УДК 004.9

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

Грачева Е.А.

Студент

Нижегородский государственный педагогический университет им. Козьмы Минина (Мининский университет),

Нижний Новгород, Россия

Поначугин А.В.

Кандидат экономических наук, доцент

Нижегородский государственный педагогический университет им. Козьмы Минина (Мининский университет),

Нижний Новгород, Россия

Аннотация: С развитием информационных технологии и перехода от индустриального общества к информационному, люди столкнулись с таким понятием как кибератаки. Они могут быть направлены как на обычного пользователя сети интернет, компанию, а иногда ещё серьезнее, для нанесения ущерба основным политическим и государственным институтам, что говорит о масштабности данной проблемы.

Актуальность данной темы обусловлена резким ростом количества кибератак на различные учреждения, особенно в период пандемии 2020 года.

Цель работы – рассмотреть основные современные категории кибератак.

Научная новизна – предложен комплекс мер, направленных на снижение киберугроз, с учетом современных требований кибербезопасности.

Ключевые слова: кибербезопасность, киберпреступление, мошенники, информация, защита.

CYBER SECURITY PROBLEMS IN THE MODERN WORLD

Gracheva E.A.
Student
Nizhny Novgorod State Pedagogical University. Kozma Minin (Minin University), Nizhny Novgorod, Russia

Ponachugin A. V.
PhD in Economics, Associate Professor
Nizhny Novgorod State Pedagogical University. Kozma Minin (Minin University), Nizhny Novgorod, Russia

Abstract: With the development of information technology and the transition from an industrial society to an information society, people are faced with such a concept as cyberattacks. They can be aimed both at an ordinary Internet user, a company, and sometimes even more seriously, to damage the main political and state institutions, which indicates the magnitude of this problem.
The relevance of this topic is due to a sharp increase in the number of cyber attacks on various institutions, especially during the 2020 pandemic.
The purpose of this work is to consider the main modern categories of cyber attacks.
Scientific novelty - a set of measures was proposed to reduce cyber threats, taking into account modern cyber security requirements.

Key words: cyber security, cybercrime, fraudsters, information, protection.

Информационные технологии всё глубже стали проникать в жизнь современного человека и это несомненно приносит свои плоды. Внедрение информационных технологий идет на пользу обществу и упрощает жизнь.[5] Актуальность в настоящее время приобрела проблема, связанная с образованием в период пандемии. Но она решилась с помощью организации дистанционного

обучения.[4] К сожалению, в мире всегда были люди, которые ищут способы получить выгоду незаконным путем и каждый из нас может столкнуться с одним из них. Киберпреступники среди нас и этот факт нельзя игнорировать, потому что каждый из нас может стать жертвой интернет-мошенников и столкнуться с проблемой потери собственных сбережений, утечки или уничтожения личной информации, так же есть вероятность быть подвергнутым шантажу.

Цифровизация – это один из глобальных трендов современной эпохи. [13] Киберпреступность представляет собой растущую угрозу для экономики любой страны и их планов по цифровой трансформации.

Ежегодно Check Point Research – компания, работающая в сфере IT-безопасности, анализирует киберинциденты за предыдущий год, чтобы собрать ключевые сведения о глобальном ландшафте киберугроз. В Годовом отчете по кибербезопасности за 2020 год представлены следующие данные по киберинцидентам за 2019 год (таблица 1). [17]

Таблица 1 – Категории кибер-атак, %

Категории кибер-атак	В мире	Европа, Ближний восток, Африка	Америка	Страны АТР
Крипто-майнеры	38	38	33	47
Ботнеты	28	23	22	30
Мобильные мошенничества	27	26	24	34
Банковские мошенничества	18	15	14	20
Хакеры	18	15	13	18
Программы-вымогатели	7	7	5	8

С ростом популярности облачных вычислений и подключенных к сети смартфонов не секрет, что существует больше способов вторгнуться в организацию. Когда-то укрепленный периметр сети теперь размыт и уязвим для кибератак, и злоумышленники об этом хорошо осведомлены.

Если сделать общий вывод из 2019 года, так это то, что ни одна организация, большая или маленькая, не застрахована от разрушительной кибератаки. Кибер-эксплойты стали более изощренными, иллюзорными и целенаправленными, чем когда-либо прежде. Учитывая, что уровень киберпреступности, по оценкам, составил 1,5 триллиона долларов США в 2018 году, чтобы ориентироваться в сегодняшнем сложном ландшафте киберугроз, требуется комплексная кибербезопасность. [17]

Киберпреступление — это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. [8] Киберпреступление отличается от обычного преступления тем, что оно может совершаться с большей скоростью и легкостью, хотя это зависит от сравнения конкретных преступлений этих двух видов.

Цели:

• экономическая – наиболее распространенная цель мошенничества, принесение ущерба кампании либо же отдельного физического лица посредством кражи денег, либо конфиденциальной информации с целью овладения материальными благами;

• политические – нанесение ущерба основным политическим и государственным институтам которое повлечет за собой негативное влияние на систему властных отношений и доверия к власти;[14]

• идеологические – распространение идей для приобщения людей к разным идеологиям и привлечения для вступления в ряды, например, террористических или националистических группировок.

Действию киберпреступников могут быть подвержены как организации, государственные институты, так и обычные граждане. Мошенники разными способами пытаются добиться своих целей и различают несколько типов кибератак:[3]

• кража данных банковских карт – один из самых распространенных способов получения денежных средств, практически напрямую;[2]

• кража и продажа корпоративных данных – более сложная схема, где перед злоумышленником стоит уже две задачи: украсть, продать;

• кража с использованием личных данных – перед мошенником так же стоит две цели, как и в предыдущем пункте;

• кибершантаж – одна из более затруднительных схем для осуществления, после кражи личных данных злоумышленник требует деньги либо же услугу для предотвращения кибератаки.[11]

С киберпреступником может столкнуться каждый. Всё чаще можно услышать в новостях или от знакомых, увидеть рекламный баннер на улице о том, что телефонные и интернет-мошенники всё больше стали проникать в жизнь обычного человека и что их стоит опасаться. Мошенники вводят в заблуждения людей, прибегая к особенностям психологии личности, представляясь другим лицом или представителем организации, которому, казалось бы, можно доверять.[7] Так же часто мошенники используют вирусные программы для похищения, либо уничтожения данных. Киберпреступления направленные на какую-либо организацию могут прекратить работу компьютеров, системы позволяющей предоставить интернет-услуги своим клиентам, такие киберпреступления называют атакой отказа в обслуживании.

По данным исследований проведенных в 2019 году проведенных среди детей и подростков, можно сделать вывод о том, что важным фактором, который увеличивает вероятность кибератак, является несоблюдения в основной части подростками простых правил по безопасности в интернете.[16] Больше половины опрошенных сказали о том, что знакомятся с новыми людьми в социальных сетях, почти 40% отметили, что отправлять им сообщения может кто угодно, ограничений не стоит. [7] Многие ли задумываются о конфиденциальности. Далеко не многие задумываются о конфиденциальности. Распространение излишней информации в интернете, несоблюдение правил

хранения паролей. Стоит ли говорить о том, что молодежь нужно обучать поведению в интернете, но ведь и не каждый взрослый знает эти простые правила.[10]

Так как же себя уберечь от кибератак? Кибербезопасность – это воплощение всех мер защиты сетей, приложений и устройств.[6] Кибербезопасность подразумевает сохранение свойств безопасности ресурсов организации или обычных пользователей, направлена против киберугроз. Кибербезопасность является необходимым условием развития информационного общества.[16]

Выше были рассмотрены некоторые ошибки рядовых интернет-пользователей, так же можно отметить, что люди часто не обращают внимания на то, что домен присланной на почту ссылки не совсем похож на тот, который он привык видеть, что может привести к утечке данных после всего лишь одного клика.[9] Или же часто пользователи спокойно привязывают свою банковскую карту сомнительным интернет-магазинам, в таком случае можно попрощаться со своими сбережениями. Казалось бы, это всё очевидные вещи и каждый про себя подумает «я на такое точно не попадусь», но никогда нельзя забывать о бдительности. Несколько советов для снижения вероятности и повышение защиты от кибератак:

• стоит использовать только лицензионное ПО и своевременно его обновлять;

• антивирусные средства защиты помогут избежать проникновения вредоносных программ;

• использование надежных паролей, состоящих из большого количества символов, а также использование двухфакторной аутентификации ограничит доступ к электронной почте;[12]

• резервное копирование позволит сохранить данные даже при условии, что мошенники решили их уничтожить.

Любая кампания несет большую ответственность за сохранность данных своих клиентов. Способы защиты:

• инструктажи по информационной безопасности для каждого из работников компании;

• разъяснения клиентам порядка действий при подозрении в мошенничестве;

• регулярное напоминание клиентам о правилах безопасности работы в интернете;

• разъяснение клиентам методов атак и способов защиты.[15]

С развитием информационного общества мы всё чаще стали сталкиваться с проблемой информационной безопасности. [1] Киберпреступники, мошенники сети интернет среди нас и нельзя об этом забывать, нужно всегда быть бдительным иначе маленькая неаккуратность может привести к глобальным последствиям. Большинство уязвимостей в системе безопасности создают сами люди. Поэтому стоит задуматься и придерживаться простых правил, которые были рассмотрены выше. Обеспечение защиты от киберпреступлений может занять довольно продолжительное время, но всегда того стоит.

Библиографический список:

1. Афанасьев С. В. Обоснование актуальности разработки субстратно-атрибутивной модели информационной культуры в рамках философии культуры // Вестник Мининского университета. – 2020. – Т. 8. – № 3. – С. 10. [Электронный ресурс]. — Режим доступа — URL: https://vestnik.mininuniver.ru/jour/article/view/1125/800 (дата обращения 09.10.2020).

2. Багдеева В. А. Проблемы международной киберпреступности // Актуальные проблемы российского права. – 2009. – № 3(12). – С. 564-572.

3. Бондарь В. В. Киберпреступность – современное состояние и пути борьбы // Юридические записки. – 2013. – №2 – с.98 [Электронный ресурс]. —

Режим доступа — URL: https://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby/viewer (дата обращения 09.10.2020).

4. Васенин В. А. Информационная безопасность и компьютерный терроризм. [Электронный ресурс]. — Режим доступа — URL: www.crime-research.ru (дата обращения 09.10.2020).

5. Галатенко В. А. Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.

6. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.: ил.

7. Дети в интернете 2020. [Электронный ресурс]. — Режим доступа — URL: https://clck.ru/RV4QX (дата обращения 12.10.2020).

8. Интернет преступность : моногр. / Р.И. Дремлюга. –. Владивосток: Изд-во Дальневост. ун-та, 2008. – 240 с.

9. Информационная безопасность : учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

10. Как уберечь детей от опасностей интернета: правила поведения в сети. [Электронный ресурс]. — Режим доступа — URL: https://clck.ru/RV3rU (дата обращения 12.10.2020).

11. Киберпреступления: причины, виды, формы, последствия, направление противодействия. // Юристъ-Правоведъ, 2019, №4, с. 79 [Электронный ресурс]. — Режим доступа — URL: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-suschnost-i-obschaya-harakteristika (дата обращения 14.10.2020).

12. Крат Ю.Г. Основы информационной безопасности. – Хабаровск: ДВГУПС, 2008. – 112 с.

13. Самерханова Э.К., Балакин М.А. Подготовка руководителей профессиональных образовательных программ к работе в условиях цифровой среды вуза // Вестник Мининского университета. – 2020. – Т. 8. – №2. – С. 4.

[Электронный ресурс]. — Режим доступа — URL: https://vestnik.mininuniver.ru/jour/article/view/1084/777 (дата обращения 14.10.2020).

14. Селиванов Н. Проблемы борьбы с компьютерной преступностью // Законность. – 1993. – № 8. – С. 36-40.

15. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.

16. Чугунов А. В. Развитие информационного общества: теории, концепции и программы: Учебное пособие. – СПб.: Ф-т филологии и искусств СПбГУ, 2007. – 81 с.

17. Cyber security report 2020. [Электронный ресурс]. — Режим доступа — URL: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf (дата обращения 13.10.2020).

Оригинальность 75%