УДК 004.056 DOI: 10.26200/GSTOU.2023.40.98.015

КИБЕРБЕЗОПАСНОСТЬ, КИБЕРАТАКИ И СПОСОБЫ ЗАЩИТЫ

© Х.А. Исраилова [1], С.М. Саралиева [2], Т.С. Мажетова [3]

[1] к.т.н., доцент кафедры «Технология и дизайн», Чеченский государственный педагогический университет, г. Грозный, Россия

[2] студент бакалавриата по направлению «Технологическое образование и образовательная робототехника»,

Чеченский государственный педагогический университет, г. Грозный, Россия

[3] студент бакалавриата по направлению «Технология и дополнительное образование (предпринимательская деятельность)»

Чеченский государственный педагогический университет, г. Грозный, Россия

Аннотация. *В статье поднята проблема кибербезопасности, так как в современном мире компании и простые пользователи сталкиваются с различными кибератаками данных и цифровых операций. Эти атаки могут быть внутренними, вызванными сотрудниками или подрядчиками, или внешними, вызванными киберпреступниками, государствами или даже собственными клиентами. Во всем мире растет количество инцидентов, связанных с кибератаками, но продолжают сохраняться ошибочные представления, в том числе представление о том, что такое кибербезопасность.*

Ключевые слова: *кибербезопасность, данные, защита, атака.*

В настоящее время, когда количество устройств быстро растет, обеспечение безопасности этих устройств является наиболее важной темой. Обеспечение безопасности устройств на самом деле означает обеспечение безопасности наших данных.

Учреждение, которое не может предоставить безопасность тех или иных данных, всегда сталкивается с опасностью потери денег, репутации, времени и ресурсов.

Кибербезопасность – это совокупность усилий, направленных на предотвращение доступа, повреждения или захвата неавторизованными лицами сетевых систем и данных [2].

Принятие мер предосторожности является важнейшей задачей как личной, так и корпоративной, а также государственной.

Каждая информация, от изображений, которыми мы делимся в Интернете, до нашей личной информации, является частной областью, которая нас идентифицирует. Вместе с этим у нас есть информация о здоровье и финансах. Это в первую очередь данные, которые необходимо защищать.

Рассмотрим основные методы кибератак и способы защиты от них.

Вирусы и другие вредоносные программы. Вирусы, которые сначала создавал старшеклассник, чтобы подшутить над своими друзьями, сегодня могут использоваться для самых разных целей. Некоторые из них созданы только для нанесения вреда, другие предназначены для получения доступа к личным данным, взлома наших систем или получения выкупа.

В любом случае сообщения, ссылки, электронные письма от людей, которые нам не знакомы, могут сделать нас жертвой этой атаки. Кроме того, установка программ, загруженных или предоставленных из источников, о которых мы не знаем, на наших компьютерах и других устройствах может сделать нас мишенью для этих атак.

Интернет – это название, данное системе, в которой люди обмениваются данными, посредством которых они общаются друг с другом по сети [1]. Подключившись к проводным и беспроводным сетям Интернета, мы можем выполнять любые операции, которые хотим, онлайн. Злоумышленники, которые хорошо знают структуру этих сетей, могут перехватить наши данные, используя множество различных методов.

DDoS-атаки. DDoS (Distributed Denial of Service) – это атаки, которые осуществляются по логике, когда большое количество разрозненных и контролируемых компьютеров (сеть ботнетов) отправляет пакеты данных в определенную точку или запрашивает соединение.

Одновременная передача запроса на подключение или передача данных ресурсу, значительно превышающему его пропускную способность, приведет к отключению сервера, к которому подключен этот ресурс. Таким образом, веб-сайт или сети становятся недоступными для других посетителей, поскольку неработающий сервер не может выполнять трансляцию.

DDoS-атаки обычно совершаются с целью нанесения ущерба веб-сайтам, банковским системам, биржам и другим системам безопасности. Одним из основных способов защиты от этой атаки является использование Cloudflare. Серверы Cloudflare относительно менее подвержены этим атакам из-за их большого количества по всему миру и очень высокой пропускной способности. Опять же, мы можем добиться меньшего воздействия, поддерживая высокие значения пропускной способности текущего сервера [3].

SQL Injection. Метод SQL injection – это метод, используемый для проникновения в базы данных. Уязвимости, возникающие в наших базах данных, обнаруживаются и используются с помощью форм на веб-сайтах, а доступ к конфиденциальной информации, хранящейся в базах данных, такой как личные данные, данные кредитной карты, адрес, телефон, учетные данные, может быть доступен.

Обеспечение того, чтобы наша база данных и версии PHP были последними и актуальными, – это шаги, которые относительно защитят от проникновения посторонних лиц.

BruteForce Attack. Процесс поиска имени пользователя и пароля методом проб и ошибок называется атакой методом перебора. С помощью современных мощных компьютеров и некоторого программного обеспечения можно очень быстро попытаться найти пароль, который использовал человек, попробовав множество комбинаций паролей. Обычно это программное обеспечение начинает с того, что сначала пробует наиболее часто используемые пароли. Затем другие комбинации пробуются индивидуально, выбирая их из специально созданных файлов паролей. Этот процесс выполняется так быстро, что пароль будет получен в кратчайшие сроки. Одним из самых основных способов защиты от этой атаки является установка паролей, состоящих из цифр и символов верхнего регистра, а также множества различных комбинаций.

Кроме того, еще один используемый метод – автоматическое отключение системы на некоторое время после определенного количества попыток ввода неверного пароля.

Виды кибербезопасности:

– Сетевая безопасность – предотвращение манипулирования компьютерными сетями, в которых выполняются важные операции, вредоносными программами и вредоносными лицами, подпадает под это покрытие. Такие сети должны быть организованы таким образом, чтобы они были максимально закрытыми.

– Информационная безопасность – это один из видов кибербезопасности, который имеет первостепенное значение в современных условиях.

– Безопасность платежей – это меры безопасности, направленные на безопасное осуществление платежей за предоставленную услугу или проданный продукт. Несмотря на то, что в этом отношении было принято много мер предосторожности, многие проблемы все еще возникают.

Наиболее эффективные меры кибербезопасности:

– Использование современного антивирусного программного обеспечения.

Антивирусное программное обеспечение основано на том, что все вредоносные программы, распространяющиеся в Интернете и сообщаемые людьми, регистрируются в базе данных и блокируются. Обновленное антивирусное программное обеспечение в значительной степени защитит систему. Доступно множество антивирусных программ, платных или бесплатных. Включение в систему антивирусной программы, которую пользователь определит из них, в значительной степени поможет защитить ее.

– Использование аппаратного и программного обеспечения брандмауэра

Программное обеспечение, называемое брандмауэром, обычно работает интегрированным и комбинированным образом с антивирусными программами. Но есть также оборудование брандмауэра, используемое для сложных сетей. Эти специальные устройства защищают сетевую безопасность от вредоносных программ и вредоносных приложений. Вместо этих

систем, которые стоят довольно дорого, можно использовать программное обеспечение брандмауэра по относительно более доступной цене.

– Обновление операционных систем

Наличие обновленной операционной системы, которую использует пользователь, также будет означать, что он более защищен от кибератак. Каждое новое обновление повышает безопасность операционных систем, предотвращая появление всех вредоносных программ, появившихся в последнее время. Если пользователь использует пиратское программное обеспечение, он обычно отключает обновления системы. В таком случае он становится довольно уязвимым для кибератак. По этой причине использование лицензионного программного обеспечения и поддержание систем в актуальном состоянии были бы самыми разумными шагами.

– Использование программы паролей

Чем лучше пароль, который создается для учетной записи пользователя, тем труднее манипулировать этой учетной записью другим. Обычно пользователи создают пароли, которые легко запомнить. Именно в этом заключается тактика программ для проверки паролей. Если пользователь создает разные пароли для каждой учетной записи и меняет их через определенные промежутки времени, маловероятно, что его системы будут скомпрометированы кем-либо еще.

Запоминание паролей – довольно сложный процесс. По этой причине можно использовать программы паролей. Программа паролей, которую будет использовать пользователь, сохранит все его существующие пароли, и вы сможет вытащить их оттуда, когда ему это понадобится.

– Получение услуги от компании, занимающейся кибербезопасностью

Существует множество частных организаций, предоставляющих услуги кибербезопасности. Эти организации подготавливают наши системы к возможным угрозам, устанавливают необходимое программное обеспечение и обеспечивают нашу осведомленность, а также проверяют нашу систему в определенные периоды, чтобы мы могли обнаруживать вредоносное ПО и принимать меры предосторожности. Необходимо учитывать проблему кибербезопасности, которая является одной из самых основных потребностей сегодняшнего дня, и предпринять шаги в этом направлении. Компании также могут иметь собственных специалистов по кибербезопасности. Специализация в области кибербезопасности – это позиция, которую, как считается, компании откроют довольно широко в будущем.

Ключевыми поставщиками решений в сфере кибербезопасности являются американские компании Cisco, IBM Corporation и Palo Alto Networks, а также японская Trend Micro. На их долю приходится около 41,60% рынка, а оставшаяся часть принадлежит многочисленным вендорам по всему миру, среди которых наиболее известными являются:

- в США – Fortinet, CyberArk, F5 Networks, FireEye, Forcepoint, Imperva, Juniper Networks, McAfee, Microsoft, Oracle, Proofpoint, Qualys, Rapid7, RSA Security, Splunk, SentinelOne, NortonLifeLock и Microsoft;
- в Европе – AVG Technologies (Чехия), F-Secure (Финляндия), Micro Focus и Sophos со штаб-квартирами в Великобритании;
- в Израиле – Check Point Software;
- в Индии – Wi-Jungle и Aristi Labs [4].

В 2021 году несколько крупных инфраструктурных компаний стали жертвами дорогостоящих и знаковых кибератак. Взлом центра управления газопроводом Colonial Pipeline в США привел к остановке транзита газа и выплате $5 млн. вымогателям, атака на бразильскую компанию JBS – крупнейшего производителя мяса в мире – привела к остановке несколько заводов и выкупу в $11 млн., а страховая компания CNA Financial заплатила хакерам $40 млн. за расшифровку заблокированных злоумышленниками данных.

Компания Gartner прогнозирует, что к 2025 году 45% организаций столкнутся с атаками на свои цепочки поставок программного обеспечения, что в три раза больше, чем в 2021 году. Правительства во всем мире наращивают свои усилия по защите персональных данных своих граждан. Также Gartner прогнозирует, что в 2023 году 65% населения мира будут иметь свои персональные данные, защищенные современными правилами конфиденциальности, по

сравнению с 10% в 2020 году. Также по оценкам Gartner, расходы на кибербезопасность достигнут $188,3 млрд. в 2023 году и превысят $260 млрд. во всем мире к 2026 году [8].

В России же рынок кибербезопасности по результатам 2021 года оценивается в 185,9 млрд руб. При этом совокупная доля услуг составляет 27% всего объема рынка, а поставки средств защиты информации, в том числе программных, – 73% [7].

По итогам событий 2022 года индустрия кибербезопасности подошла к необходимости переосознания основных принципов построения защиты и реагирования на угрозы в масштабах бизнеса, отраслей и страны, и в 2023 году кибербезопасность как индустрию ожидает период активной пересборки с большей ориентированностью на практику результативной защиты.

Киберугрозы уже представляют собой огромную проблему для бизнеса, и по мере того, как операции продолжают переходить на цифровые модели, есть все признаки того, что эти угрозы будут продолжать расти. Только программы-вымогатели ежегодно наносят ущерб в десятки миллиардов долларов по всему миру. Этому росту способствуют технически подкованные киберпреступники. Те же самые передовые технологии, которые используются законными компаниями, также используются преступными группировками и даже странами-изгоями. Используя искусственный интеллект и огромные вычислительные мощности, злоумышленники совершенствуют свои возможности в области вредоносных программ, опережая эффективность многих традиционных решений для защиты от вредоносных программ и делая атаки нулевого дня более разрушительными.

Следовательно, можно сделать вывод, что проникновение на сайты, подверженные риску в Интернете, установка пиратского программного обеспечения, использование общих и простых для запоминания паролей – самые большие ошибки, которые можно совершить с точки зрения кибербезопасности.

ЛИТЕРАТУРА

1. Алисултанова Э.Д. Профориентационная школьная лаборатория по основам кибербезопасности в сфере интернет вещей (IOT)// Алисултанова Э.Д., Хаджиева Л.К., Исаева М.З. // Вестник ГГНТУ. Гуманитарные и социально-экономические науки. 2019. № 4 (18). С. 51-58.

2. Бусленко, Т. О. Кибербезопасность. Виды киберугроз и контрмер / Т. О. Бусленко, Е. О. Бусленко. Текст: непосредственный // Юный ученый. 2023. № 3 (66). С. 89-93.

3. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2023. 161 с.

4. Кибербезопасность: кратные возможности для роста. Режим доступа: https://gazprombank.investments/blog/market/cybersecurity/

5. Концепция стратегии кибербезопасности Российской Федерации. Режим доступа: http://www.council.gov.ru/ 2. media/files/41d4b3dfbdb25cea8a73.pdf

6. Обзор кибербезопасности на финансовом рынке. Режим доступа: https://kapital.kz/tehnology/115497/obzor-kiberbezopasnosti-na-finansovom-rynke.html

7. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы. Режим доступа: https://www.csr.ru/upload/iblock/13f/ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf

8. Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23. Режим доступа: https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

CYBERSECURITY, CYBERATTACKS AND METHODS OF PROTECTION

© H.A. Israilova, S.M. Saralieva,T.S. Mazhetova
Chechen State Pedagogical University, Grozny, Russia

Abstract: *The article raises the issue of cybersecurity, as in the modern world companies and ordinary users face various cyber-attacks of data and digital operations. These attacks can be internal, caused by employees or contractors, or external, caused by cybercriminals, states, or even their own customers. The number of incidents related to cyberattacks is growing all over the world, but misconceptions continue to persist, including the idea of what cybersecurity is.*

Keywords: *cybersecurity, data, protection, attack.*