Математические структуры и моделирование
2024. № 1 (69). С. 110–116

УДК 004.056
DOI 10.24147/2222-8772.2024.1.110-116

КИБЕРАТАКИ: НЕКОТОРЫЕ ПОДХОДЫ К СИСТЕМНОМУ АНАЛИЗУ

А.И. Горев
к.ю.н., доцент, e-mail: gorevai@omsu.ru
Е.Г. Горева
к.ф.-м.н., e-mail: gorevaeg@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Отсутствие единого подхода к пониманию и реагированию на кибератаки и инциденты между производителями программного обеспечения в сфере защиты информации, пользователями и государственными структурами, курирующими сферу кибербезопасности, приводит к невозможности взаимодействия и совместного противодействия. Рассмотрены различные подходы к классификации кибератак. Сделана попытка систематизации и анализа существующих угроз в виде атак на сетевую информационную инфраструктуру.

Ключевые слова: компьютерная атака, информационная инфраструктура, компьютерный инцидент, структура, классификация.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ о КИИ) определил начало нового этапа существования государства в эпоху информационного общества. До принятия закона задачи борьбы с нелигитимными действиями в сети возлагались на собственника информационных ресурсов, что ставило под сомнение успешность противодействия преступлениям в виртуальном пространстве. Это объяснялось многими факторами, в числе которых можно выделить отсутствие обмена опытом по противодействию преступному посягательству между собственниками информационных ресурсов, незаинтересованность собственников ресурсов в их защите от утечек информации и др. ФЗ о КИИ определил необходимость создания централизованного формата сбора, обработки и хранения информации об инцидентах информационной безопасности на объектах критической инфраструктуры.

Выделим два термина, определённых законодателем:

- компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры (далее – КИИ), сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;
- компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации

взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Интерес к терминологии объясним необходимостью однозначного понимания применяемых при взаимодействии аббревиатур, выражений, терминов. Формализация запросов и сообщений, регламентированная Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ), не может быть реализована без предварительного терминологического согласования. В настоящее время в сфере кибербезопасности нет единого подхода в данном вопросе, что обязательно приведёт к непониманию и коллизиям в правоприменительной практике взаимодействия с НКЦКИ. В формализованном сообщении о компьютерном инциденте субъект КИИ обязан сообщить о случившемся. Но если это сообщение будет формализовано только формально, т. е. при наличии структуры сообщения с выделенными полями об объекте КИИ, дате и времени инцидента и пр., поле с описанием зафиксированного события будет заполняться пользователем произвольно, то задачи систематизации, возложенные на НКЦКИ, не смогут быть реализованы в приемлемое время. Исходя из обнародованной статистики только зафиксированных кибератак, можно утверждать, что ежедневное количество сообщений о компьютерных инцидентах в НКЦКИ будет составлять десятки тысяч, что делает задачу обобщения практики и выдачу рекомендаций невыполнимой без предварительной формализации представления информации.

Отметим, что в сфере кибербезопасности нет единого сложившегося подхода к оценке инцидентов, что объясняется естественностью процесса развития любой сферы человеческой деятельности: появление новых технологий даёт развитие новым общественным отношениям, что, в свою очередь, требует своего урегулирования только после практических наработок и накопленного опыта.

В настоящее время можно отметить существование различных подходов к классификациям кибератак даже среди крупных производителей в сфере программного обеспечения (далее – ПО) защиты информации. Так, «Лаборатория Касперского» выделяет следующие виды: вредоносное ПО (далее – ВПО), распределённые атаки типа «отказ в обслуживании» (DdoS), фишинг, атаки с использованием SQL-инъекций, межсайтовый скриптинг (XSS) и ботнеты [1].

Positive Technologies предлагает следующую классификацию: фишинг, брутфорс-атака, ВПО, атака Drive-By Download, SQL-инъекции, атака «человек посередине» (Man-in-the-Middle, MITM), атаки типа «отказ в обслуживании» (Denial of Service, DoS) [2].

PVS-Studio выделяет среди основных видов кибератак: применение вредоносных программ; DdoS-атаки; фишинг; организация ботнетов; SQL-инъекция (внедрение кода SQL); XSS (межсайтовый скриптинг или применение межсайтовых сценариев); использование программы-вымогателя или шантажиста [3].

Подобная ситуация и в иностранных источниках. Так, М. Шиванандхан выделяет следующие виды атак: атаки типа «человек посередине» (MITM), фишинг и ВПО, скрытые загрузки во время перехода по гиперссылкам, ботнет-атаки, атаки социальной инженерии, атаки с использованием SQL-инъекции, вредоносные атаки, атаки с использованием межсайтовых скриптов (XSS), атаки с использованием паролей,

атаки типа «отказ в обслуживании» (DoS), распределённые атаки типа «отказ в обслуживании» (DdoS), внутренние атаки и утечка данных, атаки с криптоджекингом: деньги для вредоносных майнеров [4].

Сложность обобщения состоит в том, что благодаря современному состоянию информационного пространства право голоса имеют не только традиционные СМИ и компании, занимающиеся профессиональной деятельностью в данной сфере, но и любой блогер, желающий высказаться по вопросу. При этом уровень профессиональных компетенций никем не определён и не оценивается, благодаря чему в инфосфере создаётся высокий уровень «информационного шума». Как один из многих негативных примеров можно привести блог М. Кульгина, автор которого предлагает выделить 54 (!) вида атак, смешивая и многократно повторяя схожие составы [5].

Уведомления о компьютерной атаке, которые можно экспортировать в НКЦКИ, включают следующие виды: DdoS-атака, неудачные попытки авторизации, попытки внедрения ВПО, попытки эксплуатации уязвимости, публикация мошеннической информации, сетевое сканирование, социальная инженерия. При этом допустимые категории и типы инцидентов НКЦКИ, которые можно экспортировать в НКЦКИ, включают: вовлечение контролируемого ресурса в инфраструктуру ВПО, замедление работы ресурса в результате DdoS-атаки, заражение ВПО, захват сетевого трафика, использование контролируемого ресурса для фишинга, компрометация учётной записи, несанкционированное изменение информации, несанкционированное разглашение информации, публикация на ресурсе запрещённой законодательством РФ информации, рассылка спам-сообщений с контролируемого ресурса, успешная эксплуатация уязвимости [6].

В табл. 1 сведены сравнительные классификации атак производителей ПО защиты информации и формализованного запроса НКЦКИ.

Приведённый анализ показывает различие в подходах классификации у производителей ПО защиты информации и регламентирующим данный процесс государственным органом в лице НКЦКИ. Но менее объяснимым является то, что при определении перечня компьютерных атак отечественные производители ПО защиты информации не выделяют наиболее опасные виды, такие как APT- и LoTL-атаки. При этом описание данных видов атак присутствует в блогах указанных фирм [7, 8].

С другой стороны, отдельным видом кибератак выделены ботнеты, хотя ботнет определяется как единая сеть компьютеров, которыми можно управлять удалённо и контроль над которыми получен при использовании специальных троянских программ [9]. Таким образом, ботнет является инструментом для осуществления различных действий, в том числе атак. Вызывают нарекания и некоторые другие выделенные категории. Но особое внимание следует обратить на то, что оценки кибератак со стороны производителей ПО защиты информации сильно отличаются от классификации, предлагаемой НКЦКИ. В некоторых случаях однотипные атаки имеют различные наименования, что также недопустимо. Данное несоответствие существенным образом негативно скажется на практике регистрации кибератак субъектами КИИ, передаче данных об атаках в НКЦКИ, последующем обобщении зафиксированной информации и выдачу рекомендаций конечным пользователям.

Исходя из этого, считаем необходимым обратить особое внимание на классификацию кибератак. Основываясь на анализе источников, считаем необходимым

Таблица 1. Сравнительные классификации атак

Тип атаки	Лаборатория Касперского	Positive Technologies	PVS-Studio	НКЦКИ
Вредоносное ПО	+	+	+	+
Распределенные атаки «отказ в обслуживании» DdoS	+	–	+	+
«Отказ в обслуживании» DoS	–	+	–	–
Фишинг (социальная инженерия)	+	+	+	+
Использование SQL-инъекций	+	+	+	–
Межсайтовый скриптинг (XSS)	+	+	–	–
Ботнеты	+	–	+	–
Брутфорс-атака	–	+	–	–
Drive-By Download	–	+	–	–
«Человек посередине», MITM	–	+	–	–
Программа-вымогатель или шантажист	–	–	+	–
Неудачные попытки авторизации	–	–	–	+
Попытки эксплуатации уязвимости	–	–	–	+
Публикация мошеннической информации	–	–	–	+
Сетевое сканирование	–	–	–	+

выделить следующие категории:

- Вредоносное ПО – представляет нецеленаправленные атаки на широкую аудиторию, например, пользователей сети «Интернет». «Программа-вымогатель или шантажист», выделенные в таблице, представляют частный случай данной категории.
- Распределённые атаки «отказ в обслуживании» DdoS – целевые атаки, направленные на блокирование работы конкретного сетевого ресурса. Атака может быть реализована следующими тремя механизмами: переполнение канала связи, т. е. различные типы флуда, использование уязвимости стека сетевых протоколов и атаки на прикладной уровень [10]. DoS является упрощённой разновидностью атаки DdoS. Отличительной особенностью является явное проявление момента атаки.
- APT-атаки – advanced persistent threat (расширенные, таргетированные постоянные угрозы) – хорошо организованная, тщательно спланированная кибер-

атака, направленная на конкретную компанию или целую отрасль. Отличительной особенностью является использование уязвимостей нулевого дня. Продолжительность атаки может составлять несколько месяцев. Атака «попытка эксплуатации уязвимости», выделенная НКЦКИ, является разновидностью APT-атаки на неисправленную администратором системы уязвимость.

- LoTL-атаки (Living off the Land – атаки «подножным кормом») – метод использования легитимного ПО для осуществления деструктивных действий, таких как: получение неправомерного доступа, повышение привилегий, отправка и получение файлов, изменение системных настроек и т. д. Популярными инструментами являются PowerShell, WMI, CMD, CLI, BASH и др. Отличительной особенностью является отсутствие «цифрового следа», поскольку используются инструменты операционной системы (далее – ОС).
- Атаки «человек посередине», MITM – тип кибер-атаки, при котором злоумышленник перехватывает передачу данных путём прослушивания или притворяясь легальным участником [11]. Подготовка к атаке проводится с помощью сниффера пакетов – прикладной программы, которая использует сетевую карту в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). Сниффер перехватывает все сетевые пакеты, которые передаются через определённый домен. Некоторые исследователи выделяют сниффер в самостоятельный вид атаки, однако снифферы работают в сетях на законном основании для диагностики неисправностей и анализа трафика.
- Атака «ускоренная передача данных» – захват канала передачи данных, при котором работа конкурирующих TCP-соединений в том же коммуникационном канале блокируется, поскольку из-за резко возросшей интенсивности трафика другие соединения диагностируют состояние затора и принимают соответствующие меры по уменьшению скорости передачи данных, фактически освобождая канал для злоумышленника. Отличительной особенностью является лигитимность действий злоумышленника, который используя уязвимости протокола обмена может повысить скорость своего обмена с сервером за счёт других пользователей. Отличительной особенностью является отсутствие необходимости технических знаний. Данный вид атаки можно рассматривать как лигитимную DoS-атаку.
- Фишинг (социальная инженерия) – совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию [12]. Атака «Drive-By Download» часто является следствием фишинга, поскольку происходит при обращения пользователя к «заражённому» сайту. Публикация мошеннической информации для обмана пользователя является разновидностью фишинга. Отличительной особенностью является отсутствие необходимости технических знаний. Фишинговые мошенники не пытаются воспользоваться уязвимостями в ОС устройства, они прибегают к методам социальной инженерии.
- Неудачные попытки авторизации (брутфорс-атака, Brute-force) – попытка подобрать пароль или ключ шифрования. Метод заключается в последовательном переборе разных комбинаций символов до тех пор, пока одна из них не

подойдёт. Поиск пароля ведётся с использованием специальных программ и сервисов [13].

- Использование SQL-инъекций – уязвимость, которая позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации. Атаки на основе таких уязвимостей – одни из самых распространённых и опасных: они могут быть нацелены на любое веб-приложение или веб-сайт, которые взаимодействуют с базой данных SQL [14].
- Межсайтовый скриптинг (XSS) – атаки с внедрением вредоносного кода на доверенные веб-сайты, в процессе которой происходит внедрение вредоносных скриптов в контент веб-сайта. Эти скрипты включаются в динамический контент, отображаемый в браузере жертвы, и браузер выполняет их. В результате вредоносные скрипты могут получить доступ к конфиденциальной информации, сохранённой браузером и используемой на этом сайте. Отличительной особенностью является то, что атака нацелена не на приложение – риску подвергаются пользователи веб-приложения [15].
- Сетевое сканирование – является возможным предвестником атаки. Выделяются два вида. Ping-сканирование – обнаружение «живых» узлов в сети с помощью широковещательной рассылки пакетов ICMP. Сканирование портов – пробные попытки подключения к внешним узлам, определяет доступные порты на узлах, на основе чего делается предположение о типе используемой ОС или конкретного приложения, запущенного на конечном узле [16].

Подводя итоги, можно отметить, что современное состояние безопасности информационной инфраструктуры существенным образом зависит от понимания угроз в сетевом пространстве. Многообразие компьютерных атак делает необходимым проведение системного анализа и исследования уязвимостей, на которые нацелены эти угрозы. Дальнейшие разработки систем безопасности без проведения системного анализа кибератак, принятия единой классификации и единого подхода к анализу инцидентов на базе НКЦКИ делает эту работу неэффективной.

Литература

1. Предотвращение кибератак. URL: `https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-prevent-cyberattacks` (дата обращения: 10.01.2024).
2. Основные типы кибератак и способы борьбы с ними. URL: `https://www.securitylab.ru/analytics/535598.php` (дата обращения: 23.01.2023).
3. Кибератака. URL: `https://pvs-studio.ru/ru/blog/terms/6651/` (дата обращения: 11.03.2023).
4. 13 типов кибератак, о которых вам следует знать в 2023 году. URL: `https://www.freecodecamp.org/news/types-of-cyber-attacks-to-know/` (дата обращения: 12.09.2023).
5. 54 вида кибератак, о которых следует знать в 2024 году. URL: `https://dzen.ru/a/ZUYNJUusBWYBYvzz` (дата обращения: 04.11.2023).
6. Допустимые категории и типы инцидентов НКЦКИ. URL: `https://support.kaspersky.ru/help/KUMA/2.1/ru-RU/220462.htm` (дата обращения: 29.11.2023).

7. 5 признаков APT-атаки и советы по ее предотвращению. URL: https://www.kaspersky.ru/resource-center/threats/advanced-persistent-threat (дата обращения: 23.01.2024).
8. Living-off-the-land (LotL): скрытые атаки, уничтожающие целые организации. URL: https://www.securitylab.ru/analytics/546134.php (дата обращения: 23.01.2024).
9. Что такое ботнет? URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (дата обращения: 23.01.2024).
10. Классификация DDoS: полное руководство по типам атак. URL: https://ddos-guard.net/ru/info/blog-detail/classification-of-ddos-attacks-a-short-overview-of-modern-approaches (дата обращения: 26.01.2023).
11. Что такое атака Man-in-the-Middle (MITM)? Определение и предотвращение. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351898.php (дата обращения: 24.02.2022).
12. Как работает современный веб-фишинг. URL: https://www.anti-malware.ru/How-Modern-Web-Phishing-Works (дата обращения: 08.09.2020).
13. Что такое брутфорс. URL: https://developers.sber.ru/help/business-development/what-is-a-brute-force (дата обращения: 23.06.2023).
14. Что такое SQL-инъекция? Определение и описание. URL: https://www.kaspersky.ru/resource-center/definitions/sql-injection (дата обращения: 06.03.2022).
15. Методы предотвращения межсайтовых скриптингов (XSS). URL: https://www.geeksforgeeks.org/cross-site-scripting-xss-prevention-techniques/ (дата обращения: 02.10.2021).
16. Проводим сканирование сети самостоятельно. URL: https://www.securitylab.ru/blog/company/pt/349200.php (дата обращения: 04.08.2021).

RULES FOR JOURNAL ARTICLES “MATHEMATICAL STRUCTURES AND MODELING”

A.I. Gorev
Ph.D. (Law), Associate Professor, e-mail: gorevai@omsu.ru
E.G. Goreva
Ph.D. (Phys.-Math., e-mail: gorevaeg@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The lack of a unified approach to understanding and responding to cyber attacks and incidents between information security software manufacturers, users and government agencies in charge of cybersecurity leads to the impossibility of interaction and joint counteraction. Various approaches to the classification of cyber attacks are considered. An attempt is made to systematize and analyze existing threats in the form of attacks on the network information infrastructure.

Keywords: computer attack, information infrastructure, computer incident, structure, classification.

Дата поступления в редакцию: 01.03.2024