УДК 004.056.53

ТИПЫ УГРОЗ КИБЕРБЕЗОПАСНОСТИ И СПОСОБЫ БОРЬБЫ С ХАКЕРСТВОМ

И.Д. Алекперов

к.т.н., доцент

Южный университет (ИУБиП), e-mail: ilgar@iubip.ru

А.А. Горбачева

Аспирант 5-го года обучения

Южный университет (ИУБиП), e-mail: asya379@yandex.ru

Аннотация: Статья направлена на изучение и обобщение основ кибербезопасности. В результате оснащения темы, обобщения материала. Пользователи сети Интернет должны приобрести базовые знания о информационной безопасности, угрозах, методах защиты от них. Так же, статья позволяет сформировать и использовать полученные знания по использованию сети Интернет и защите от злоумышленников от разных видов информационных угроз. В статье указаны и перечисляются понятия кибербезопасности, кибергигиены, типы угроз информационной безопасности, различные способы борьбы с вирусами, способы сохранения персональных данных посетителей сети Интернет. Целью данной статьи является оснащение населения о базовых способах защиты от угроз злоумышленников в сети Интернет, о способах разоблачения взлома, слива персональных данных. Не мало важным так же является указание статистики взломов, хакерства; дальнейшие прогнозы о будущих информационных проблем. Указано мнение выдающегося программиста о данной проблеме, его оценка нынешней ситуации в сети Интернет, советы для пользователей. В результате будут выделены наиболее важные знания, обобщены различные положения информационной безопасности и будет знакомство с понятиями кибергигиена, киберугроза, кибербезопасность.

Ключевые слова: кибергигиена, безопасность, сеть Интернет, киберугроза, злоумышленники, кибербезопасность, защита от угроз.

TYPES OF CYBER SECURITY THREATS AND METHODS TO FIGHT HACKING

I.D. Alekperov

A.A. Gorbachev

Abstract: The article is aimed at studying and generalizing the basics of cybersecurity. As a result of equipping the topic, generalizing the material. Internet users should acquire basic knowledge of information security, threats, methods of protection against them. Also,

the article allows you to form and use the knowledge gained on the use of the Internet and protection from intruders from various types of information threats. The article identifies and lists the concepts of cybersecurity, cyberhygiene, types of information security threats, various ways to combat viruses, ways to save personal data of Internet visitors. The purpose of this article is to equip the population about the basic methods of protection against cybercriminals' threats on the Internet, about ways to expose hacking, and drain personal data. It is also important to indicate statistics of hacking, hacking; further predictions about future information problems. The opinion of an outstanding programmer about this problem, his assessment of the current situation on the Internet, tips for users are indicated. As a result, the most important knowledge will be highlighted, various provisions of information security will be summarized and familiarity with the concepts of cyber hygiene, cyber threat, cyber security will be provided.

Keywords: cyber hygiene, security, Internet, cyber threat, attackers, cyber security, protection against threats.

Тема кибербезопасности актуальна на государственном уровне, так как распространено финансовое жульничество, продажа нелегальных услуг и предметов, а также низкая осведомленность пользователей сети Интернет и отсутствие быстрого реагирования. По данным причинам уровень устойчивости личных данных в киберсистеме низкий.

Кибербезопасность – совокупность мер и методов защиты от взломов, атак хакеров для компьютеров, планшетов, мобильных устройств, серверов, электронных серверов, приложений, сетей и использования информации в корыстных целях. Данная система имеет популярность и используется в разных областях: бизнес-сфера, IT-сфера, юриспруденция и так далее[1, 2, 5].

Масштаб распространения угроз в сети Интернет возрастает с каждым годом. Так, согласно отчетам RiskBased в период с 01.01.2019 по 01.09.2019 было обнаружено 7,9 миллиардов случаев утечки информации из киберсистемы. Данные значения превышают показатели 2018 года в два раза.

Компания International Data Corporation дала следующие прогнозы. По их подсчетам, если количество утечек информации будет расти и дальше, то только в Америке к 2022 году их число приблизится к 134 миллионам, а расходы по обеспечению кибербезопасности достигнет 133,7

миллиардов долларов. Правительства разных стран стараются бороться с преступниками, злоумышленниками и стараются организовывать и внедрять различные методы информационной безопасности [3, 4, 7].

Типы угроз кибербезопасности:

– Фишинг– отсылка мошеннических электронных писем, схожих на сообщения от надежных адресатов. Целью является кража персональных данных, секретной информации(например, номера кредитных карт, паспортные данные). Способом защиты является обучение юзеров всемирной паутины совокупностей методов по блокировке вирусных и мошеннических электронных писем.

– Вирусы-вымогатели– способ вымогания денег, при котором блокируется доступ к файлам и социальным системам до оплаты выкупа. Однако, уплата не гарантирует восстановления компьютерных систем.

– Вредоносное ПО– несанкционированное программное обеспечение, причиняющее вред компьютеру или мобильному устройству.

– Большинство компаний, служб сталкиваются с киберугрозой. Многие теряют безвозвратно теряют важную информацию, данные, денежные средства из-за отсутствия должной информационной безопасности. Бывали случаи, когда секретные материалы становились доступны в сети Интернет и ими могли пользоваться разные люди. Не менее распространенная ситуация, когда обычные юзеры всемирной паутины не могли сохранить личные сведения и ими злоумышленники пользовались в корыстных целях, выпрашивая денежные средства или шантажируя по-иному [8, 9].

Пользователи должны иметь представление о базовых способах защиты данных, например, использование надежных паролей, осторожные переходы на незнакомые сайты, использование и распространение

персональных данных при обращении с электронной почтой и резервными данными.

Создание организациями кибербезопасности совокупностей мер по остановление кибератак и их негативных последствий. Для этого необходимо ознакомиться с способами выявления, обнаружения киберугроз, защиты систем.

Необходимость создания технологий по организации компьютерной безопасности частных лиц, различных компаний и государств.

Кибергигиена - это способы соблюдения правил информационной безопасности при работе в сети Интернет. Данные навыки полезны для использования всемирной паутины и обеспечения личной безопасности.

Интересный факт, что две трети пользователей имеют, как правило, одно незащищенное устройство, которое может быть раскрыто злоумышленниками. Также, используя незащищенные сети Wi-Fi подвергают риску утечки данных.

Соблюдение простых правил кибербезопасности позволят сохранить личную защиту. Соблюдение кибергигиены является потребностью каждого пользователя сети Интернет[6, 10].

Анализируя мнение ведущего аналитика отдела развития ООО «Доктор Веб» Вячеслава Медведева, можно прийти к выводу, что 100%, абсолютной защиты в киберсистеме нет. Однако пользуясь методами обеспечения защищенности можно постараться сохранить собственные данные и при этом спокойно использовать электронными серверами.

Аналитик рассказывает о новом популярном способе программы с мошенническими программами это троянцы-шифровальщики, требующие выкуп за расшифровку информации.

Также, он рекомендует не пользоваться незнакомыми сайтами, не подключаться к неизвестным бесплатнымсетевым подключениям.

Различные способы борьбы с хакерством:

– Установление антивирусной защиты(антивирусные программы);

– Создание службы по управлению кибербезопасностью;

– Установление программ, обеспечивающих своевременное обновление

– Установление оборудования, снащенного защитой от киберугроз;

– Резервное копирование информации;

– Ограниченное использование социального пространства с целью сохранения личной информации, копирования данных и так далее

– Отсутствие доступа к некоторым сетям, системам и информации

Способы сохранения личных данных пользователям сети Интернет:

– НЕ посещать сомнительные сайты;

– НЕ переходить по ссылкам в неизвестные источники;

– НЕ распространять сомнительные сайты;

– НЕ распространять и не вводить свои персональные данные(номер телефона, паспортные данные, адрес места жительства и так далее) на незнакомых сайтах и так далее;

– Устанавливать антивирусные программы;

– Регулярно проверять и обновлять программы безопасности [9, 10].

Исходя из вышеперечисленного, можно прийти к следующим выводам:

– Вирусы-вымогатели – способ вымогания денег, при котором блокируется доступ к файлам и социальным системам до оплаты выкупа. Однако, уплата не гарантирует восстановления компьютерных систем.

– Информационная безопасность является потребностью, а также обязанностью каждого юзера. Чем больше людей будут соблюдать кибергигиену, тем скорее уменьшиться количество кибератак и расходов со стороны государства и частных лиц на них.

– Соблюдение базовых правил позволяет спокойно использовать электронные сети.

– Даже специалисты, изучающие область информационной безопасности не гарантируют 100% защиты от атак злоумышленников в сети Интернет.

– Существует 3 вида киберугроз: вредоносное ПО, фишинг, вирусы-вымогатели.

– Изучение и распространение данной темы позволит уменьшить количество кибератак, расходы на них, обезопасит все больше частных лиц, организаций, компаний, государства.

Библиографический список литературы

1. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И.Д. Алекперов, В.В. Храмов, А.А. Горбачева, Д.П. Фомичев; ЮУ (ИУБиП). – Ростов-на Дону, 2019. – 114 с.
2. Алекперов И.Д. Разработка информационного ресурса выпускников “Школы развития личности и успеха ИУБиП” в интернет пространстве с использованием языков программирования PHP, MySQL. – Ростов–на–Дону: ИУБИП, 2013.
3. Алекперов И.Д. Электронная коммерция (E–commerce). [Электронный ресурс] LAP LAMBERT Academic Publishing. ISBN 978–3–330–35282–7, URN: 101:1–201708141845, EAN: 9783330352827. – URL: http://d–nb.info/Erschei–nungsdatum: 2017 г. (Дата обращения 07.06.2019 г.).
4. Алекперов И.Д. Электронный бизнес–консалтинг как средство развития региональной электронной коммерции // Интеллектуальные ресурсы – региональному развитию.– 2016. – №2. – С. 6-9.
5. Литвинов С.А., Алекперов И.Д. Проблемные аспекты реализации кибербезопасности в XXI веке // Интеллектуальные ресурсы – региональному развитию. – 2020.
6. «Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности. «Кибербезопасность» [Электронный ресурс]. –

URL: https://www.kaspersky.ru/resourse-center/definitions/what-is-cybersecurity(Дата обращения 09.04.2021 г.).

7. «Мой-сервис-гид Кибербезопасность» - путеводитель в области ремонта техники. «Кибербезопасность».[Электронный ресурс]. – URL: https://www.my-cervice-guide.ru/press-center/articles/advices-and-instructions/235 (Дата обращения 09.04.2021 г.)

8. «Cyberlininka» - научная электронная библиотека. «Кибербезопасность».[Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/primenenie-metodov-glubokogo-obucheniya-v-zadachah-kiberbezopasnosti-chast-2 (Дата обращения 09.04.2021).

9. «RU-SCIENCE» – научная электронная библиотека [Электронный ресурс]. – .URL: https://ru-science.com/ru/kategorii-okso/stati-pro-informacionnuyu-bezopasnost (Дата обращения 09.04.2021 г.)

10. «Cisco» – мировой лидер в области информационных технологий и сетей [Электронный ресурс].– URL: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (Дата обращения 09.04.2021 г.).