УДК 338

ВЛИЯНИЕ КИБЕРПРЕСТУПНОСТИ НА РОССИЙСКУЮ ЭКОНОМИКУ

Исмоилов З.Ш., студент 4 курса экономического факультета
Научный руководитель – Климушкина Н.Е.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

***Ключевые слова**: киберпреступность, кибершпионаж, цифровизация, Демонетизация, экономический рост, факторы риска*

Интернет стал предметом домашнего обихода в России и почти вся информация и данные работают онлайн. Благодаря этому киберпреступность стремительно наращивает свое влияние на российскую экономику. Существуют различные виды киберпреступлений, создающие воздействие и угрозу экономике страны и даже нарушающие мир и безопасность. В данной статье уделяют внимание тому, как киберпреступность оказывает опасное влияния на российскую экономику

С тех пор как Интернет стал в России товаром домашнего обихода, киберпреступность стала сегодня главной проблемой. Любое преступление, совершенное с использованием компьютера и интернета, называется киберпреступностью. Это преступление может быть совершено против человека, коммерческой, некоммерческой организации или государства. Это оказывает серьезное влияние как на нашу экономику, так и на наше общество. Согласно различным опросам и отчетам, киберпреступность затрагивает различные отрасли промышленности и увеличивает факторы риска [1]. Согласно данным МВД России за три месяца 2020 года число преступлений с использованием информационных технологий выросло почти на 84% по сравнению с аналогичным периодом прошлого года.

Из-за данного фактора уровень преступности в стране в целом увеличился на 4% за указанный период. Количество IT-преступлений выросло на 83,9%, а удельный вес таких деяний достиг 19,9% от общего числа по

сообщили ТАСС в пресс-службе ведомства.

Число мошенничеств за март текущего года увеличилось на 48,5% по сравнению с прошлым годом, при этом количество преступлений с использованием электронных средств платежа возросло более чем в два раза. При этом потери экономики РФ составили в 2019 году около 2,5 трлн рублей. К концу 2021 года данный ущерб, по оценке экспертов Сбербанка, может вырасти до 7 трлн рублей.

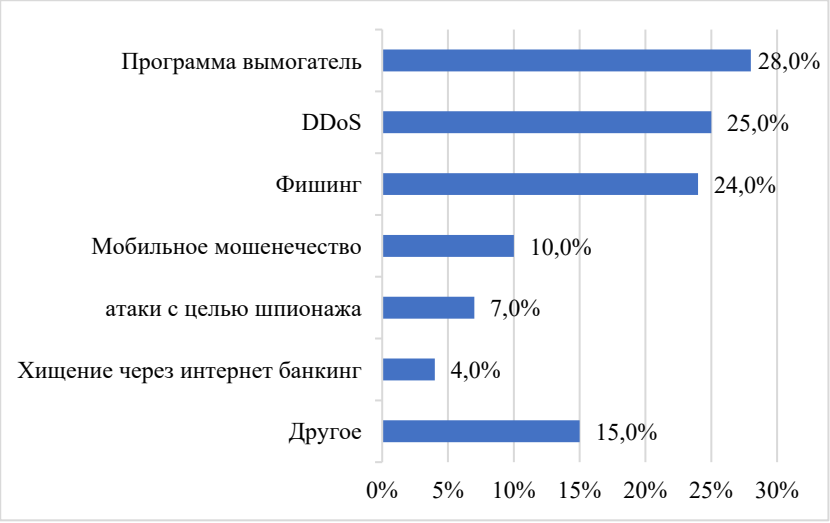

Рисунок-1 Данные о киберпреступлениях в России

Выявлены следующие виды киберпреступлений

• Кибер-преследование — это тип киберпреступности создает физические угрозы с помощью таких технологий, как смартфоны, электронная почта, сообщения, веб-сайты или видео. Нападение путем угрозы лицу или членам его семьи с использованием.

• Кибер-отмывание — это вид киберпреступности включает в себя онлайн-перевод валюты с намерением скрыть ее источник и назначение.

• Кибер-терроризма — это вид преступления включает в себя использование технологии для уничтожения или причинения вреда человеку или организации. Это преступление включает в себя взлом и кибер-кражу. Все действия, такие как отравление кэша DNS, кража личных данных,

мошенничество, отправка спам-сообщений, фишинг, плагиат и пиратство.

Другие преобладающие атаки:

1.Угон Оборудования — это угон сетевого оборудования. В 2015 году CISCO выпустила предупреждение о том, что злоумышленники получают физический доступ к устройствам Cisco IOS и заменяют их вредоносным образом ROMMON.

2.Инсайдеры - Общий процент этой категории атакующих составляет 20%, но она наносит 80% урона. Таким образом, они подвергаются наибольшему риску, поскольку находятся внутри организации [3-5].

В заключение остается добавить, что в качестве наиболее эффективных мер по противодействию киберпреступности эксперты Group-IB, ФРИИ и Microsoft выделяют следующие:

— повышение уровня киберграмотности (осведомленность об угрозах и способах защиты);

— обязательное раскрытие информации о киберинцидентах;

— совершенствование как международных процедур взаимной правовой

помощи, так и национального законодательства о составах преступлений

и процедурах расследования;

— расширение трехстороннего партнерства бизнеса, представителей рынка кибербезопасности и государства

Библиографический список

1. Актуальные киберугрозы. II квартал 2019 г. - [Электронный ресурс]. – Режим доступа: www.ptsecurity.com

2. Александрова, Н.Р. Использование информационных технологий в исследовании экономической безопасности муниципальных образований / Н.Р. Александрова, А.А. Настин, Н.Е. Климушкина // Экономика и предпринимательство. 2020 - № 10 (123). - С. 392-395.

3. Банникова, Е.В. Внутренний аудит в системе экономической безопасности / Е.В. Банникова, О.И. Хамзина, А.А. Навасардян //Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения: материалы Национальной научно-практической конференции. В

2-х томах. -Ульяновск.- 2019. -С. 225-229.
4. Хамзина, О.И. Роль риск-менеджмента в обеспечении экономической безопасности сельскохозяйственного предприятия/ О.И. Хамзина, И.И. Хамзин, Е.В. Банникова// Экономика и предпринимательство. - 2018. - № 11 (100). - С. 1136-1139.
5. Светуньков, М.Г. Теория и методология государственного регулирования патримониальными предпринимательскими сетями: автореферат дис. ... доктора экономических наук: 08.00.05 / Светуньков М.Г. - Санкт-Петербург, 2011. - 43 с.

THE IMPACT OF CYBERCRIME ON THE RUSSIAN ECONOMY THE ECONOMY

Ismailov Z. SH.,

Keywords: *cybercrime, cyber espionage, digitalization, Demonetization, economic growth, risk factors*

The Internet has become a household item in Russia and almost all information and data work online. Thanks to this, cybercrime is rapidly increasing its impact on the Russian economy. There are various types of cybercrime that create an impact and threat to the country's economy and even violate peace and security. This article focuses on how cybercrime has a dangerous impact on the Russian economy as It moves towards new investments, digitalization and demonetization.