дата обращения: 26.04.2018);
32. Эмм Д., Унучек Р., Kaspersky Security Bulletin: обзор 2017 года// Kaspersky security bulletin 2017 / URL: <https://securelist.ru/ksb-review-of-the-year-2017/88142/> (дата обращения 15.05.2018);
33. Якимова Е. М., Нарутто С. В., Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. №2. с 374 URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu (дата обращения: 26.04.2018);

Ресурсы

1. Anonymous - The TRUTH about Donald Trump// Anonimous Official YouTube Channel 28.01.2017 <https://www.youtube.com/watch?v=rM-WpZ0ZO4Y> (дата обращения: 18.04.2018).
2. Anonymous взломали более 5 тысяч аккаунтов "Исламского государства"//РИА Новости «В мире» 17.11.2015 URL: <https://ria.ru/world/20151117/1322879329.html> (дата обращения: 18.04.2018);
3. Miles T., U.N. survey finds cybersecurity gaps everywhere except Singapore // Reuters “Cyber Risk” 05.07.2017 URL: <https://www.reuters.com/article/us-cyber-un/u-n-survey-finds-cybersecurity-gaps-everywhere-except-singapore-idUSKBN19Q19L> (дата обращения: 27.04.2018);
4. Анонимные хакеры взломали сервер консультантов Пентагона// Русская Служба BBC 12.06.2011 URL: <https://www.bbc.com/russian/international/2011/07/110712_new_anonymous_attack> (дата обращения: 18.04.2018);
5. Аудитория пользователей интернета в России в 2017 году составила 87 млн. человек // Новости Российского Интернет Форума / Февраль - 2017 URL: <http://2017.russianinternetforum.ru/news/1298/> (дата обращения: 08.05.2018);
6. Ващенко В., «Шалтай» получил двушечку //Газета.ru 06.07.2017, - URL: <https://www.gazeta.ru/social/2017/07/06/10775462.shtml> (дата обращения: 15.04.2018 );
7. Волуйская М., Крупнейшие хакерские группировки мира. Инфографика// Аргументы и Факты 11.03.2017 URL: <http://www.aif.ru/dontknows/infographics/krupneyshie_hakerskie_gruppirovki_mira_infografika> (дата обращения: 18.04.2018);
8. Егоров И. Киберпрокурор. Юрий Чайка рассказал о борьбе с интернет-преступностью// Российская Газета Федеральный выпуск №7356 (190) 24.08.2017/ URL: <https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html> (дата обращения: 14.03.2018);
9. Ершов А., К 2018 году потери РФ от киберпреступлений превысят 2 трлн рублей// Российская Газета официальный сайт / Рубрика «Экономика от 01.10.2016 г. URL: <https://rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html> (дата обращения 24.03.2018)
10. Зайцев В., Самые известные кибератаки. Как хакеры угрожают миру // Газета Коммерсант 29.06.2017. URL: <https://www.kommersant.ru/doc/3338435#id=4> (дата обращения: 25.03.2018);
11. Иванов К., Группа Fancy Bears взломала почту Ричарда Макларена и других спортивных чиновников// 10.01.2016 URL: <https://www.spb.kp.ru/daily/26780.4/3813416/> (дата обращения: 16.04.2018);
12. Интернет-пропаганда – одна из главных киберугроз 2017 года// Digital Report Инфобезопасность 19.12.2016 URL: <https://digital.report/internet-propaganda-odna-iz-glavnyih-kiberugroz-2017-goda/> (дата обращения: 26.03.2018);
13. Кибератаки на правительственные сети связи в Германии продолжаются// Русская Служба BBC 01.03.2018 URL: <https://www.bbc.com/russian/news-43247681> (дата обращения: 16.04.2018);
14. Лаборатория Касперского» опубликовала подробности хакерской атаки на ядерный проект Ирана// RT 13.11.2014URL: <https://russian.rt.com/article/59295> (дата обращения: 25.03.2018);
15. Меркачева Е., Шалтай-Болтай сел на измену// "Московский комсомолец" №27312 от 31.01. 2017 URL: <http://www.mk.ru/social/2017/01/30/khakerskie-tayny-shaltayboltaya-kto-publikoval-vzlomannuyu-pochtu-vipov.html> (дата обращения: 15.04.2018);
16. Николаев А. Вирус Wanna Cry заразил десятки тысяч компьютеров по всему миру// Официальный сайт Новости Первого Канала – репортаж от 13.05.2017 URL: <https://www.1tv.ru/news/2017-05-13/325201-virus_wanna_cry_zarazil_desyatki_tysyach_kompyuterov_po_vsemu_miru> (дата обращения: 24.12.2017);
17. О Международном союзе электросвязи (МСЭ)// Официальный сайт МСЭ URL: <https://www.itu.int/ru/about/Pages/default.aspx> (дата обращения: 26.04.2018);
18. ООО «ГикБрейнс» // Самые громкие кибератаки 21 века 15.06.2016 URL: <https://geekbrains.ru/posts/hackers_attacks_xxi> (дата обращения: 24.03.2018);
19. Перекалин A., Bad Rabbit: новая эпидемия шифровальщика// Блог Лаборатории Касперского, статья от 24.10.2017 URL: <https://www.kaspersky.ru/blog/bad-rabbit-ransomware/19072/> (дата обращения: 24.12.2017);
20. Покончил с собой Аарон Шварц // Коммерсант.ру 20.12.2013 URL: <https://www.kommersant.ru/doc/2360699> (дата обращения: 18.04.2018);
21. Ромашенко С., Der Spiegel: Хакеры атаковали бундестаг по поручению властей РФ. // Deutsche Welle 30.01.2016 URL: <http://p.dw.com/p/1Hm92> (дата обращения: 26.03.2018);
22. Российские СМИ атаковал вирус-шифровальщик Bad Rabbit// Русская Служба BBC. 24.10.2017 URL: <https://www.bbc.com/russian/news-41739756> (дата обращения: 24.12.2017);
23. Самые известные хакеры и их атаки // Официальный сайт Исторического журнала «Дилетант» 19.09.2015 URL: <http://diletant.media/articles/26011961/> (дата обращения: 18.04.2018);
24. Сирийская электронная армия" взломала сайт морпехов США // РИА Новости «Сирия» 02.09.2013 URL: <https://ria.ru/arab_sy/20130902/960209048.html> (дата обращения: 16.04.2018);
25. Слободян Е., Что представляет собой группировка хакеров Fancy Bears? // Аргументы и Факты 14.09.2016 <URL:http://www.aif.ru/dontknows/file/chto_predstavlyaet_soboy_gruppirovka_hakerov_fancy_bears> (дата обращения: 16.04.2018);
26. Совет Европы принял конвенцию по киберпреступности // Коммерсант.ру 09.11.2001 URL: <https://www.kommersant.ru/doc/926130> (дата обращения 25.04.2018);
27. Управление «К» МВД России // История подразделения/ Официальный сайт Министерства Внутренних Дел Российской Федерации URl: <https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii> (дата обращения: 10.05.2018);
28. Управление «К» МВД России // Официальный сайт Министерства Внутренних Дел Российской Федерации URl: <https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii> (дата обращения: 10.05.2018);
29. Хакеры "Сирийской электронной армии" взломали сайты мировых СМИ // РИА Новости – «Технологии» 27.11.2014 <URL:https://ria.ru/technology/20141127/1035484262.html> (дата обращения: 16.04.2018);
30. Хакеры Anonymous утверждают, что взломали сотни сайтов в Китае// Украинская Служба BBC 06.04.2012 <URL:https://www.bbc.com/ukrainian/ukraine_in_russian/2012/04/120405_ru_s_anonymous_attack> (дата обращения: 18.04.2018);
31. Хакеры LulzSec взломали сайт знакомств американских военнослужащих// Вести.ру – В мире , 28.03.2012 URL: <http://www.vesti.ru/doc.html?id=754172> (дата обращения: 16.04.2018);
32. Хакеры группы Anonymous присоединяются к иранским протестам // ИноПресса 15.02.2011. URL: <https://www.inopressa.ru/article/15Feb2011/times/anonym.html> (дата обращения: 15.04.2018);
33. Хакеры обокрали россиян на 2 миллиарда долларов // Вести.ру 14.09.2012 URL <http://www.vesti.ru/doc.html?id=907003&cid=780> (дата обращения: 14.03.2018).
34. Шадрин И., Хакерская группа LulzSec вызвалась отомстить за взлом серверов Sega// РИА Новости «Наука» Москва . 20.06.2011 URL: <https://ria.ru/science/20110620/390610091.html> (дата обращения: 16.04.2018).

# ПРИЛОЖЕНИЕ 1

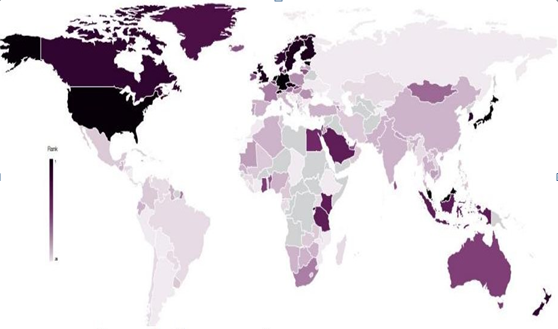


Рисунок – Страны подверженные киберугрозам, по данным IBM на 2016 год.

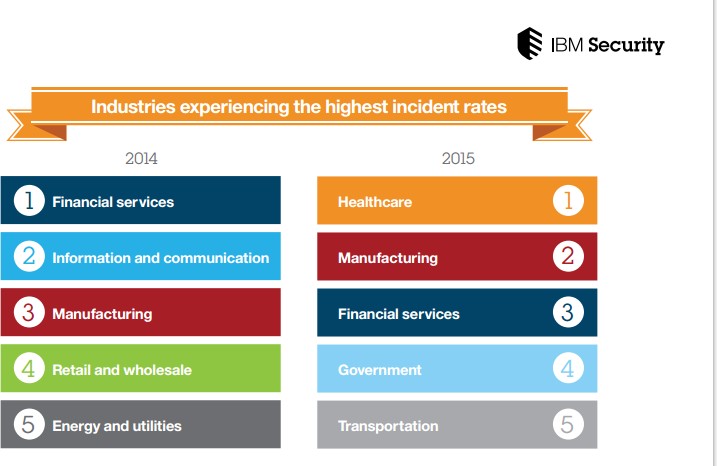


Рисунок 2 – Основные отрасли, подвергшиеся кибератакам в 2014 и 2015 годах.

# ПРИЛОЖЕНИЕ 2

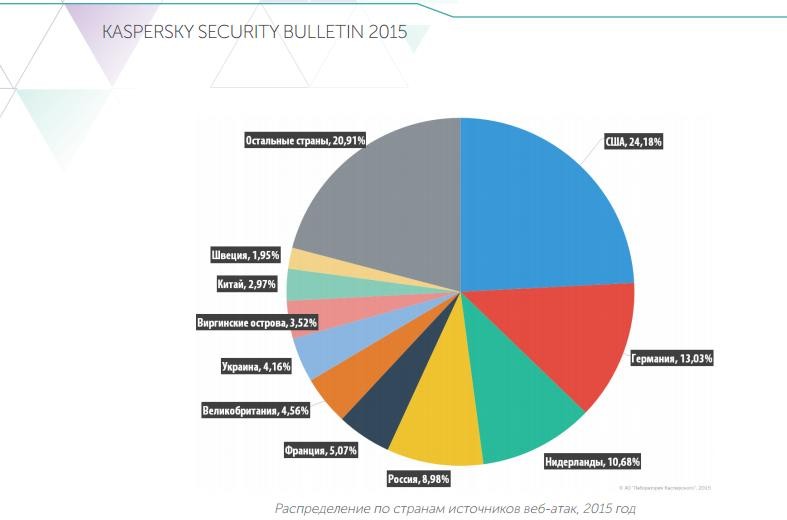


Рисунок 3 – Распределение по странам – источникам веб-атак на 2015 год.

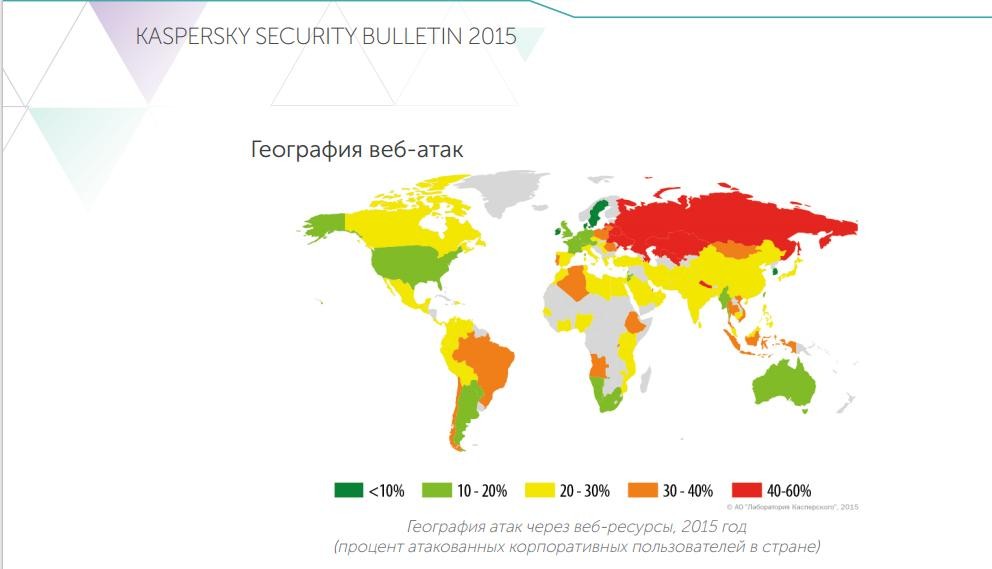


Рисунок 4 – География атак через веб-ресурсы за 2015 год.

# ПРИЛОЖЕНИЕ 3.

Рисунок 5 – Количество уникальных корпоративных пользоватаелей атакованных в 2014 и 2015 годах.

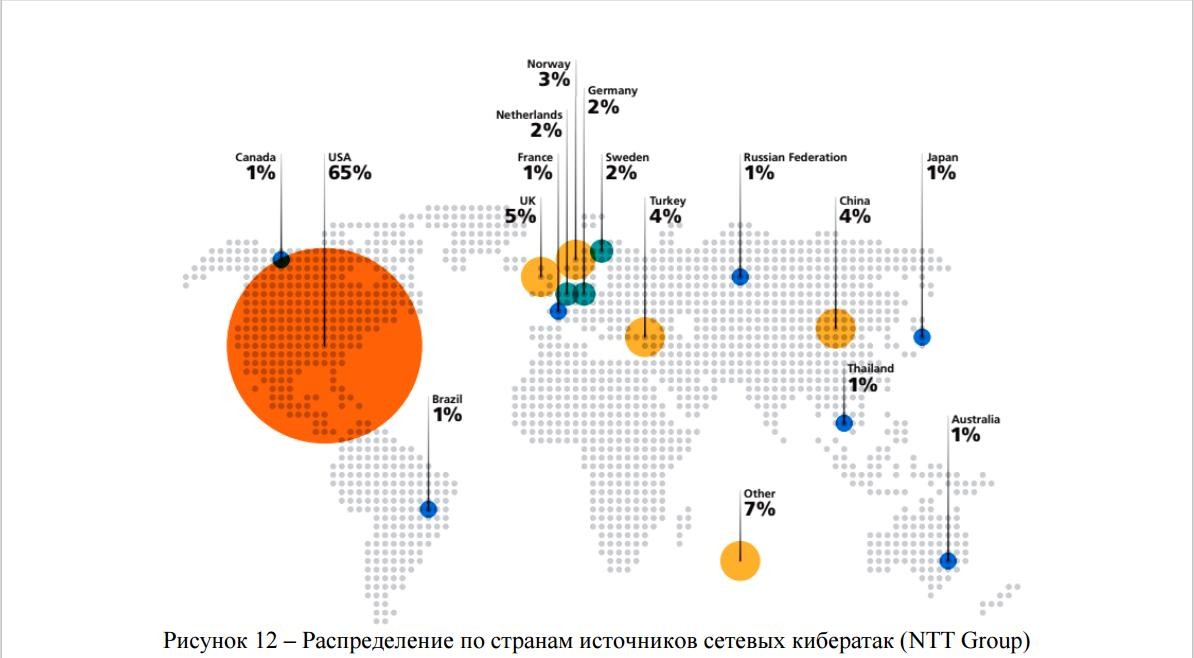


Рисунок 6 – Распеделение стран источников сетевых кибератак. По данным NTT Group.

ПРИЛОЖЕНИЕ 4

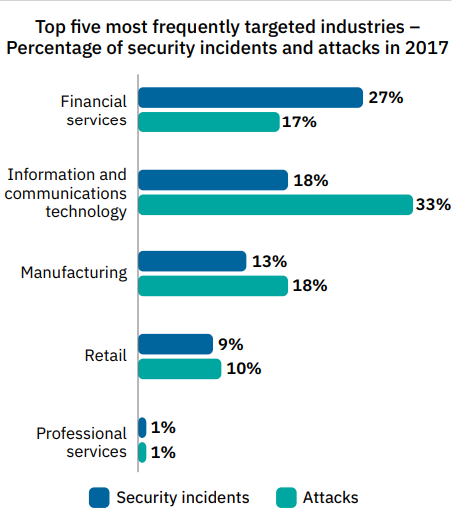


Рисунок 7 – Лист пяти отраслей, наиболее часто испытывавших атаки на протяжении 2017 года.

# ПРИЛОЖЕНИЕ 5

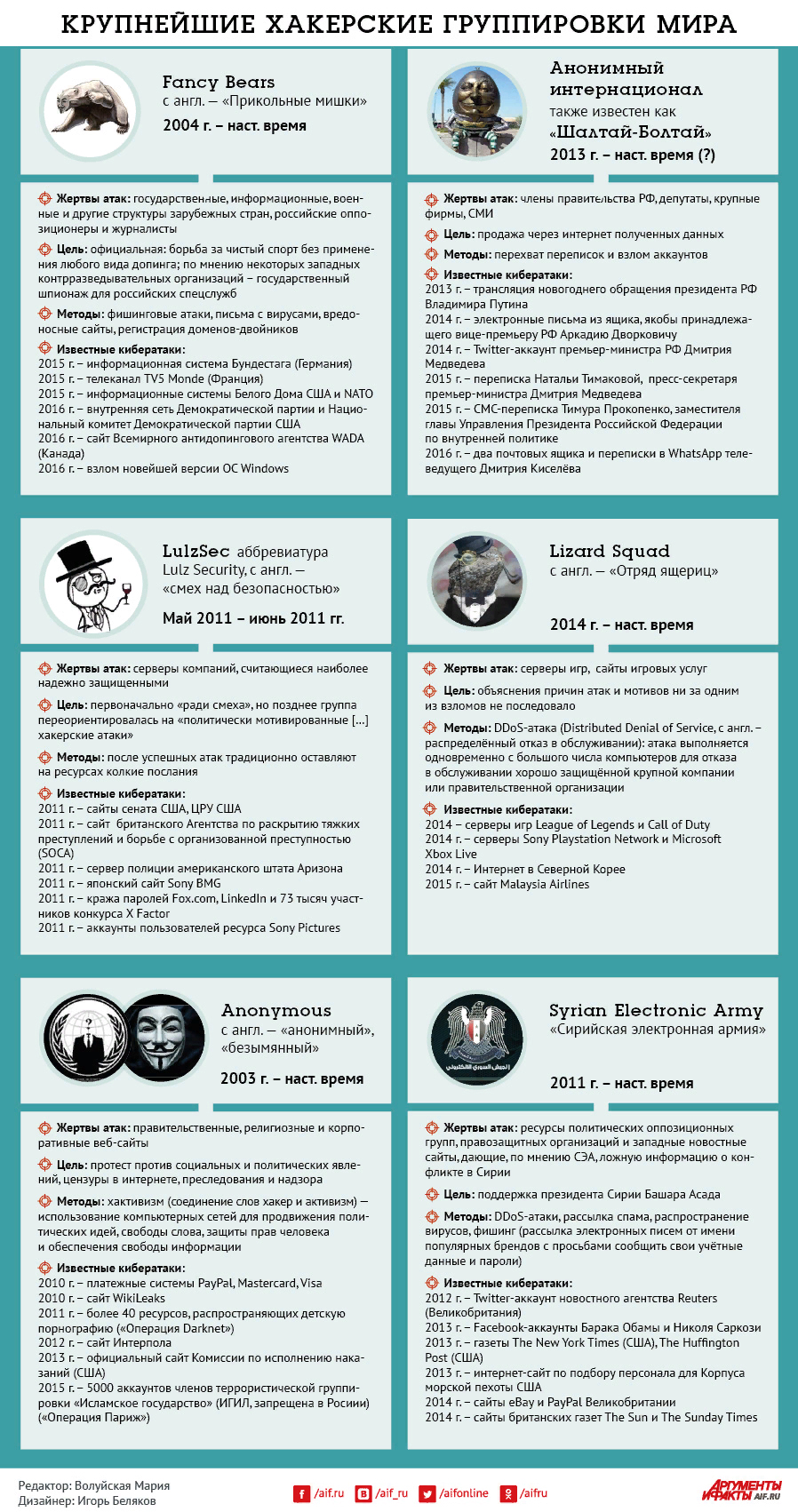


Рисунок 8 – Крупнейшие хакерские группировки мира. АиФ от 11.03.2017

# ПРИЛОЖЕНИЕ 6

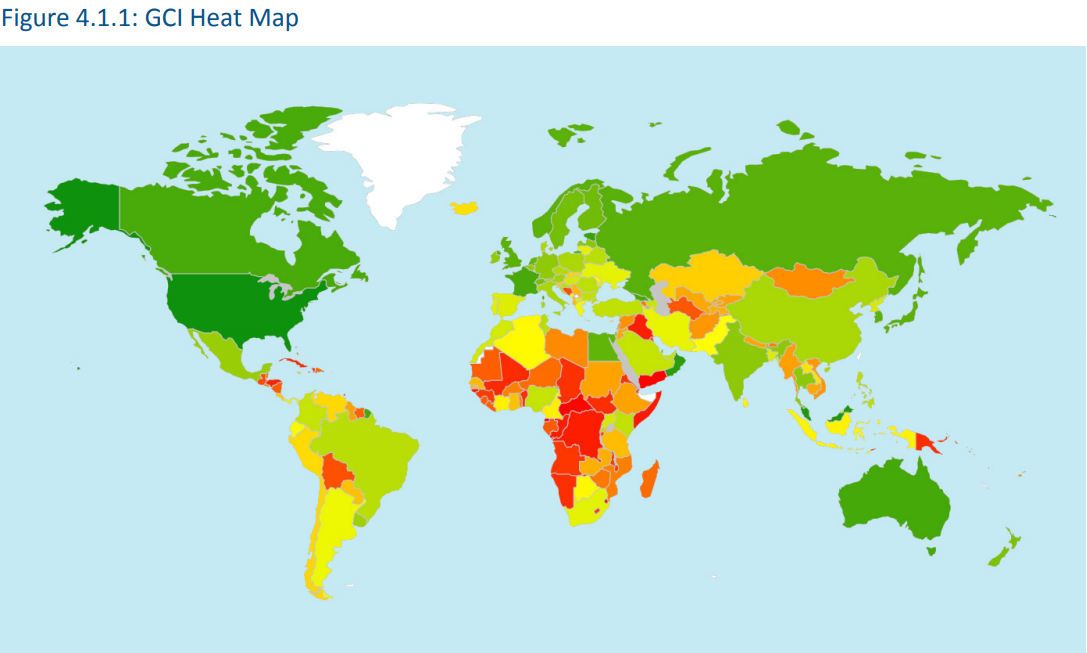


Рисунок 9 – Сводная карта по Глобальному Индексу Кибербезопасности на 2017 год.

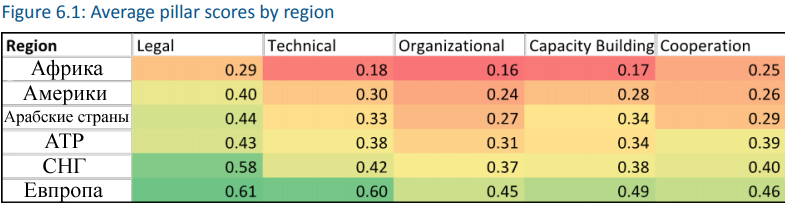


Рисунок 10 – Сводная таблица по регионам по Глобальному Индексу Кибербезопасности на 2017 год.[[147]](#footnote-147)\*

# ПРИЛОЖЕНИЕ 7

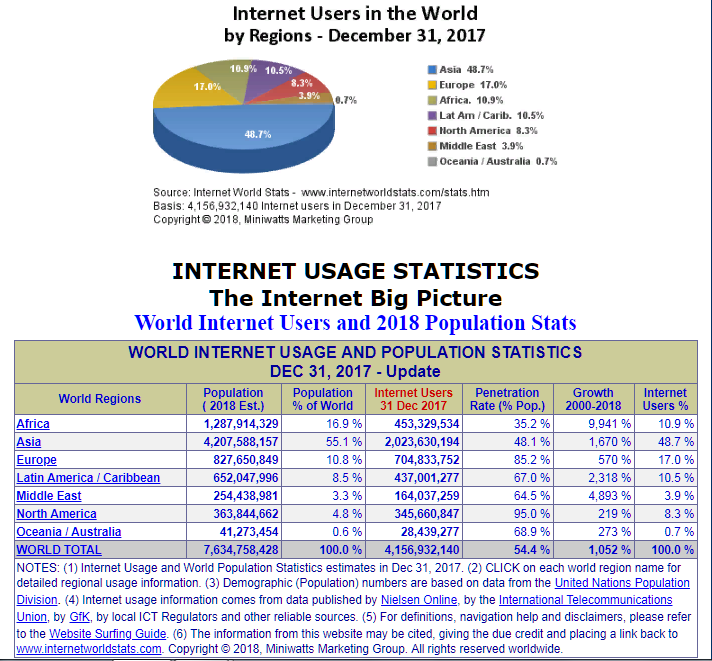


Рисунок - Статистика использования интернет на 31 декабря 2017 года.

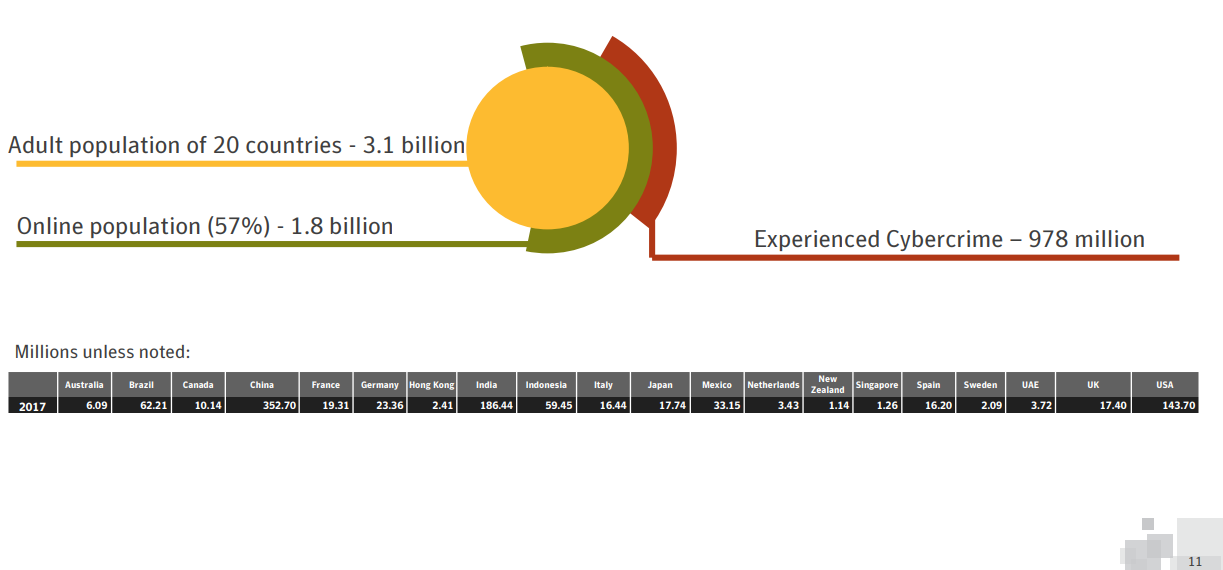


Рисунок – Статистические данные по жертвам киберпреступленний. Norton 2017.

# ПРИЛОЖЕНИЕ 8

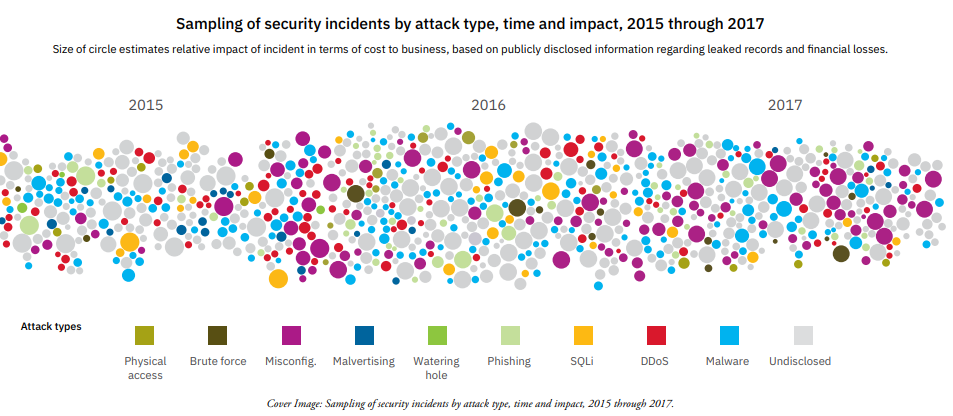


Рисунок – Динамика способов преступлений от 2015 до 2017 года, по данным IBM X-Force 2018

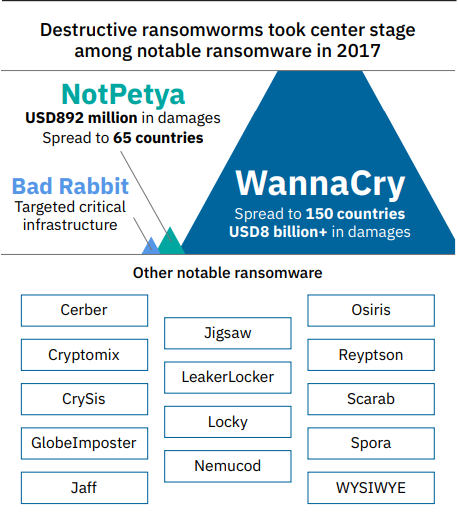


Рисунок - Вредоносное ПО, которое принесло наибольшие убытки за 2017 год. IBM X-Force.

1. World Internet Users and 2018 Population Stats// Internet World Stats 31.12.2017 URL: <https://www.internetworldstats.com/stats.htm> (дата обращения: 10.03.2018). [↑](#footnote-ref-1)
2. См. Приложение 7 рис.11. [↑](#footnote-ref-2)
3. Хакеры обокрали россиян на 2 миллиарда долларов // Вести.ру 14.09.2012 URL <http://www.vesti.ru/doc.html?id=907003&cid=780> (дата обращения: 14.03.2018). [↑](#footnote-ref-3)
4. Егоров И. Киберпрокурор. Юрий Чайка рассказал о борьбе с интернет-преступностью// Российская Газета Федеральный выпуск №7356 (190) 24.08.2017/ URL: <https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html> (дата обращения: 14.03.2018). [↑](#footnote-ref-4)
5. Norton Cyber Security Insights Report 2017 Global Results // Norton by Symantec 2018 URL: <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf> (дата обращения: 17.03.2018). [↑](#footnote-ref-5)
6. Егоров И. Киберпрокурор. Юрий Чайка рассказал о борьбе с интернет-преступностью// Российская Газета Федеральный выпуск №7356 (190) 24.08.2017/ URL: <https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html> (дата обращения: 18.03.2018). [↑](#footnote-ref-6)
7. Доктрина информационной безопасности Российской Федерации// Утверждена Президентом Российской Федерации от 9.09.2000. №1895 ( утратила силу)/ Иформационно-правовой портал Гарант.ру URL: <http://base.garant.ru/182535/> (дата обращения: 18.03.2018); [↑](#footnote-ref-7)
8. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях М.: Норма, 2004.- - 432 c. [↑](#footnote-ref-8)
9. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО «Издательство «Юрлитинформ», 2001. – 496 с. [↑](#footnote-ref-9)
10. Булай. Ю. Г., Булай Р. И., Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. №1. URL: https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam (дата обращения: 15.04.2018). [↑](#footnote-ref-10)
11. Каберник В. В., Проблемы классификации кибероружия // Вестник МГИМО. 2013. №2 (29). URL: https://cyberleninka.ru/article/n/problemy-klassifikatsii-kiberoruzhiya (дата обращения: 23.04.2018). [↑](#footnote-ref-11)
12. Журавленко Н. И., Шведова Л.Е., Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. №3 (53). URL: https://cyberleninka.ru/article/n/problemy-borby-s-kiberprestupnostyu-i-perspektivnye-napravleniya-mezhdunarodnogo-sotrudnichestva-v-etoy-sfere (дата обращения: 23.04.2018). [↑](#footnote-ref-12)
13. Тропина, Т. Л. (Татьяна Львовна). Киберпреступность :Понятие, состояние, уголовно-правовыемеры борьбы// Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08- Уголовное право и криминология ; Уголовно-исполнительное право /Т. Л. Тропина ; Науч. рук. В. А. Номоконов. Владивосток,2005. -26 с [↑](#footnote-ref-13)
14. Marc D. Goodman AND Susan W. Brenner «THE EMERGING CONSENSUS ON CRIMINAL CONDUCT IN CYBERSPACE» // Archive.org URL: <https://archive.org/details/TheEmergingConsensusOnCriminalConductInCyberspace> (дата обращения: 23.04.2018); [↑](#footnote-ref-14)
15. Williams P., Organized Crime and Cybercrime: Synergies, Trends, and Responses// Crime Research URL: <http://www.crime-research.org/library/Cybercrime.htm> (дата обращения: 23.04.2018); [↑](#footnote-ref-15)
16. Denning D.E., Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy// Information Warfare Site URL: <http://www.iwar.org.uk/cyberterror/resources/denning.htm> (дата обращения: 23.04.2018); [↑](#footnote-ref-16)
17. Lewis J.A., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats//Center for Strategic and International Studies, December 2002. - 12p [↑](#footnote-ref-17)
18. Collin B., The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge// Crime Research URL: <http://www.crime-research.org/library/Cyberter.htm> (дата обращения: 24.04.2018); [↑](#footnote-ref-18)
19. Brown C., Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice// International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015.- 65p [↑](#footnote-ref-19)
20. Shinder D.L., Tittel E. Scene of the Cybercrime: Computer Forensics Handbook // BookReader URL: <http://bookre.org/reader?file=495251> (дата обращения: 24.04.2018); [↑](#footnote-ref-20)
21. Norton Cyber Security Insights Report 2017 Global Results // Norton by Symantec 2018 / URL: <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf> [↑](#footnote-ref-21)
22. Cyber Security Intelligence Index 2016 // IBM Security. – 2016 URL: [http://www-01.ibm.com/common/ssi/cgi bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF](http://www-01.ibm.com/common/ssi/cgi%20bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF) (дата обращения 15.05.2018). [↑](#footnote-ref-22)
23. 1. Bissel K., LaSalle R.M., Richards K., «The Assenture Security Index»/ REDEFINING SECURITY PERFORMANCE AND HOW TO ACHIEVE IT 2017. – 16p; [↑](#footnote-ref-23)
24. KASPERSKY SECURITY BULLETIN: 2017. РАЗВИТИЕ УГРОЗ // Лаборатория касперского 2017/ URL: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09043350/KSB_Review-of-2017_final_RU.pdf> (дата обращения 15.05.2018). [↑](#footnote-ref-24)
25. Эмм Д., Унучек Р., Kaspersky Security Bulletin: обзор 2017 года// Kaspersky security bulletin 2017 / URL: <https://securelist.ru/ksb-review-of-the-year-2017/88142/> (дата обращения 15.05.2018). [↑](#footnote-ref-25)
26. Отчет «Global Cybersecurity Index (GCI) 2017» // Официальный сайт Международного Союза Электросвязи URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI-17Report.pdf (дата обращения: 20.03.2018); [↑](#footnote-ref-26)
27. Киберпреступность и отмывание денег // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма./ Проект типологического исследования ЕАГ URL:https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya\_kiber\_EAG\_2014.pdf (дата обращения: 20.03.2018 [↑](#footnote-ref-27)
28. Окинавская хартия Глобального информационного общества 21 июля 2000 года// Официальный сайт Президента РФ / URL: <http://www.kremlin.ru/supplement/3170> (дата обращения 25.04.2018). [↑](#footnote-ref-28)
29. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 г. URL: <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081580> (дата обращения 25.04.2018) [↑](#footnote-ref-29)
30. Резолюция принятая Генеральной Ассамблеей ООН // Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию/ A/RES/65/230 1.04.2011. URL: <http://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf> (дата обращения 27.04.2018) [↑](#footnote-ref-30)
31. Указ Президента Российской Федерации от 31.12.2015 г. № 683 «О стратегии национальной безопасности»/ URL: <http://www.kremlin.ru/acts/bank/40391> [↑](#footnote-ref-31)
32. Доктрина информационной безопасности Российской Федерации от 05.12.2016г // Сайт Министерства Иностранных Дел РФ/ URL: <http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163> [↑](#footnote-ref-32)
33. Конвенция об обеспечении международной информационной безопасности (концепция) от 22.09.2011г// Сайт МИД РФ/ URL: <http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666> [↑](#footnote-ref-33)
34. Когаловский М. Р. и др. Глоссарий по информационному обществу / Под общ. ред. Ю. Е. Хохлова. — М.: Институт развития информационного общества, 2009. — 160 с. [↑](#footnote-ref-34)
35. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.07.2016) "Об информации, информационных технологиях и о защите информации"// Официальный сайт компании «КонсультантПлюс» URL <http://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/> (дата обращения: 18.03.2018). [↑](#footnote-ref-35)
36. World Internet Users and 2018 Population Stats// Internet World Stats / 31.12.2017 URL: <https://www.internetworldstats.com/stats.htm> (дата обращения: 18.03.2018). [↑](#footnote-ref-36)
37. Шарапова М. И. ИКТ в образовании // Вестник МГЛУ. 2011. №620. URL: https://cyberleninka.ru/article/n/ikt-v-obrazovanii (дата обращения: 18.03.2018). [↑](#footnote-ref-37)
38. Киберпреступность и отмывание денег // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма./ Проект типологического исследования ЕАГ URL: <https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014.pdf> (дата обращения: 20.03.2018 [↑](#footnote-ref-38)
39. Definition of Cybersecurity Gaps and overlaps in standardisation// European Union Agency For Network And Information Security V1.0 DECEMBER 2015. Heraklion, Greece. – 35p. [↑](#footnote-ref-39)
40. Dennis M.A., Defenition of «Cybercrime»// Encyclopædia Britannica 09.03.2018 Encyclopædia Britannica, inc. URL: <https://www.britannica.com/topic/cybercrime> (дата обращения: 20.03.2018) [↑](#footnote-ref-40)
41. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. - 2014. - №8. – С. 46-50. [↑](#footnote-ref-41)
42. Отчет «Global Cybersecurity Index (GCI) 2017» // Официальный сайт Международного Союза Электросвязи URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI-17Report.pdf> (дата обращения: 20.03.2018) [↑](#footnote-ref-42)
43. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО «Издательство «Юрлитинформ», 2001. – 25 с. [↑](#footnote-ref-43)
44. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. - 2014. - №8. – С. 46-50. [↑](#footnote-ref-44)
45. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года// Официальный сайт МВД Республики Беларусь URL. <http://mvd.gov.by/main.aspx?guid=4603> (дата обращения 20.03.2018) [↑](#footnote-ref-45)
46. Киберпреступность и отмывание денег // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма./ Проект типологического исследования ЕАГ URL: <https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014.pdf> (дата обращения: 21.03.2018 [↑](#footnote-ref-46)
47. Багдеева В. А. Проблемы международной киберпреступности // Актуальные проблемы российского права. – 2009. – № 3(12). – С. 564-572. [↑](#footnote-ref-47)
48. Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности. Проект, февраль 2013. Вена , 2013. – 153с. [↑](#footnote-ref-48)
49. Бондарь Владимир Владимирович Киберпреступность – современное состояние и пути борьбы // Юридические записки. 2013. №2. <URL:https://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby> (дата обращения: 22.03.2018).  [↑](#footnote-ref-49)
50. Ершов А., К 2018 году потери РФ от киберпреступлений превысят 2 трлн рублей// Российская Газета официальный сайт / Рубрика «Экономика от 01.10.2016 г. URL: <https://rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html> (дата обращения 24.03.2018) [↑](#footnote-ref-50)
51. Cyber Security Intelligence Index 2016 // IBM Security. - URL: [http://www-01.ibm.com/common/ssi/cgi-](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&amp;infotype=SA&amp;htmlfid=SEW03133USEN&amp;attachment=SEW03133USEN.PDF) [bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&amp;infotype=SA&amp;htmlfid=SEW03133USEN&amp;attachment=SEW03133USEN.PDF) (дата обращения 24.03.2018) [↑](#footnote-ref-51)
52. Валько Д.В., Киберпреступность в России и мире: Сравнительный анализ Управление в Социально- Политических и Правовых системах, №3(10) 2016 с- 33. [↑](#footnote-ref-52)
53. См. Приложение 1 рис 1 [↑](#footnote-ref-53)
54. См. Приложение 1. рис.2 [↑](#footnote-ref-54)
55. См. Приложение 2. рис.3 [↑](#footnote-ref-55)
56. Global Threat Intelligence Report 2016 // NTT Group. URL <https://www.nttsecurity.com/en-us/gtic-2016-q4-threat-intelligence-report> (дата обращения 25.03.2018); [↑](#footnote-ref-56)
57. См. Приложение 3. рис.5 . [↑](#footnote-ref-57)
58. См. Приложение 2. рис.4 [↑](#footnote-ref-58)
59. Kaspersky Security Bulletin 2015// Kaspersky Security Lab. URL: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09065518/KSB_2015_business_threats_ru.pdf> (дата обращения 25.03.2018) [↑](#footnote-ref-59)
60. См. Приложение 3 рис. 6 [↑](#footnote-ref-60)
61. Norton Cyber Security Insights Report 2017 Global Results // Norton by Symantec 2018 URL: <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf> (дата обращения: 17.03.2018). [↑](#footnote-ref-61)
62. См. Приложение 7. рис.12 [↑](#footnote-ref-62)
63. IBM X-Force Threat Intelligence Index 2018 // IBM Security © Copyright IBM Corporation 2018. – New York, USA. March, 2018. -43p. [↑](#footnote-ref-63)
64. См. Приложение 4 рис 7 [↑](#footnote-ref-64)
65. Российские СМИ атаковал вирус-шифровальщик Bad Rabbit// Русская Служба BBC. 24.10.2017 URL: <https://www.bbc.com/russian/news-41739756> (дата обращения: 24.12.2017). [↑](#footnote-ref-65)
66. Перекалин A., Bad Rabbit: новая эпидемия шифровальщика// Блог Лаборатории Касперского, статья от 24.10.2017 URL: <https://www.kaspersky.ru/blog/bad-rabbit-ransomware/19072/> (дата обращения: 24.12.2017). [↑](#footnote-ref-66)
67. Николаев А. Вирус Wanna Cry заразил десятки тысяч компьютеров по всему миру// Официальный сайт Новости Первого Канала – репортаж от 13.05.2017 URL: <https://www.1tv.ru/news/2017-05-13/325201-virus_wanna_cry_zarazil_desyatki_tysyach_kompyuterov_po_vsemu_miru> (дата обращения: 24.12.2017). [↑](#footnote-ref-67)
68. Валько Д.В., Киберпреступность в России и мире: Сравнительный анализ Управление в Социально- Политических и Правовых системах, №3(10) 2016 с - 39. [↑](#footnote-ref-68)
69. ООО «ГикБрейнс» // Самые громкие кибератаки 21 века 15.06.2016 URL: <https://geekbrains.ru/posts/hackers_attacks_xxi> (дата обращения: 24.03.2018). [↑](#footnote-ref-69)
70. «Лаборатория Касперского» опубликовала подробности хакерской атаки на ядерный проект Ирана// RT 13.11.2014URL: <https://russian.rt.com/article/59295> (дата обращения: 25.03.2018). [↑](#footnote-ref-70)
71. Зайцев В., Самые известные кибератаки. Как хакеры угрожают миру // Газета Коммерсант 29.06.2017. URL: <https://www.kommersant.ru/doc/3338435#id=4> (дата обращения: 25.03.2018). [↑](#footnote-ref-71)
72. Ромашенко С., Der Spiegel: Хакеры атаковали бундестаг по поручению властей РФ. // Deutsche Welle 30.01.2016 URL: <http://p.dw.com/p/1Hm92> (дата обращения: 26.03.2018). [↑](#footnote-ref-72)
73. «Научное сообщество студентов. Междисциплинарные исследования»: Электронный сборник статей по материалам ХII студенческой международной научно- практической конференции. – Новосибирск: Изд. АНС «СибАК». – 2017. – № 1 (12)/ URL: <http://www.sibac.info/archive/science/1(12).pdf>. с. 418. (дата обращения: 26.03.2018). [↑](#footnote-ref-73)
74. Интернет-пропаганда – одна из главных киберугроз 2017 года// Digital Report Инфобезопасность 19.12.2016 URL: <https://digital.report/internet-propaganda-odna-iz-glavnyih-kiberugroz-2017-goda/> (дата обращения: 26.03.2018). [↑](#footnote-ref-74)
75. Политические преступления// Большой юридический словарь. — М.: Инфра-М. А. Я. Сухарев, В. Е. Крутских, А.Я. Сухарева. 2003. URL: <http://www.e-reading.club/bookreader.php/135201/Bol%27shoii_yuridicheskiii_slovar%27.pdf> (дата обращения: 26.03.2018). [↑](#footnote-ref-75)
76. Краковский К. П. Государственные и политические преступления (к вопросу о понятиях) // Северо-Кавказский юридический вестник. 2009. №1. URL: <https://cyberleninka.ru/article/n/gosudarstvennye-i-politicheskie-prestupleniya-k-voprosu-o-ponyatiyah> (дата обращения: 27.03.2018). [↑](#footnote-ref-76)
77. Болгов Радомир Викторович Сообщества пользователей интернет-проектов // Вестник МГИМО. 2013. №1 (28). URL: <https://cyberleninka.ru/article/n/soobschestva-polzovateley-internet-proektov> , с 55, с 57 (дата обращения: 15.04.2018). [↑](#footnote-ref-77)
78. Там же [↑](#footnote-ref-78)
79. Хакеры группы Anonymous присоединяются к иранским протестам // ИноПресса 15.02.2011. URL: <https://www.inopressa.ru/article/15Feb2011/times/anonym.html> (дата обращения: 15.04.2018). [↑](#footnote-ref-79)
80. Там же [↑](#footnote-ref-80)
81. Меркачева Е., Шалтай-Болтай сел на измену// "Московский комсомолец" №27312 от 31.01. 2017 URL: <http://www.mk.ru/social/2017/01/30/khakerskie-tayny-shaltayboltaya-kto-publikoval-vzlomannuyu-pochtu-vipov.html> (дата обращения: 15.04.2018). [↑](#footnote-ref-81)
82. Ващенко В., «Шалтай» получил двушечку //Газета.ru 06.07.2017, - URL: <https://www.gazeta.ru/social/2017/07/06/10775462.shtml> (дата обращения: 15.04.2018 ). [↑](#footnote-ref-82)
83. Шадрин И., Хакерская группа LulzSec вызвалась отомстить за взлом серверов Sega// РИА Новости «Наука» Москва . 20.06.2011 URL: <https://ria.ru/science/20110620/390610091.html> (дата обращения: 16.04.2018). [↑](#footnote-ref-83)
84. Хакеры LulzSec взломали сайт знакомств американских военнослужащих// Вести.ру – В мире , 28.03.2012 URL: <http://www.vesti.ru/doc.html?id=754172> (дата обращения: 16.04.2018). [↑](#footnote-ref-84)
85. Хакеры "Сирийской электронной армии" взломали сайты мировых СМИ // РИА Новости – «Технологии» 27.11.2014 <URL:https://ria.ru/technology/20141127/1035484262.html> (дата обращения: 16.04.2018). [↑](#footnote-ref-85)
86. "Сирийская электронная армия" взломала сайт морпехов США // РИА Новости «Сирия» 02.09.2013 URL: <https://ria.ru/arab_sy/20130902/960209048.html> (дата обращения: 16.04.2018). [↑](#footnote-ref-86)
87. "Сирийская электронная армия" взломала сайт армии США// РИА Новости «В мире» 08.06.2015 URL: <https://ria.ru/world/20150608/1068927675.html> (дата обращения: 16.04.2018). [↑](#footnote-ref-87)
88. Иванов К., Группа Fancy Bears взломала почту Ричарда Макларена и других спортивных чиновников// 10.01.2016 URL: <https://www.spb.kp.ru/daily/26780.4/3813416/> (дата обращения: 16.04.2018). [↑](#footnote-ref-88)
89. Слободян Е., Что представляет собой группировка хакеров Fancy Bears? // Аргументы и Факты 14.09.2016 <URL:http://www.aif.ru/dontknows/file/chto_predstavlyaet_soboy_gruppirovka_hakerov_fancy_bears> (дата обращения: 16.04.2018). [↑](#footnote-ref-89)
90. Кибератаки на правительственные сети связи в Германии продолжаются// Русская Служба BBC 01.03.2018 URL: <https://www.bbc.com/russian/news-43247681> (дата обращения: 16.04.2018). [↑](#footnote-ref-90)
91. We are legion. We do not forget. We do not forgive. Expect us. [↑](#footnote-ref-91)
92. Анонимные хакеры взломали сервер консультантов Пентагона// Русская Служба BBC 12.06.2011 URL: <https://www.bbc.com/russian/international/2011/07/110712_new_anonymous_attack> (дата обращения: 18.04.2018). [↑](#footnote-ref-92)
93. Anonymous взломали более 5 тысяч аккаунтов "Исламского государства"//РИА Новости «В мире» 17.11.2015 URL: <https://ria.ru/world/20151117/1322879329.html> (дата обращения: 18.04.2018). [↑](#footnote-ref-93)
94. Хакеры Anonymous утверждают, что взломали сотни сайтов в Китае// Украинская Служба BBC 06.04.2012 <URL:https://www.bbc.com/ukrainian/ukraine_in_russian/2012/04/120405_ru_s_anonymous_attack> (дата обращения: 18.04.2018). [↑](#footnote-ref-94)
95. Самые известные хакеры и их атаки // Официальный сайт Исторического журнала «Дилетант» 19.09.2015 URL: <http://diletant.media/articles/26011961/> (дата обращения: 18.04.2018). [↑](#footnote-ref-95)
96. Anonymous - The TRUTH about Donald Trump// Anonimous Official YouTube Channel 28.01.2017 <https://www.youtube.com/watch?v=rM-WpZ0ZO4Y> (дата обращения: 18.04.2018). [↑](#footnote-ref-96)
97. Покончил с собой Аарон Шварц // Коммерсант.ру 20.12.2013 URL: <https://www.kommersant.ru/doc/2360699> (дата обращения: 18.04.2018). [↑](#footnote-ref-97)
98. Волуйская М., Крупнейшие хакерские группировки мира. Инфографика// Аргументы и Факты 11.03.2017 URL: <http://www.aif.ru/dontknows/infographics/krupneyshie_hakerskie_gruppirovki_mira_infografika> (дата обращения: 18.04.2018). [↑](#footnote-ref-98)
99. Bissel K., LaSalle R.M., Richards K., «The Assenture Security Index»/ REDEFINING SECURITY PERFORMANCE AND HOW TO ACHIEVE IT 2017. – 16p [↑](#footnote-ref-99)
100. Окинавская хартия Глобального информационного общества 21 июля 2000 года// Официальный сайт Президента РФ / URL: <http://www.kremlin.ru/supplement/3170> (дата обращения 25.04.2018). [↑](#footnote-ref-100)
101. Чугунов А.В. Ч-83 Развитие информационного общества: теории, концепции и программы: Учебное пособие. — СПб.: Ф-т филологии и ис- кусств СПбГУ, 2007. —с 81. [↑](#footnote-ref-101)
102. Конвенция Организации Объединенных Наций против транснациональной организованной преступности // Принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года/ Официальный сайт Организации Объединенных Наций URL: <http://www.un.org/ru/documents/decl_conv/conventions/orgcrime> статьи 27,28,29 (дата обращения 25.04.2018). [↑](#footnote-ref-102)
103. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 г. URL: <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081580> (дата обращения 25.04.2018) [↑](#footnote-ref-103)
104. Совет Европы принял конвенцию по киберпреступности // Коммерсант.ру 09.11.2001 URL: <https://www.kommersant.ru/doc/926130> (дата обращения 25.04.2018). [↑](#footnote-ref-104)
105. Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. — 2016. — №28. — С. 720-723. — URL https://moluch.ru/archive/132/37021/ (дата обращения: 26.04.2018). [↑](#footnote-ref-105)
106. Якимова Е. М., Нарутто С. В., Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. №2. с 374 URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu (дата обращения: 26.04.2018). [↑](#footnote-ref-106)
107. Распоряжение Президента РФ№ 144-рп - О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. N 557-рп «О подписании Конвенции о киберпреступности»22.03.2008. URL: <http://www.kremlin.ru/acts/bank/27059> (дата обращения: 26.04.2018). [↑](#footnote-ref-107)
108. См. ссылку 89. [↑](#footnote-ref-108)
109. Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. — 2016. — №28. — С. 720-723. — URL https://moluch.ru/archive/132/37021/ (дата обращения: 26.04.2018). [↑](#footnote-ref-109)
110. Соглашение «о сотрудничестве государств – участников Содружества Независимых Государств, в борьбе с преступлениями в сфере компьютерной информации» Минск. 2001 год.// Официальный сайт Исполнительного Комитета СНГ. URL: <http://www.cis.minsk.by/page.php?id=866> (дата обращения: 26.04.2018). [↑](#footnote-ref-110)
111. Талипова Л. Р., Международно-правовая регламентация киберпреступности // Гуманитарные, социально-экономические и общественные науки. 2016. №4. с 122. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovaya-reglamentatsiya-kiberprestupnosti (дата обращения: 26.04.2018). [↑](#footnote-ref-111)
112. Соглашение «о сотрудничестве государств – участников Содружества Независимых Государств, в борьбе с преступлениями в сфере компьютерной информации» Минск. 2001 год.// Официальный сайт Исполнительного Комитета СНГ. URL: <http://www.cis.minsk.by/page.php?id=866> (дата обращения: 26.04.2018). [↑](#footnote-ref-112)
113. Концепция сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий от 25 октября 2013 года.// Интернет – портал «О СНГ» URL: <http://www.e-cis.info/page.php?id=23808> (дата обращения: 26.04.2018). [↑](#footnote-ref-113)
114. Резолюция принятая Генеральной Ассамблеей ООН // Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию/ A/RES/65/230 1.04.2011. URL: <http://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf> (дата обращения 27.04.2018) [↑](#footnote-ref-114)
115. Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности. Проект, февраль 2013. ООН -Вена , 2013. – 360 с [↑](#footnote-ref-115)
116. Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. — 2016. — №28. — С. 720-723. — URL https://moluch.ru/archive/132/37021/ (дата обращения: 26.04.2018). [↑](#footnote-ref-116)
117. Киберпреступность и отмывание денег // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма./ Проект типологического исследования ЕАГ URL: <https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014.pdf> (дата обращения: 21.03.2018 [↑](#footnote-ref-117)
118. «ДОХИНСКАЯ ДЕКЛАРАЦИЯ» от 12-19 апреля 2015 года.// Тринадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию / УНП ООН. Нью-Йорк .2015 год., - 26 с. [↑](#footnote-ref-118)
119. О Международном союзе электросвязи (МСЭ)// Официальный сайт МСЭ URL: <https://www.itu.int/ru/about/Pages/default.aspx> (дата обращения: 26.04.2018). [↑](#footnote-ref-119)
120. Schjølberg S., ITU Global Cybersecurity Agenda (GCA) // REPORT OF THE CHAIRMAN OF HLEG URL: <https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf> (дата обращения: 26.04.2018). [↑](#footnote-ref-120)
121. INDEX OF CYBERSECURITY INDICES 2017 // International Telecommunication Union 2017 . Geneva, 2017 17p [↑](#footnote-ref-121)
122. Global Cybersecurity Index 2017// International Telecommunication Union . - Geneva, 2017 – p 4 - 5 [↑](#footnote-ref-122)
123. Приложение 6 красные цвета и оттенки красного на карте рис 9. [↑](#footnote-ref-123)
124. Приложение 6. желтые цвета и оттенки желтого на карте рис. 9 [↑](#footnote-ref-124)
125. Приложение 6 зеленые цвета и оттенки зеленого на карте рис 9. [↑](#footnote-ref-125)
126. Приложение 6 рис. 10. [↑](#footnote-ref-126)
127. Global Cybersecurity Index 2017// International Telecommunication Union . - Geneva, 2017 – p 13 -15 [↑](#footnote-ref-127)
128. Miles T., U.N. survey finds cybersecurity gaps everywhere except Singapore // Reuters “Cyber Risk” 05.07.2017 URL: <https://www.reuters.com/article/us-cyber-un/u-n-survey-finds-cybersecurity-gaps-everywhere-except-singapore-idUSKBN19Q19L> (дата обращения: 27.04.2018). [↑](#footnote-ref-128)
129. Global Cybersecurity Index 2017// International Telecommunication Union . - Geneva, 2017 – p 34 , p41 [↑](#footnote-ref-129)
130. Аудитория пользователей интернета в России в 2017 году составила 87 млн. человек // Новости Российского Интернет Форума / Февраль - 2017 URL: <http://2017.russianinternetforum.ru/news/1298/> (дата обращения: 08.05.2018). [↑](#footnote-ref-130)
131. Связь 2017 – Оперативная информация //Деятельность в сфере телекоммуникации (по данным Минкомсвязи России) / Официальный сайт Федеральной службы государственной статистики РФ URL: [http://www.gks.ru/wps/wcm/connect/rosstat\_main/rosstat/ru/statistics/science\_and\_innovations/it\_technology/#](http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/) (дата обращения: 08.05.2018). [↑](#footnote-ref-131)
132. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы// Утвержденная Указом Президента РФ от 9 мая 2017 г. № 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы”/ Иформационно-правовой портал Гарант.ру URL: <http://www.garant.ru/products/ipo/prime/doc/71570570/> (дата обращения: 08.05.2018). [↑](#footnote-ref-132)
133. Доктрина информационной безопасности Российской Федерации // Утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646/ “Об утверждении Доктрины информационной безопасности Российской Федерации” Иформационно-правовой портал Гарант.ру URL: http://www.garant.ru/products/ipo/prime/doc/71456224/(дата обращения: 08.05.2018). [↑](#footnote-ref-133)
134. Там же.гл 5 ст 23.а. [↑](#footnote-ref-134)
135. Стратегия национальной безопасности Российской Федерации// Утвержденная указом Президента РФ № 683 от 31декабря 2015 года/ Иформационно-правовой портал Гарант.ру URL: <http://base.garant.ru/71296054/#friends> (дата обращения: 10.05.2018). [↑](#footnote-ref-135)
136. Концепция внешней политики Российской Федерации // Утверждена Президентом Российской Федерации В.В.Путиным 30 ноября 2016 г./ Официальный сайт Министерства Иностранных Дел РФ URL: <http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248> (дата обращения: 10.05.2018). [↑](#footnote-ref-136)
137. Дмитрик Н., Обзор законодательства Российской Федерации в сфере информационной безопасности – Часть 1: Общий обзор // Digital.Report Инфобезопасность. Статья от 04.12.2016 URL: <https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/> (дата обращения: 10.05.2018). [↑](#footnote-ref-137)
138. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 23.04.2018, с изм. от 25.04.2018)// Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ/ Официальный сайт компании «КонсультантПлюс» URL: <http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/> (дата обращения: 10.05.2018). [↑](#footnote-ref-138)
139. Дмитрик Н., Обзор законодательства Российской Федерации в сфере информационной безопасности – Часть 9: Борьба с киберпреступностью // Digital.Report Инфобезопасность. Статья от 04.12.2016 URL: <https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/> (дата обращения: 10.05.2018). [↑](#footnote-ref-139)
140. Управление «К» МВД России // Официальный сайт Министерства Внутренних Дел Российской Федерации URl: <https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii> (дата обращения: 10.05.2018). [↑](#footnote-ref-140)
141. Управление «К» МВД России // История подразделения/ Официальный сайт Министерства Внутренних Дел Российской Федерации URl: <https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii> (дата обращения: 10.05.2018). [↑](#footnote-ref-141)
142. Распоряжение Правительства РФ [Об усилении борьбы с преступлениями в сфере высоких технологий] от 22 октября 1999 года N 1701-р // Электронный Фонд Правовой и Нормативно –Технической Документации «Консорциум кодекс» URL: <http://docs.cntd.ru/document/901745530> (дата обращения: 12.05.2018). [↑](#footnote-ref-142)
143. Управление «К» МВД России // История подразделения/ Официальный сайт Министерства Внутренних Дел Российской Федерации URl: <https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii> (дата обращения: 10.05.2018). [↑](#footnote-ref-143)
144. Управление «К» МВД России // Официальный сайт Министерства Внутренних Дел Российской Федерации URl: <https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii> (дата обращения: 10.05.2018). [↑](#footnote-ref-144)
145. INDEX OF CYBERSECURITY INDICES 2017 // International Telecommunication Union 2017 . Geneva, 2017 17p [↑](#footnote-ref-145)
146. Эмм Д., Унучек Р., Kaspersky Security Bulletin: обзор 2017 года// Kaspersky security bulletin 2017 / URL: <https://securelist.ru/ksb-review-of-the-year-2017/88142/> (дата обращения 15.05.2018). [↑](#footnote-ref-146)
147. \* Автором были переведены только названия регионов, для удобства восприятия. Сравниваемые принципы не были переведены, потому, как были переведены и описаны в гл. 2.2. [↑](#footnote-ref-147)