

Пинаева А.А.

Студент

4 курс, факультет экономики и финансов

ФГБОУ ВО Российская академия народного хозяйства и государственной

службы при Президенте Российской Федерации

Сибирский Институт Управления - филиал РАНХиГС

Россия, г. Новосибирск

Научный руководитель: Димитриева Е.Н.,

доцент кафедры налогообложения, учета и

экономической безопасности,

кандидат экономических наук

КИБЕРПРЕСТУПНОСТЬ - ПРОБЛЕМА МИРОВОГО МАСШТАБА

Аннотация: В статье рассматривается проблема современного общества - киберпреступность. С каждым годом в мире растет количество киберпреступлений. Это связано с постоянным техническим развитием компьютерных и информационных технологий, что, в свою очередь, помогает преступникам создавать все новые методы и пути обхода защитных систем. В статье разбирается данная проблема, и предлагаются пути решения для Российской Федерации.

Ключевые слова: вирусы, хакеры, кибератака, кибермошенничество, киберпреступность.

Pinaeva A.A.

Student

4 year, Faculty of Economics and Finance

Russian Academy of National Economy and Public Administration under the

President of the Russian Federation

Siberian Institute of Management - branch of the RANEPA

Russia, Novosibirsk

Scientific adviser: Dimitrieva E.N.,

Associate Professor of the Department of Taxation, Accounting and

economic security,

candidate of economic sciences

CYBERCRIME IS A GLOBAL PROBLEM

Abstract: The article deals with the problem of modern society - cybercrime. Every year the number of cybercrimes in the world is growing. This is due to the constant technical development of computer and information technologies, which, in turn, helps criminals to create all new methods and ways to bypass protective systems. This article deals with this problem, and suggests solutions for the Russian Federation.

Key words: viruses, hackers, cyber attack, cyber fraud, cybercrime.

Киберпреступлением считается преступление в так называемом виртуальном пространстве. К ним можно отнести кражу данных банковских карт, распространение вредоносных программ, фишинг (взлом конфиденциальной информации), распространение запрещенного контента (клеветы, материалов, возбуждающих межнациональную и межрелигиозную вражду), а также вмешательство в сети различных компьютерных систем.

Потенциальными жертвами данного вида преступлений могут быть не только именитые бизнесмены или политики, а также дети и пожилые люди. При этом, как правило, преступник и его цель находятся за тысячи километров друг от друга.

Вред, нанесенный преступниками частным компаниям, государственным учреждениям и обычным людям, с каждым годом неизменно растет. Согласно данным отчета международной службы по обеспечению безопасности в области киберугроз Symantec Security, за секунду в мире совершается 12 кибератак, что в год составляет 556 млн. киберпреступлений. Общий ущерб оценивается в 100 млрд. долларов США.

По данным Лаборатории Касперского только за третий квартал 2017 года было отражено 277 646 376 атак, которые проводились из 185 стран мира. На рисунке 1 приведена география киберугроз: чем ярче цвет, тем выше уровень опасности.¹

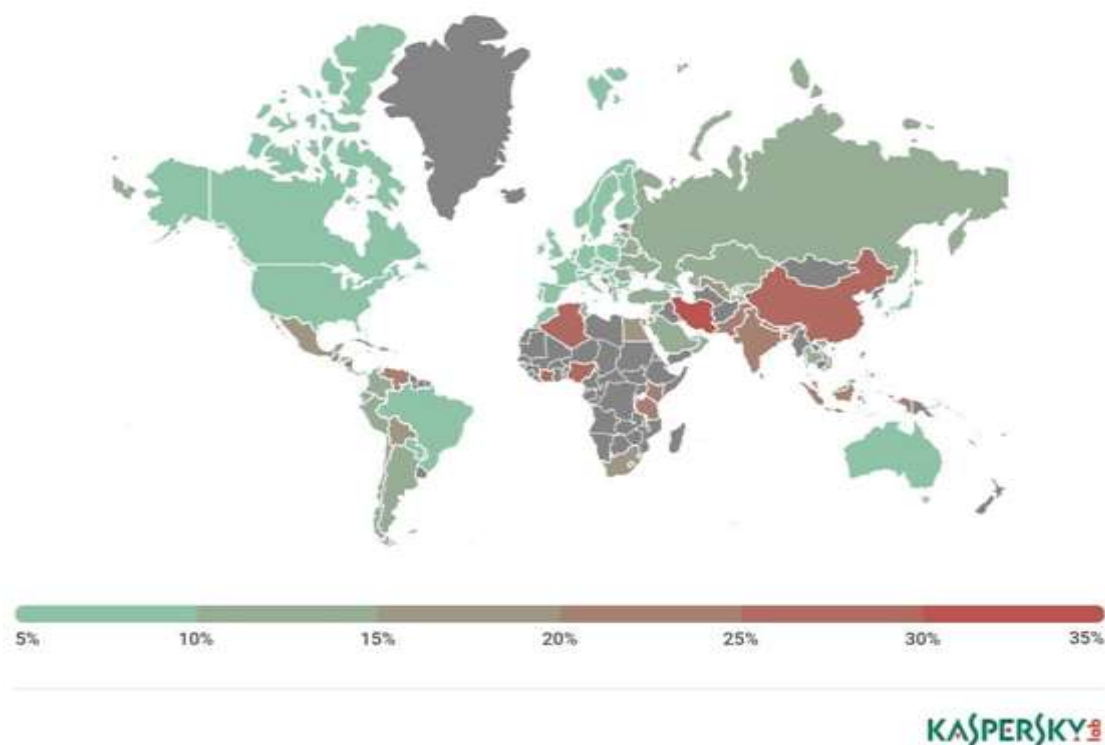


Рис. 1 - География киберугроз по данным Лаборатории Касперского

В России рост данного вида преступности связан с тем, что уровень компетенции следователей, занимающихся киберпреступностью, часто

¹ Официальный сайт Лаборатории Касперского [Электронный ресурс]. - Режим доступа: <https://www.kaspersky.ru/> (дата обращения: 08.05.18).

невысок, соответственно, раскрываемость таких правонарушений мала. Исходя из информации, предоставленной Генеральной прокуратурой Российской Федерации, в 2016 г. было раскрыто только 8% от всех преступлений. В свою очередь, законодательство страны в данной области развивается слишком медленно. По данным департамента при Верховном суде, всего 26% осужденных за кибермошенничество были осуждены к лишению свободы, 11% - к штрафам.

Рассмотрим статистику киберпреступлений в России, совершенных с 2015 по 2017 гг.

Таблица 1 – Количество киберпреступлений в России за 2015-2017 гг.

	Преступления, совершенные с использованием компьютерных и телекоммуникационных технологий, тыс.
2015 год	41
2016 год	66
2017 год	91

Только в России за последние 3 года количество IT-преступлений возросло с 41 тыс. до 91 тыс., то есть более чем в 2 раз, а ущерб от них составил приблизительно 45 миллионов долларов.²

Преступления хакеры совершают в основном посредством вредоносных программ. Распространяться они могут самыми различными способами, например, файловые компьютерные вирусы вставляют свой вредоносный код в тело программных файлов таким образом, что при запуске программы управление передается вирусу. Затем вирус выполняет свои вредоносные действия и возвращает управление программе-жертве. Также популярным среди преступников способом является заражение устройств путем мобильных троянцев через смс или почту.

² Состояние преступности в Российской Федерации [Электронный ресурс]. - Режим доступа: <https://xn--b1aew.xn--p1ai/folder/101762> (дата обращения: 08.05.18).

Вред от данных программ всегда заключается в хищении информации или денежных средств. В частности, вирусы семейства Svrpeng способны самостоятельно выдавать все необходимые права и воровать данные из других программ или шифровать информацию и требовать за нее выкуп.

Другие виды подобных программ могут красть деньги посредством подписок пользователя, они имеют возможность посещать сайты и оплачивать услуги средствами со счета мобильного телефона, причем делают они это совершенно незаметно для владельца гаджета.

Однако это далеко не все, чем могут промышлять хакеры. Так, в 2016 г. крупнейшие банки России, такие как Сбербанк, Альфа-банк и др., оказались в самой сложной ситуации за свою историю: в атаке участвовали тысячи компьютеров по всему миру. Были совершены покушения на хищения средств в 5 млрд. рублей, 2 из которых злоумышленникам удалось украсть. Также были атакованы электронные почты: 57 млн. пользователей Mail.ru, 40 млн. Yahoo, 33 млн. Hotmail и 24 млн. Gmail потеряли в общей сложности 272 млн. своих данных, а киберпреступнику под псевдонимом Pease удалось заполучить доступ к аккаунтам социальной сети «ВКонтакте». В его руках оказались данные 70 млн. пользователей.

12 мая 2017 года была осуществлена одна из крупнейших кибератак с использованием вредоносной программы под названием WannaCry, которая поражает гаджеты только под управлением Microsoft Windows.³ Первой была атакована Испания, затем другие страны. Россия заняла первое место по количеству заражений. Программа поразила более 500 тыс. компьютеров правительственных учреждений, коммерческих организаций и частных лиц, зашифровав данные и требуя с пользователей от 300-600 долларов под угрозой удаления всей информации.

По данным социологического исследования, проведенного факультетом психологии МГУ им. М.В. Ломоносова и Фонда развития

³ Центр исследования компьютерной преступности [Электронный ресурс]. - Режим доступа: <http://www.crime-research.ru/articles/cyber12991/> (дата обращения: 08.05.18).

Интернет в рамках проекта «Дети России онлайн», росту числа киберпреступлений также помогают сами люди, которые пользуются интернетом.⁴ Так, не всегда соблюдаются основные правила безопасности: афиширование излишней информации о себе при общении с незнакомцами, несоблюдение правил хранения паролей. Люди зачастую недооценивают угрозы со стороны хакеров и вредоносных программ: скачивают музыку, фильмы, онлайн-игры.

Киберпреступность в России и мире с каждым годом становится все популярнее в виду безнаказанности и труднораскрываемости. В нашей стране, на мой взгляд, для успешной борьбы с данным видом угрозы требуется привести составы киберпреступлений в Уголовный кодекс Российской Федерации. Нынешние статьи 272, 273, 274 не учитывают современных технологических особенностей, наказание несоизмерно тяжести преступлений - похитители миллионов рублей могут отделаться условным сроком.

Также необходимо проводить с населением профилактические беседы, доносить до людей угрозу, которая скрывается в сети интернет. Как известно, раскрытие компьютерных преступлений возможно только с помощью компьютерных технологий, поэтому необходимо уделить должное внимание переподготовке существующих кадров в сфере киберпреступлений и подготовке новых сотрудников. Высокая квалификация специалистов обеспечит быструю реакцию на изменчивый виртуальный мир, сбор, отыскивание и изъятие доказательств в электронной форме.

Популярность преступлений в компьютерной сфере обусловлена невероятными доходами и минимальными рисками. Рост числа подобных киберугроз, несомненно, будет расти, поэтому данная проблема должна быть первой на повестке современного государства.

⁴ Цифровая компетентность подростков и родителей (под ред. Г.У. Солдатовой, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова). 2016. М.: Фонд развития Интернет, 144 с.

Использованные источники:

1. Цифровая компетентность подростков и родителей (под ред. Г.У. Солдатовой, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова). 2016. М.: Фонд развития Интернет, 144 с.
2. Официальный сайт Лаборатории Касперского [Электронный ресурс]. - Режим доступа: <https://www.kaspersky.ru/> (дата обращения: 08.05.18).
3. Состояние преступности в Российской Федерации [Электронный ресурс]. - Режим доступа: <https://xn--b1aew.xn--p1ai/folder/101762> (дата обращения: 08.05.18).
4. Центр исследования компьютерной преступности [Электронный ресурс]. - Режим доступа: <http://www.crime-research.ru/articles/cyber12991/> (дата обращения: 08.05.18).