# КИБЕРБЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

***Абдоков Аслан РАщидович***

*Северо-Кавказская государственная академия, г.Чекесск*

*Данная статья рассказывает о том, что в связи с развитием информационных и компьютерных технологий возникают проблемы, которые связаны с информационной безопасностью. На современном этапе развития общества киберпреступность приобрела глобальный характер. Рассматриваются проблемы организации противодействия преступлениям, которые совершаются в сфере информационных технологий. Для эффективной борьбы предлагается совершенствовать правовую базу и разработать концепцию организации противодействия киберпреступности.*

**Ключевые слова:** киберугроза, киберпространство, кибертерроризм, информационное пространство, киберпреступления, киберзащита, защита информации.

В современном мире наблюдается резкий рост инцидентов в области информационной безопасности. Они широко распространяются и как правило, носят угрожающий характер. Большинство из таких атак затрагивают частные, корпоративные и государственные интересы. Причины развития угроз очень разнообразны, например: возрастание числа атак, ведущих к большим потерям; воздействие на все электронные устройства, в особенности мобильные телефоны; применение наиболее развитыми странами технологических средств и методов кибернападения на другие государства.

Все это подтверждается ежедневными сводками новостей, где постоянно сообщают о новых атаках преступников в сфере информаций.

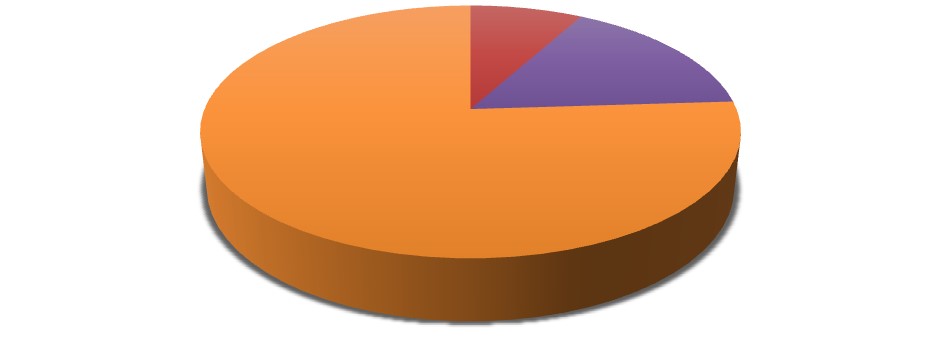
Ежегодно в сети обнаруживают миллиарды вредоносных объектов. За их распространение отвечает более чем 100 миллионов адресов. И каждый год это число увеличивается на 40%. Все атаки в информационном пространстве наносят колоссальный ущерб. За минувший год проведено 73% хакерских атак по экономическим причинам. На 2017 год убытки составили три триллиона долларов. А на 2021 год прогнозируют убыток шесть триллионов долларов.

В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)» [3, с. 4]. Если говорить о кибербезопасности, то можем сказать, что это совокупность условий, при которой все составляющие киберпространства защищены от максимально возможного числа угроз и действий с нежелательными последствиями.

Киберпространство – это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей. Его мы можем рассмотреть, как триаду, в которую входят три составляющие: информация в цифровом представлении (файлы, записанные на носители данных; пакеты, команды и т.д. передаваемые по различным сетям); техническая инфраструктура, с помощью которых осуществляется реализация основных действий с информацией (сбор, обработка, хранение и передача); информационное взаимодействие [2, с. 340].

Каждый день вирусы-вымогатели атакуют 4000 компьютеров. Если рассматривать в глобальном масштабе, то киберпреступность стала вторым наиболее частым преступлением. В течение нескольких минут происходят 93% хищения данных и из них 83% утечек не обнаруживаются владельцами на протяжении несколько недель. Самым крупным хищением данных был инцидент с Yahoo, когда в 2013 году злоумышленники похитили три миллиарда телефонных номеров. На (рис. 1) представлена статистика по количеству киберпреступлений по наиболее частым видам кибератак.

компьютерное мошенничество



8

%

16

%

76

%



нарушение информационной безопасности компьютерные атаки

Рисунок 1. Количество киберпреступлений по видам (март – апрель 2017 год)

Статистика компании Positive Technologies дает право утверждать, что в течение всего 2017 года финансовые компании входили в пятерку наиболее атакуемых киберпреступниками типов организации. В этом же году киберпреступники выработали основные схемы по быстрой монетизации. Самые распространенные атаки на АТМ (логические атаки на банкоматы). Такой тип демонстрирует драматический рост в этом году: за первое полугодие 2017 года общий объем атак такого типа в странах Европы вырос на 500% [4, с. 7].

Существует ряд требований по защите от кибервоздействий. Система киберзащиты сетевого коммуникационного оборудования (КЗСКО) предназначена для защиты сетевого коммуникационного оборудования (коммуникаторов, маршрутизаторов, модемов). Эта система обеспечивает: защиту сетевого коммуникационного оборудования от кибервоздействий из внешних сетей; защиту от компьютерных вирусов и иного вредоносного ПО.

В рамках киберпреступности можно выделить отдельный вид – это кибертерроризм. Так называемые, современные преступники – террористы используют все возможные и легкодоступные средства и способы для достижения желаемого результата. С каждым годом профессионализм кибертеррористов в использовании информационных сетей растет. Следовательно, кибербезопасность является проблемой государственной важности. Масштабность угрозы требует внимания и применения решительных мер ведущими государствами мира и объединения в целях предотвращения преступлений, которые совершаются в киберпространстве.

**Литература**

1. Гриняев С.Н., Поле битвы – киберпространство. М., 2004. 426 с.
2. Климов С.М. Методы и модели противодействия компьютерным атакам// КАТАЛИТ. Люберцы, 2008. 316 с.
3. Тонких И. М., Комаров М. М., Ледовской В. И., Михайлов А. В. Основы кибербезопасности // Описание курса для средних школ, 2-11 классы. М., 2016. 113 с.
4. Positive cinema cyberdocumentary// Кибербезопасность 2017-2018: цифры, факты, прогнозы. URL https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-20172018-rus.pdf