МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.23670/IRJ.2023.137.39

КРАТКАЯ ИСТОРИЯ ЭВОЛЮЦИИ КИБЕРАТАК

Научная статья

Васильев А.[1, *]
[1] ORCID : 0009-0008-9909-2385;
[1] ScienceSoft, Минск, Беларусь

* Корреспондирующий автор (alexey_vasilyev96[at]mail.ru)

Аннотация

Использование интернета выросло в геометрической прогрессии за последние десятилетия, и как отдельные лица, так и компании осуществляют множество ежедневных транзакций в киберпространстве. Пандемия коронавируса (COVID-19) лишь ускорила этот процесс. В результате широкого использования цифровой среды, традиционные преступления также переместились в цифровое пространство. Новые технологии, такие как облачные вычисления, интернет вещей (IoT), социальные медиа, беспроводная связь и криптовалюты, вызывают опасения в области кибербезопасности. Недавно киберпреступники начали предлагать кибератаки как услугу (CaaS) для автоматизации кибератак и увеличения их разрушительного эффекта. Злоумышленники выявляют и используют уязвимости, существующие в аппаратном обеспечении, программном обеспечении и коммуникационных уровнях. Различные виды киберугроз включают в себя распределенные атаки (DDoS), фишинг, вредоносные программы, программы для вымогательства и многое другое. Данная работа поможет разобраться в эволюции киберугроз с момента появления первых компьютеров и ставит своей основной целью показать стремительную динамику в развитии вредоносного ПО и важность развития кибербезопасности для любого бизнеса, организации и отдельного человека.

Ключевые слова: кибербезопасность, кибератаки, киберугрозы, сетевая безопасность.

A BRIEF HISTORY OF THE EVOLUTION OF CYBERATTACKS

Research article

Vasilyev A.[1, *]
[1] ORCID : 0009-0008-9909-2385;
[1] ScienceSoft, Minsk, Belarus

* Corresponding author (alexey_vasilyev96[at]mail.ru)

Abstract

The use of the Internet has grown exponentially in recent decades, with individuals and businesses both conducting many daily transactions in cyberspace. The coronavirus (COVID-19) pandemic has only accelerated this process. As a result of the widespread use of the digital environment, traditional crime has also moved into the digital space. New technologies such as cloud computing, the Internet of Things (IoT), social media, wireless communications, and cryptocurrencies have raised cybersecurity concerns. Recently, cybercriminals have begun offering cyberattacks as a service (CaaS) to automate cyberattacks and increase their disruptive effect. Attackers identify and exploit vulnerabilities that exist in hardware, software and communication layers. Different types of cyber threats include distributed denial of service (DDoS) attacks, phishing, malware, ransomware, and more. This article will help to understand the evolution of cyber threats since the first computers were invented and its main aim is to show the rapid dynamics in the development of malware and the importance of cybersecurity development for every business, organization and individual.

Keywords: cybersecurity, cyberattacks, cyber threats, network security.

Введение

Интернет, возникший как среда для коммуникации и обмена информацией, быстро повлиял на экономику и бизнес во всем мире. 21 век стал периодом постиндустриального перехода и развития постинформационного общества, в котором все процессы неразрывно связаны с Интернетом. Сегодня люди с разных концов земного шара могут общаться мгновенно с помощью высокоскоростных соединений. Благодаря глобальной сети Интернет между государствами и континентами сформировалась крепкая связь в экономических, политических и социокультурных областях. Интернет имеет три основных составляющих: компьютеры, пользователи и сети [1]. Эволюция сетей идет в ногу с постоянно меняющимися компьютерными технологиями и сегментами пользователей, обладающим различными потребностями и способностями. Однако развитие и широкое использование сетевых технологий также привело к серьезным проблемам безопасности. Именно поэтому сейчас предпринимаются активные попытки создать кибербезопасную среду для защиты данных различных учреждений, организаций и физических лиц [2].

Слово «кибер» означает принадлежность к чему-то, связанному с кибернетикой (киберспорт, киберпреступность, кибербезопасность и т.д.). Для начала, внесем ясность в некоторые понятия и определения. Согласно определению компании Gartner:

Кибербезопасность (англ. – cybersecurity) – это сочетание людей, политик, процессов и технологий, используемых предприятием для защиты своих киберактивов. Подмножества кибербезопасности включают ИТ-безопасность,

безопасность Интернета вещей (IoT), информационную безопасности (ИБ) и безопасность операционных технологий (OT) [3].

По аналогии с классическим определением информационной безопасности в стандарте под кибербезопасностью фактически понимают свойство защищенности активов от угроз триады безопасности – конфиденциальности, целостности и доступности, но в некоторых абстрактных рамках – киберпространстве.

Киберпространство (англ. – cyberspace) определяется как комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет или других коммуникационных структур посредством ИКТ [4], [5].

В общем кибербезопасность обеспечивает безопасность виртуальной жизни в киберсетях. Основная цель кибербезопасности – обеспечение безопасности данных физических лиц и организаций в Интернете. Игнорирование данного вопроса может вызвать серьезные проблемы. Например, злоумышленник может внедриться в корпоративную систему по сети и завладеть конфиденциальными данными [6] или украсть учетные данные пользователей, такие как данные кредитных карт или пароли пользователей. Такие атаки могут причинить финансовый ущерб физическим лицам, организациям, крупным компаниям и даже государственным органам. Согласно последним исследованиям, кибератаки обходятся мировой экономике в миллиарды долларов ежегодно. В наши дни хакерство – это уже не просто единичные атаки со стороны злоумышленников-одиночек, а крупный бизнес, который поддерживается и зачастую финансируется крупными компаниями и правительствами. Практически каждая кибератака может быть предотвращена только при наличии грамотной Политики безопасности в организации [7].

С учетом вышеизложенной информации, в этой статье объясняется история киберпреступности и ключевые аспекты кибербезопасности, а также обсуждаются причины увеличения числа кибератак и изменения ландшафта киберугроз с технической и нетехнической точек зрения.

Ландшафт угроз (threat landscape) – совокупность выявленных и потенциальных киберугроз для определенной отрасли, группы пользователей, конкретного периода времени и так далее.

Методы и принципы исследования

В статье был использован публикационный метод прогнозирования, прогнозирование на основе метода экспертных оценок и методы экстраполяции. Исследование проводилось следующим образом:

1) автором были собраны и изучены источники (монографии, научные статьи, международные стандарты, материалы из Интернета и т.д.);

2) затем выделены базовые этапы в развитии истории киберпреступлений и кибербезопасности;

3) при построении прогнозов учитывалось экспертное мнение ведущих компаний в области кибербезопасности в виде аналитических отчетов. Также использовались международные стандарты в области ИБ;

4) автор использовал метод экстраполяции: таким образом можно экстраполировать тенденцию с развитием определенного вида киберпреступлений на ближайшие годы;

5) интуитивные методы автор применил в попытке выразить в этой научной публикации свой собственный опыт работы и исследований в ИБ-сфере.

Цель работы:

· обобщить имеющиеся литературные данные по истории киберпреступлений;

· выделить наиболее опасные кибератаки на сегодня, показать вектора атак, наиболее вероятные угрозы ИБ и тренды их развития;

· показать, какие методы противодействия угрозам и атакам используют сегодня специалисты в области кибербезопасности (превентивные и проактивные методы защиты);

· показать связь практических методов кибербезопасности с методологией, изложенной в международных стандартах в этой области.

История киберпреступности и кибербезопасности

Существуют разные определения кибербезопасности, выше были обозначены наиболее употребимые определения согласно международным стандартам.

Кибербезопасность направлена на обеспечение максимальной защиты цифровых данных от несанкционированного доступа, изменения или раскрытия на протяжении всего жизненного цикла продукта информационных технологий [8].

Информационная безопасность представляет собой практику предотвращения несанкционированного доступа, использования, раскрытия, изменения, просмотра, записи или уничтожения физической или электронной информации [9]. Основная цель информационной безопасности – защитить конфиденциальность, целостность и доступность данных.

Сетевая безопасность направлена на обеспечение конфиденциальности, целостности и доступности компьютерных сетей и данных, передаваемых по средствам связи [10]. С другой стороны, кибербезопасность – это практика защиты компьютеров, серверов, мобильных устройств, электронных систем, компьютерных сетей и данных от злонамеренных атак. В то время как защита данных, информационная безопасность и сетевая безопасность направлены на предотвращение несанкционированного доступа, использования, изменения или уничтожения хранимых данных или данных в пути, кибербезопасность имеет гораздо более широкую область применения, охватывающую потоки информации от начала до конца.

Киберпреступность ведет свою историю со второй половины 20-го века. 30 или 40 лет назад было намного легче защищать данные в цифровом мире, потому что в цифровой среде было меньше машин, и атаки не были такими сложными, как сейчас.

Однако с течением времени технологические разработки позволили киберпреступникам создавать автоматизированные инструменты для запуска сложных кибератак. Кроме того, различные устройства и платформы (смартфоны, планшеты, устройства интернета вещей, облачные платформы, платформы социальных сетей и многие другие) получили доступ в Интернет [11]. Все эти факторы позволили киберпреступности сделать резкий рывок в развитии: от простых взломов компьютеров и сетей до сложных атак (как целевые кибератаки – APT), которые год от года обходятся мировой экономике в миллиарды долларов. Классификация киберпреступлений на протяжении десятилетий представлена в Таблице 1.

Таблица 1 - Классификация киберпреступлений по десятилетиям

DOI: https://doi.org/10.23670/IRJ.2023.137.39.1

Период	Киберпреступления
1940-е	Годы без киберпреступлений
1950-е	Телефонный фрикинг
1960-е	Появление терминов «хаккинг» и уязвимость ПО
1970-е	Зарождение компьютерной безопасности
1980-е	Эволюция от ARPANET до Интернета
1990-е	Широкое распространение компьютерных вирусов и червей
2000-е	Стремительный рост Интернета
2010-е	Киберпреступники выявили несколько серьезных брешей в защите компьютерных систем
2020-е	Киберпреступления становятся целой индустрией

Первые компьютеры появились в начале 1940-х годов [12]. В то время не было Интернета и компьютерных сетей, появились первые большие ЭВМ, однако их возможности использования были крайне ограниченными. Поскольку не было обмена информацией между компьютерами, то не было даже такого понятия, как угрозы или атаки.

Телефонной фрикинг (взлом телефонных сетей или сетей мобильной связи) начинает появляться лишь в 1950-х годах. Телефонные фрики пытались использовать протоколы, применяемые в телефонных системах, чтобы совершать бесплатные звонки или уменьшить оплату за звонки. В то время нескольким телефонным компаниям не удалось предотвратить данный вид мошенничества.

В будущем аналогичные методы как для телефонного фрикинга, начали использоваться для взлома компьютерных систем. Термин «хакинг» для компьютерных систем впервые появился в 1960-х годах. В 1965 году была обнаружена первая уязвимость в машине IBM 7094 Compatible Time-Sharing System (CTSS) [13]. В 1967 году IBM наняла группу студентов для исследования их новейшего компьютера [12]. Студенты изучили язык компьютерной системы и получили доступ к различным ее частям. Этот пример доказал, что компьютерные системы имеют уязвимости, и этот случай стал первым примером этичной практики хакинга.

Основы кибербезопасности были заложены в начале 1970-х годов с проекта под названием «Сеть Проектов По Передовым Исследованиям» (ARPANET —англ. Advanced Research Projects Agency Network). Это была первая пакетно-коммутационная сеть до создания Интернета. В 1971 году Боб Томас создал первый вирус под названием «Creeper, который мог передвигаться по сети ARPANET [13]. После «Creeper» Рей Томлинсон создал«Reaper», который также мог передвигаться по ARPANET и удалять «Creeper» [14]. «Reaper» стал первым примером антивирусной программы. В 1979 году известного хакера Кевина Митника впервые арестовали за киберпреступления [13].

В 1980-х годах наблюдались несколько атак, связанных с компьютерами. Главным образом, в этом десятилетии широкое применение получили компьютерные вирусы. Термин «кибершпионаж» также начал использоваться в этот же период времени, так как значительно возросла угроза вмешательства государств в дела друг друга. В 1985 году Департамент обороны Соединенных Штатов Америки (США) создал руководство по компьютерной безопасности под названием «Критерии определения безопасности компьютерных систем» (TCSEC), который позднее был назван «Оранжевой Книгой» [15], [16]. TCSEC стал первым руководством по безопасности компьютерных систем.

В 1986 году немецкий хакер Маркус Хесс взломал системы правительств США, Восточной Азии и Европы [17]. Он смог получить доступ к 400 военным компьютерам. Взломанная информация включала в себя данные по новейшим аэрокосмическим технологиям, спутникам и авиации [18]. В это же время кибербезопасность становится одной из основных проблем для бизнеса. Первое коммерческое антивирусное программное обеспечение было выпущено в 1987 году. В 1990-х годах произошел огромный рост в развитии компьютерных систем и Интернета. Компьютерные вирусы и их различные версии стали очень популярны. В 1996 году были выпущены макровирусы. В конце 1990-х годов вирусы Melissa и ILOVEYOU заразили миллионы компьютеров в десятках стран [19]. В 1995 году компания Netscape представила протокол Secure Sockets Layer (SSL), который обеспечивал защищенные соединения пользователей через компьютерную сеть.

В 2000-х годах Интернет экспоненциально рос, а персональные компьютеры стали все более распространенными как на рабочих местах, так и в домашних хозяйствах. Широкое использование ПЭВМ повысило производительность, но также создало риски для безопасности многих пользователей. Другими словами, увеличение использования компьютеров также увеличило киберпреступность. Первая организованная группа хакеров появилась в начале 2000-х, и компьютерные черви и трояны стали часто использоваться для кибератак. Простого посещения зараженного веб-сайта было достаточно, чтобы заразиться вирусом без загрузки файлов. В 2004 году червь MyDoom был ответственен за распределенные атаки (DDoS) и получение удаленного доступа к конфиденциальным файлам [19]. В 2007 году троян Zeus просочился через спам и «загрузки браузера». Он был использован для кражи учетных данных банковских приложений, социальных сетей и других электронных аккаунтов.

В 2010-х годах киберпреступники выявили несколько уязвимостей в программном обеспечении и протоколах компьютерных сетей. Эти нарушения привели к потере миллионов долларов частными лицами и миллиардов долларов крупными компаниями ежегодно. В 2016 году вредоносное программное обеспечение Mirai использовало уязвимость устройства IoT для запуска атак DDoS [20]. Между 2010 и 2020 годами атаки, связанные с вымогательством, становились все более популярными. Например, вредоносная программа для вымогательства WannaCry зашифровала компьютерные данные на миллионах компьютеров и была задействована злоумышленниками в 150 странах по всему миру [21], [22], в то время как LockerGoga блокировал уже зараженные системы и причинил дополнительный ущерб на миллионы долларов [23]. В 2020 году вредоносная программа CovidLock зашифровала данные на устройствах Android и отказала пользователям в доступе к данным [24].

В 2020-х годах стало возможным взломать что угодно в цифровом мире. Некоторые профессиональные веб-сайты даже предоставляют автоматические приложения и инструменты для хакинга «как услугу». Своевременные и эффективные кибератаки могут привести к огромным потерям для компаний и принести гигантскую прибыль для своих организаторов. По этой причине крупные компании и государства все более активно инвестируют свои средства в кибербезопасность. Эволюцию развития кибератак на протяжении многих лет можно видеть в Таблице 2.

Таблица 2 - Эволюция развития кибератак

DOI: https://doi.org/10.23670/IRJ.2023.137.39.2

Кибератака	Год	Метод распространения атаки	Последствия
Атака Владимиром Левиным Citibank1	1994-1995	Неизвестно.	Похищены 10 млн долларов.
Melissa (вирус)	1999	Переход по ссылке из прикрепленного файла.	Миллиарды долларов были похищены по всему миру.
ILOVEYOU Worm3	2000	Переход по ссылке из прикрепленного файла.	Более 45 млн компьютеров были заражены вирусом.
MyDoom worm4	2004	Использование привлекательных заголовков для электронных писем и текстов.	Были запущены DDoS-атаки, предоставив возможность для удаленного доступа к миллионам компьютеров по всему миру.
Троян Zeus	2007	Рассылка спама с загрузками при посещении сайта.	Были украдены банковские данные и пароли для входа в почтовые ящики.
Червь Stuxnet	2010	Атака программируемого логического блока (PLC) с кражей исходного кода.	Злоумышленники заполучили контроль над промышленными процессами крупных предприятий.
Атака на USA Natural Gas Pipeline	2012	Получение доступа к конфиденциальной информации с помощью фишинга.	Кража данных по обеспечению безопасности.
Вредоносное ПО Mirai	2016	Была использована уязвимость устройств интернета-вещей	Начата крупная DDoS-атака на устройства по всему

		(IoT).	миру.
WannaCry Ransomware	2017	Была использована уязвимость в операционной системе Windows.	Жесткие диски тысяч компьютеров были зашифрованы, а данные похищены. Пострадали более 150 стран.
Троян Emotet	2018	Рассылка спама и фишинговых файлов.	Украдены данные о кредитных картах по всему миру.
MyFitnessPal	2018	Рассылка спама и фишинговых файлов.	Пострадали более 150 млн пользователей.
Атака на Magellan	2020	Рассылка спама и фишинговых файлов.	Кража данных о здоровье более 365,000 пациентов.
CovidLock Ransomware	2020	Использование статистики о COVID-19.	Данные андроид-устроиств были зашифрованы и к ним ограничили доступ.
Accellion Supply Chain	2021	Использование уязвимостей сторонних компаний-партнеров.	Кража конфиденциальной информации о крупных компаниях.
Kaseya Ransomware	2021	Использованы уязвимости нулевого дня.	Данные около 1500 компаний были скомпрометированы. Размер выкупа данных составил от $50,000 до $5 млн долларов каждый.

Кибербезопасность: актуальные угрозы на сегодня

Методы распространения атак меняются с течением времени. Уязвимости в аппаратном обеспечении, программном обеспечении и сетях, фишинговое мошенничество и методы социальной инженерии стали часто использоваться злоумышленниками. Эти атаки чаще всего распространяются с помощью скаченных файлов в браузере и вредоносных вложений в электронных письмах.

Кибератаки стали более сложными и опасными и даже появился новый вид – APT (англ. advanced persistent threat, «развитая устойчивая угроза») или «целевая кибератака». Данный вид атак является наиболее сложным и долговременным. Злоумышленники тщательно готовятся к проведению APT, долго выбирают и изучают «жертву», они могут месяцами находиться внутри периметра корпоративной сети. Предварительно хакеры могут использовать методы фишинга и социальной инженерии, старые учетные данные.

Эти атаки обходятся мировой экономике в миллиарды долларов ежегодно. Кроме того, новые устройства, такие как смартфоны и устройства IoT, увеличили потенциальное количество точек входа для кибератаки. Хакеры постоянно совершенствуют существующие инструменты для своих преступлений, создавая различные версии и используя новые варианты атак через доступ к смартфонам и устройствам IoT. Последние исследования показывают, что поддельные приложения, бэкдоры и банковские трояны становятся все более распространенными для мобильных устройств. Кроме того, увеличивается количество кибератак, связанных с социальными медиа, устройствами IoT, криптовалютой и облачными решениями.

Также происходит рост числа атак на системы промышленной автоматизации и АСУ. Вот последняя статистика подобных угроз и атак, полученная в Лаборатории Касперского:

• В первые шесть месяцев 2023 года на 34 процентах компьютеров АСУ были заблокированы вредоносные объекты (все угрозы).

• Во втором квартале 2023 года в мире этот процент достиг максимального с 2022 года значения за квартал – 26,8%.

• Показатель угроз за полугодие варьируется от 40,3% в Африке до 14,7% в Северной Европе.

• В странах – от 53,3% в Эфиопии до 7,4% в Люксембурге.

Основными источниками угроз являлись: Интернет (19,3% угроз заблокировано на компьютерах АСУ), почтовые клиенты (на 6% компьютерах АСУ), съемные носители (на 3,4% компьютерах АСУ) [27].

В последнее время во многих отраслях внедряются системы искусственного интеллекта и машинного обучения. Однако, эти передовые технологии также подвержены угрозам и атакам злоумышленников.

Ниже отметим основные типы атак на системы машинного обучения. Бывают атаки на алгоритм и на модель соответственно. Это атаки с уклонением, отравлением, троянскими программами, бэкдорами, перепрограммированием

и инференс-атаками. Приведем пример одной подобной атаки, чтобы было понятно, о чем вообще идет речь. Специалисты считают, что «уклонение» – это самая типичная атака на модель машинного обучения, выполняемая во время логического вывода. Некоторые вещи для человека воспринимаются нормальными, а вот модель машинного обучения их классифицирует ошибочно. К примеру, можно изменить отдельные пиксели на картинке перед загрузкой ее в систему, человек это даже не заметит, а вот система распознавания изображений уже не сможет классифицировать результат.

Очень много данных по таким видам атак, как «отравление модели». Что это означает? Существует четыре общих стратегии атаки отравления для изменения модели на основе возможностей злоумышленника. Это модификация меток, внедрение данных, модификация данных, логическое искажение.

Злоумышленники начали использовать и троянские атаки на модели машинного обучения. В чем смысл такой атаки? Дело в том, что многие компании, которые занимаются проблемами машинного обучения, не обучают модели с нуля, а берут уже существующие на рынке модели и дообучают их на своих сетах данных. Т.е. компании и специалисты просто загружают популярные модели из Интернета, в то же время хакеры могут в эти модели внедрить вредоносный код. В последнее время хакеры стали применять и бэкдоры (вредоносные закладки) в модели машинного обучения. Злоумышленники взламывают сервера и подменяют модели, которые там хранятся, на свои (с закладками) [28].

Отдельно необходимо упомянуть виды атак на блокчейн, так как они принципиально отличаются от обычных атак на компьютеры и сети. Приведем примеры атак на блокчейны с механизмом консенсуса PoW (Proof of Work):

1. «Атака 51%» – смысл атаки заключается в том, что если один (или несколько) участников сети получат большую часть «голосов», то он (они) смогут взять под контроль консенсус и включать в блокчейн нужные им данные.

2. Атака «Double-spending» – основной принцип атаки – потратить больше денег, чем есть у пользователя блокчейна. Для этого пользователь создает ряд транзакций с использованием одних и тех же монет.

3. «Атака Сибиллы» описывается ситуацией, когда один узел сети приобретает несколько «сущностей». Блокчейн не может различать физические машины, поэтому атакующий может попытаться заполнить сеть подконтрольными ему клиентами. Такая атака может привести дополнительно к уязвимостям, которые позволят реализовать угрозы «Атаки 51%» и «Double-spending». Также с её помощью фальсифицируют интернет-голосования или накручивают рейтинги.

4. DDoS – смысл атаки в пересылке огромного числа одинаковых запросов. Биткойн имеет встроенную защиту от атак типа «отказ в обслуживании».

Взлом криптографии. Подобные опасения базируются на теоретических исследованиях ученых в области квантовой криптографии. Есть предположение, что квантовые компьютеры будут способны взламывать даже самые стойкие алгоритмы. Поэтому уже в настоящее время ведутся исследования, цель которых – повышение устойчивости блокчейн-проектов к атакам, которые будут исходить от квантовых компьютеров [29].

Противодействие киберугрозам на современном этапе

В статье описана история эволюции кибератак, а также рассказано о современном состоянии ландшафта киберугроз. Возникает закономерный вопрос: как этому противостоять? Конечно же, тема построения систем кибербезопасности столь обширна, что является предметом для отдельной статьи. В этой статье мы только кратко затронем эту тематику.

Если рассматривать методы защиты от атак и угроз глобально, то есть два тренда в построении систем защиты – это превентивные методы защиты (классические) и проактивная защита. Превентивная защита строится на основе выделения периметра безопасности корпоративной сети, такая система безопасности гарантирует защиту от вирусов и троянов, ransomware, DDos-атак, атак на веб- и мобильные приложения (см. OWASP Top 10), защиту от утечек и внутренних угроз, от фишинга и методов социальной инженерии.

Среди превентивных методов можно выделить следующие:

1. Контроль доступа к ресурсам корпоративной сети (парольная защита, двухфакторная аутентификация и т.д.).

2. Защита от вредоносного ПО (антивирусы последнего поколения).

3. Предотвращение внутренних угроз и утечек конфиденциальной информации (DLP-системы и др.).

4. Контроль веб-трафика и корпоративной электронной почты (межсетевые экраны, UTM, NGFW и т.д.).

5. Системы обнаружения и предотвращения вторжений и хакерских атак (англ. IDS/IPS, Intrusion detection system/Intrusion prevention system).

Однако все вышеперечисленные методы слабо применимы против «целевых атак» (APT), поэтому специалисты в сфере ИБ часто переходят к методам проактивной защиты – это «ханипоты» (honeypots и honeynets) и более современные «Технологии обмана» (англ., Deception technology). С помощью «ханипота» (специального хоста в сети) можно обманным путем завлечь злоумышленника в сеть. Прямой перевод с английского слова honeypot – это «горшочек с медом». У хакера создается ложное впечатление, что он попал в корпоративную сеть, а на самом деле он находится в изолированном сегменте под полным контролем сотрудников департамента ИБ компании. В последние годы методы проактивной защиты получили свое развитие, и на рынок вышли системы распределенной инфраструктуры ложных целей (англ. Distributed Deception Platform, DDP). С помощью DDP разворачивается полная имитация ИТ-инфраструктуры организации, атакующий вводится в полное заблуждение и таким образом происходит предотвращение целевой атаки (APT). В результате такой проактивной защиты информационные ресурсы компании не подвергаются ущербу от атак и угроз, и бизнес сохраняет свои активы [30].

Заключение

В современном мире, где технологии все глубже проникают во все сферы жизни, роль кибербезопасности становится несравненно выше, чем это было еще несколько лет назад. Угрозы в киберпространстве набирают обороты,

становясь более изощренными и масштабными, что создает серьезные риски для организаций, компаний и частных лиц. Защита от кибератак становится неотъемлемой частью успешной деятельности любого бизнеса, независимо от его масштабов. Эффективная защита от киберугроз требует не только технических решений, но и осознанности со стороны каждого участника цифрового пространства. Компании и организации должны внедрять комплексные меры безопасности, включая обучение сотрудников, мониторинг сетевой активности, использование передовых инструментов и применение современных технологий.

Важность инвестирования в кибербезопасность распространяется на компании и организации любого размера, ведь даже небольшие нарушения безопасности могут привести к серьезным потерям и утечкам данных. Поддерживание защищенной цифровой среды не только обеспечивает безопасность конфиденциальных данных, но и укрепляет доверие клиентов, деловых партнеров и инвесторов. Именно поэтому в нашу эпоху информационных технологий инвестирование в кибербезопасность становится стратегическим приоритетом, обеспечивая стабильность и устойчивость в динамичном и потенциально опасном цифровом мире.

Научная новизна работы заключается в инновационном подходе к изучению истории эволюции кибератак, стремительному развитию киберпреступности и развитию кибербезопасности. Автор провел глубокий анализ зарубежных и российских литературных источников по данной тематике. В отличие от подобных исследований зарубежных авторов, которые перечислены в списке литературы, была проделана исследовательская работа по анализу киберпреступлений за последние 60 лет, эволюции их в современные сложные кибератаки (например, APT). Также данное исследование опирается на методологию, изложенную в международных стандартах по кибербезопасности. На основе ее излагаются методы противодействия киберпреступлениям на современном этапе. Статья будет полезна как научным работникам в этой области, так и специалистам-практикам в сфере ИБ.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск, Беларусь
DOI: https://doi.org/10.23670/IRJ.2023.137.39.3

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk, Belarus
DOI: https://doi.org/10.23670/IRJ.2023.137.39.3

Список литературы на английском языке / References in English

1. Pan J. A Survey of the Research on Future Internet Architectures / J. Pan, S. Paul, R. Jain // IEEE Commun. Mag. — 2011. — 49. — P. 26-36. — DOI: 10.1109/MCOM.2011.5936152
2. Safa N.S. Information Security Policy Compliance Model in Organizations / N.S. Safa, R. Von Solms, S. Furnell // Comput. Secur. — 2016. — 56. — P. 70-82. — DOI: 10.1016/j.cose.2015.10.006
3. Von Solms R. From Information Security to Cyber Security / R. Von Solms, J. Van Niekerk // Comput. Secur. — 2013. — 38. — P. 97-102. — DOI: 10.1016/j.cose.2013.04.004
4. Craigen D. Defining Cyber Security / D. Craigen, N. Diakun-Thibault, R. Purse // Technol. Innov. Manag. Rev. — 2014. — 4. — P. 13-21. — DOI: 10.22215/timreview/835
5. Wang W. Cyber Security in the Smart Grid: Survey and Challenges / W. Wang, Z. Lu // Comput. Netw. — 2013. — 57. — P. 1344-1371. — DOI: 10.1016/j.comnet.2012.12.017
6. Papp D. Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy / D. Papp, Z. Ma, L. Buttyan // Proceedings of the 2015 13th Annual Conference on Privacy, Security and Trust. — Izmir, 2015. — P. 145-152.
7. Denning D.E.R. Cryptography and Data Security / D.E.R. Denning. — Boston: Addison-Wesley, 1982. — 112 p.
8. Blackley J.A. Information Security Fundamentals / J.A. Blackley, T.R. Peltier, J. Peltier. — Boca Raton: Auerbach Publications, 2004. — DOI: 10.1201/9780203488652
9. Cole E. Network Security Bible / E. Cole. — Hoboken: John Wiley & Sons, 2011. — 768 p.
10. Aslan O. A New Malware Classification Framework Based on Deep Learning Algorithms / O. Aslan, A.A. Yilmaz // IEEE Access. — 2021. — 9. — P. 87936-87951. — DOI: 10.1109/ACCESS.2021.3089586
11. Cyber-Security.Degree. — URL: https://cyber-security.degree/resources/history-of-cyber-security/ (accessed: 01.01.2023).
12. Wikipedia. List of Security Hacking Incidents. — URL: https://en.wikipedia.org/wiki/List_of_security_hacking_incidents (accessed: 01.01.2023).
13. Avast Blog. — URL: https://blog.avast.com/history-of-cybersecurity-avast (accessed: 01.01.2023).
14. Russell D. Computer Security Basics / D. Russell, S. Gangemi, G.T. Gangemi. — Sebastopol: O'Reilly Associates, 1991.
15. Lehtinen R. Computer Security Basics: Computer Security / R. Lehtinen, G.T. Gangemi. — Sebastopol: O'Reilly Media, 2006.
16. Wikipedia. Markus Hess. — URL: https://en.wikipedia.org/wiki/Markus_Hess (accessed: 01.01.2023).
17. Popularmechanics. A. Digital Spies: The Alarming Rise of Electronic Espionage // Pop. Mech. — URL: https://www.popularmechanics.com/technology/security/how-to/a7488/digital-spies-the-alarming-rise-of-electronic-espionage/ (accessed: 01.01.2023).
18. Aslan O. Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment / O. Aslan, M. Ozkan-Okay, D. Gupta // IEEE Access. — 2021. — 9. — P. 83252-83271. — DOI: 10.1109/ACCESS.2021.3087316.

19. Center For Internet Security: The Mirai Botnet–Threats and Mitigations. — URL: https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/ (accessed: 01.01.2023).

20. Kaspersky. — URL: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed: 01.01.2023).

21. CSO: Ransomware. — URL: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (accessed: 01.01.2023).

22. Trendmicro. — URL: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware (accessed: 01.01.2023).

23. Cyware. — URL: https://cyware.com/research-and-analysis/covidlock-android-ransomware-spreading-amid-covid-19-epidemic-4a5b (accessed: 01.01.2023).