ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 056.57
DOI: 10.21822/2073-6185-2023-50-4-93-100

Оригинальная статья /Original article

Разработка методов нейтрализации угроз «нулевого дня»

А.И. Дубровина[1,2], Мустафа Х. Алкорди[1]
[1] Донской государственный технический университет,
[1]344000, г. Ростов-на-Дону, пл. Гагарина, 1, Россия,
[2]Частное образовательное учреждение высшего образования
«Южный университет» (Институт управления, бизнеса и права),
[2]344000, г. Ростов-на-Дону, ул. Мечникова, 130, Россия

Резюме. Цель. Целью данного исследования является разработка и анализ методов нейтрализации угроз «нулевого дня» с целью повышения уровня кибербезопасности и защиты информационных систем. **Метод.** В настоящей статье использован поведенческий анализ угрозы. Изучены характерные признаки поведения эксплойта «нулевого дня». Модель угрозы основана на решении задач по своевременному обнаружению и нейтрализации угрозы. **Результат.** Рассмотрена актуальная проблема безопасности информационных систем - угроза «нулевого дня». Проведены обзор существующих методов нейтрализации и обсуждение эффективных новых подходов. Выявлено, что основным уязвимым местом являются устаревшие сигнатуры угроз. Обнаружение угроз основано на исследовании поведения программных обеспечений – сравнение с предыдущим днем, отслеживание возможно преимущественно засчет анализа log-файлов, снятых с автоматизированного рабочего места. **Вывод**. Доказана важность разработки методов нейтрализации угроз «нулевого дня» во избежание централизованного распространения уязвимости и заражения большого числа автоматизированных рабочих мест, что может привести к приостановке производственных процессов в рамках большого предприятия.

Ключевые слова: информационная безопасность, атака нулевого дня

Для цитирования: А.И. Дубровина, Мустафа Х. Алкорди. Разработка методов нейтрализации угроз «нулевого дня». Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(4):93-100. DOI:10.21822/2073-6185-2023-50-4-93-100

Development of methods for neutralizing «Zero-day» threats

A.I. Dubrovina[1,2], Mustafa H. Alcordi[1]
[1]Don State Technical University,
[1] 1 Gagarin Square, Rostov-on-Don 344000, Russia
[2]Southern University (Institute of Management, Business and Law),
[2] 130 Mechnikova St., Rostov-on-Don 344000, Russia

Abstract. Objective. The purpose of this study is to develop and analyze methods for neutralizing «zero-day» threats in order to increase the level of cybersecurity and protection of information systems. **Method.** In this article, a behavioral analysis of the threat is used. The characteristic features of the zero-day exploit behavior have been studied. The threat model is based on solving the tasks of timely detection and neutralization of the threat. **Result.** The actual problem of information systems security - the threat of «zero-day» is considered. The review of existing neutralization methods and discussion of effective new approaches were carried out. It has been revealed that the main vulnerability is outdated threat signatures. Threat detection is based on a study of the behavior of software a comparison with the previous day tracking is possible mainly by analyzing log files taken from an automated workplace. **Conclusion.** The content of this work emphasizes the importance of developing methods to neutralize «zero-day» threats in

order to avoid the centralized spread of vulnerability and infection of a large number of automated workplaces, which can lead to the suspension of production processes within a large enterprise.

Keywords: information security, zero-day attack

For citation: A.I. Dubrovina, Mustafa H. Alcordi. Development of methods for neutralizing «Zero-day» threats. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4):93-100. DOI:10.21822/2073-6185-2023-50-4-93-100

Введение. Развитие методов нейтрализации угроз «нулевого дня» является актуальной проблемой на сегодняшний день в связи с масштабами распространения и неоднозначности возникновения. Современная информационная среда становится все более сложной и уязвимой перед новыми видами кибератаками. Угрозы «нулевого дня» представляют собой особый вызов для сферы кибербезопасности, так как атаки происходят на стадии, когда уязвимости еще не известны владельцам системы или разработчикам программного обеспечения.

Постановка задачи. Атаки «нулевого дня»: захват уязвимостей в мире кибербезопасности. «Нулевой день» - это широкий термин, описывающий недавно обнаруженные уязвимости в системе безопасности, которые хакеры могут использовать для атак на системы [1]. Термин «нулевой день» относится к тому факту, что поставщик или разработчик только что узнал об ошибке, что означает, что у них есть «нулевые дни», чтобы исправить ее. Для достижения цели исследования были поставлены следующие задачи:

1. Изучить сущность и особенности угроз «нулевого дня».
2. Провести обзор существующих методов нейтрализации киберугроз, добавив реальные примеры.
3. Разработать новые подходы и методы нейтрализации угроз «нулевого дня».

Методы исследования. Атака нулевого дня происходит, когда хакеры используют уязвимость до того, как разработчики успевают ее устранить. Нулевой день иногда записывается как 0-day. Слова уязвимость, эксплойт и атака обычно используются вместе с нулевым днем, и полезно понимать разницу:

Уязвимость нулевого дня - это уязвимость программного обеспечения, обнаруженная злоумышленниками до того, как о ней стало известно производителю. Поскольку поставщики ничего не знают, для уязвимостей нулевого дня не существует исправлений при проведении пентестинга, что повышает вероятность успеха атак [2].

Эксплойты «нулевого дня»: скрытая угроза и импакт в киберпространстве, в связи с чем применяется поведенческий метод мсследования. Эксплойт нулевого дня - это метод, который хакеры используют для атаки на системы с ранее неизвестной уязвимостью. Атака нулевого дня - это использование эксплойта нулевого дня для нанесения ущерба или кражи данных из системы, затронутой уязвимостью. Для атаки нулевого дня хакеры разрабатывают и применяют специализированные программные коды, называемые эксплойтами. Эксплойты представляют собой инструкции, которые позволяют злоумышленникам взламывать уязвимые компоненты системы. Эти коды могут использоваться для разнообразных целей, включая кражу данных, установку вредоносных программ или даже блокировку системы (рэнсомвары) [3,4].

Программное обеспечение часто имеет уязвимости в системе безопасности, которые хакеры могут использовать для создания хаоса рэнсомвары [5]. Разработчики программного обеспечения всегда ищут уязвимости, чтобы «залатать», то есть разработать решение, которое они выпускают в новом обновлении.

Однако иногда хакеры или злоумышленники замечают уязвимость раньше разработчиков программного обеспечения. Пока уязвимость все еще открыта, злоумышленники могут написать и внедрить код, чтобы воспользоваться ею. Это известно как код эксплойта. Код эксплойта может привести к тому, что пользователи программного

обеспечения станут жертвами, например, в результате кражи личных данных или других форм киберпреступности. Как только злоумышленники обнаруживают уязвимость нулевого дня, им нужен способ добраться до уязвимой системы [6]. Они часто делают это с помощью электронной почты с социальной инженерией, т. е. электронной почты или другого сообщения, которое предположительно исходит от известного или законного корреспондента, но на самом деле от злоумышленника. Сообщение пытается убедить пользователя выполнить действие, например, открыть файл или посетить вредоносный веб-сайт. При этом загружается вредоносное ПО злоумышленника, которое проникает в файлы пользователя и крадет конфиденциальные данные.

Результатом успешной атаки нулевого дня может быть серьезное нарушение безопасности, что ведет к потенциальным убыткам как для организаций, так и для отдельных пользователей. Кража личных данных, финансовые потери, нарушение репутации – все это возможные последствия атак нулевого дня [7]. Когда об уязвимости становится известно, разработчики пытаются исправить ее, чтобы остановить атаку (рис. 1).

Однако зачастую уязвимости системы безопасности обнаруживаются не сразу. Иногда могут пройти дни, недели или даже месяцы, прежде чем разработчики определят уязвимость, которая привела к атаке. И даже когда патч нулевого дня выпущен, не все пользователи быстро внедряют его. В последние годы хакеры стали быстрее использовать уязвимости вскоре после их обнаружения. Эксплойты можно продавать в даркнете за большие деньги. Как только эксплойт обнаружен и исправлен, его больше не называют угрозой нулевого дня.

Рис. 1. Timeline of zero-day attack
Fig. 1. Timeline of zero-day attack

Атаки нулевого дня особенно опасны, потому что о них знают только сами злоумышленники. Как только они проникли в сеть, преступники могут либо немедленно атаковать, либо сидеть и ждать наиболее выгодного момента для этого [8].

Мотивации и цели злоумышленника при внедрении уязвимости «нулевого дня». Злоумышленники, осуществляющие атаки нулевого дня, делятся на разные категории в зависимости от их мотивации.

Например: киберпреступники - хакеры, мотивация которых обычно связана с финансовой выгодой; хактивисты - хакеры, мотивированные политическими или социальными причинами, которые хотят, чтобы атаки были видны, чтобы привлечь внимание к их делу; корпоративный шпионаж - хакеры, которые шпионят за компаниями, чтобы получить информацию о них; кибервойна - страны или политические деятели, шпионящие или атакующие кибер инфраструктуру другой страны.

Взлом нулевого дня может использовать уязвимости в различных системах, в том числе: операционные системы; Веб-браузеры; офисные приложения; компоненты с открытым исходным кодом; аппаратное обеспечение и прошивка; интернет вещей (IoT).

В результате существует широкий круг потенциальных жертв: люди, использующие уязвимую систему, например, браузер или операционную систему; хакеры могут использовать уязвимости в системе безопасности для взлома устройств и создания крупных бот-сетей;

лица, имеющие доступ к ценным бизнес-данным, таким как интеллектуальная собственность; аппаратные устройства, микропрограммы и Интернет вещей; крупные предприятия и организации; государственные органы; политические цели и/или угрозы национальной безопасности.

К разновидности атак «нулевого дня» относят следующие:

1. Целевые атаки «нулевого дня» осуществляются против потенциально ценных целей, таких как крупные организации, государственные учреждения или высокопоставленные лица.
2. Нецелевые атаки нулевого дня обычно проводятся против пользователей уязвимых систем, таких как операционная система или браузер.

Даже когда злоумышленники не нацелены на конкретных лиц, большое количество людей все равно может быть затронуто атаками нулевого дня, обычно в качестве побочного ущерба. Нецелевые атаки направлены на захват как можно большего числа пользователей, а это означает, что могут быть затронуты данные среднего пользователя [9].

Поскольку уязвимости нулевого дня могут принимать различные формы, такие как отсутствие шифрования данных, отсутствие авторизации, неработающие алгоритмы, ошибки, проблемы с безопасностью паролей и т. д., их может быть сложно обнаружить. Из-за характера этих типов уязвимостей подробная информация об эксплойтах нулевого дня доступна только после того, как эксплойт будет идентифицирован.

Ниже представлена архитектура трех уровней для обнаружения и анализа атак «нулевого дня» (рис. 2).

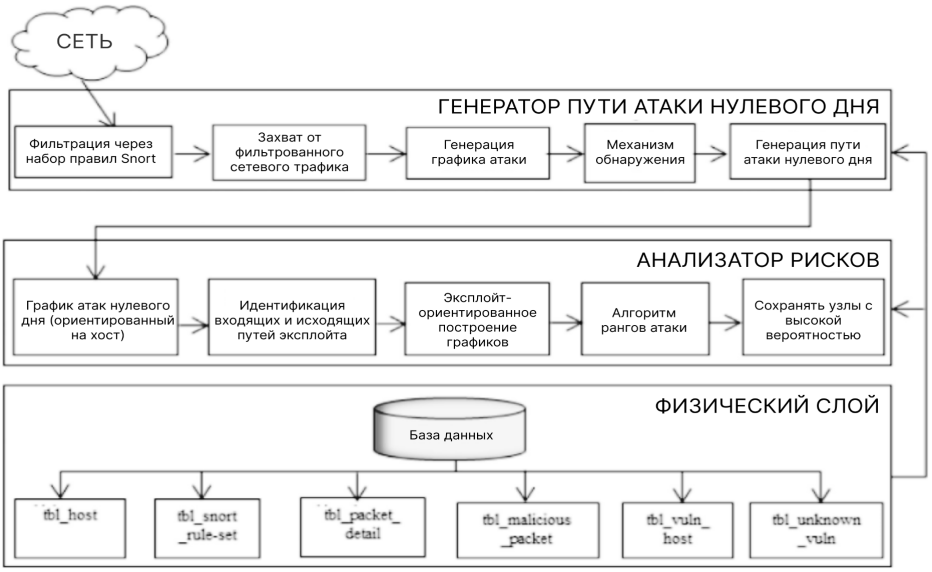

Рис. 2. The proposed three layer architecture for zero-day attack detection and analysis
Fig. 2. The proposed three layer architecture for zero-day attack detection and analysis

Организации, атакованные эксплойтом нулевого дня, могут обнаружить неожиданный трафик или подозрительную активность сканирования, исходящие от клиента или службы. Некоторые из методов обнаружения нулевого дня включают в себя:

Использование существующих баз данных вредоносных программ и их поведение в качестве эталона. Хотя эти базы данных обновляются очень быстро и могут быть полезны в качестве ориентира, эксплойты нулевого дня по определению являются новыми и неизвестными [10]. Таким образом, существует предел того, что существующая база данных может вам сообщить. Кроме того, некоторые методы ищут характеристики вредоносных программ нулевого дня на основе того, как они взаимодействуют с целевой системой. Вместо изучения кода входящих файлов этот метод рассматривает их взаимодействие с существующим программным обеспечением и пытается определить, являются ли они результатом злонамеренных действий.

Машинное обучение все чаще используется для обнаружения данных ранее зарегистрированных эксплойтов, чтобы установить базовый уровень безопасного поведения системы на основе данных о прошлых и текущих взаимодействиях с системой. Чем больше данных доступно, тем надежнее становится обнаружение [11]. Часто используется гибрид различных систем обнаружения.

Новейшие атаки нулевого дня, примеры и исходы. В данной подборке мы рассмотрим несколько выдающихся случаев, где уязвимости были эксплуатированы до их обнаружения и устранения. Наиболее опасными инцидентами информационной безопасности являются следующие [12]:

2021: Уязвимость «нулевого дня в Chrome». В 2021 году Google Chrome столкнулся с серией угроз «нулевого дня», в результате чего Chrome стал выпускать обновления. Уязвимость возникла из-за ошибки в движке JavaScript V8, используемом в веб-браузере.

2020: Zoom. В популярной платформе для видеоконференций обнаружена уязвимость. В этом примере атаки «нулевого дня» хакеры получили удаленный доступ к ПК пользователя, если тот работал под управлением более старой версии Windows. Если целью был администратор, хакер мог полностью захватить его компьютер и получить доступ ко всем его файлам.

2020: Apple iOS. iOS от Apple часто называют самой безопасной из основных платформ для смартфонов. Однако в 2020 году он стал жертвой как минимум двух наборов уязвимостей нулевого дня iOS, включая ошибку нулевого дня, которая позволяла злоумышленникам удаленно скомпрометировать iPhone.

2019: Microsoft Windows, Восточная Европа. Эта атака была направлена на привилегии локального повышения, уязвимую часть Microsoft Windows и правительственные учреждения в Восточной Европе. Эксплойт нулевого дня злоупотреблял уязвимостью локальных привилегий в Microsoft Windows для запуска произвольного кода и установки приложений, а также для просмотра и изменения данных в скомпрометированных приложениях. После того, как атака была обнаружена и о ней было сообщено в Центр реагирования Microsoft Security Response Center, было разработано и выпущено исправление.

2017: Microsoft Word. Этот эксплойт нулевого дня взломал личные банковские счета. Жертвами стали люди, которые невольно открыли вредоносный документ Word. В документе отображалось приглашение «загрузить удаленный контент», показывающее пользователям всплывающее окно с запросом внешнего доступа из другой программы. Когда жертвы нажимали «да», документ устанавливал на их устройства вредоносное ПО, которое могло перехватывать учетные данные для входа в банк [13].

Stuxnet. Одним из самых известных примеров атаки «нулевого дня» стал Stuxnet. Этот вредоносный компьютерный червь, впервые обнаруженный в 2010 году, но уходящий корнями в 2005 год, поражал производственные компьютеры, на которых установлено программное обеспечение программируемого логического контроллера (ПЛК). Основной целью были иранские заводы по обогащению урана, чтобы сорвать ядерную программу страны. Червь заражал ПЛК через уязвимости в программном обеспечении Siemens Step7, заставляя ПЛК выполнять неожиданные команды на конвейерном оборудовании.

В условиях быстрого развития киберугроз и постоянно меняющихся методов атак, разработка новых подходов и методов нейтрализации угроз «нулевого дня» становится неотъемлемой составляющей в обеспечении безопасности информационных систем [14].

Основными действенными подходами и методами, которые могут быть эффективно применены для предотвращения атак «нулевого дня» являюся следующие.

1. Искусственный интеллект и машинное обучение: Применение методов искусственного интеллекта (ИИ) и машинного обучения (МО) имеет огромный потенциал в обнаружении атак «нулевого дня». Алгоритмы МО могут анализировать необычное поведение в системе, выявлять аномалии и определять потенциально опасные ситуации. Такие системы способны обнаруживать атаки на ранних стадиях,

когда уязвимости еще неизвестны [14].

2. Анализ поведения и контекста: Одним из ключевых аспектов при разработке методов нейтрализации атак «нулевого дня» является анализ поведения и контекста пользователей и системы [15,16]. Системы могут отслеживать действия пользователей и выявлять аномалии в их поведении. Кроме того, контекстная информация, такая как тип устройства, местоположение, время суток, также может быть использована для более точного определения атак.
3. Проактивное обнаружение уязвимостей: Одним из способов снижения риска атак «нулевого дня» является акцент на проактивном обнаружении и устранении уязвимостей [17]. Это включает в себя регулярное тестирование на уязвимости, аудит кода программного обеспечения, а также использование инструментов автоматического сканирования для поиска потенциальных слабых мест.
4. Децентрализованные системы и блокчейн: Использование децентрализованных систем и технологии блокчейн также может способствовать повышению безопасности от атак «нулевого дня» [17,18]. Блокчейн может обеспечить надежное хранение данных об уязвимостях и атаках, а децентрализованные системы могут осложнить процесс атаки, требуя атакующему контролировать большое количество узлов.
5. Разработка адаптивных систем: Атаки «нулевого дня» могут быть чрезвычайно многообразными и могут обходить существующие меры защиты. Разработка адаптивных систем, способных быстро реагировать на новые угрозы и атаки, может значительно повысить эффективность нейтрализации атак «нулевого дня».

Обсуждение результатов. Разработка новых подходов и методов нейтрализации угроз «нулевого дня» является необходимой задачей в сфере кибербезопасности. Интеграция искусственного интеллекта, анализа поведения, проактивного обнаружения уязвимостей, использование децентрализованных систем и создание адаптивных решений способствуют более надежной защите информационных систем от этого сложного типа атак [19]. Дальнейшие исследования и разработки в этой области могут значительно содействовать созданию более безопасной киберсреды.

В ходе исследования был проведен анализ угроз «нулевого дня» на примере известных атак и уязвимостей. Был проведен обзор существующих методов защиты информационных систем, включая методы обнаружения и предотвращения уязвимостей, контроля доступа и шифрования данных.

На основе проведенного анализа были разработаны новые методы нейтрализации угроз «нулевого дня», включая комбинацию проактивного обнаружения уязвимостей, механизмов автоматического обновления программного обеспечения и обучения персонала.

Предложенные в данной статье инновационные подходы и методы представляют собой своего рода революцию в области кибербезопасности. Искусственный интеллект и машинное обучение вместе с анализом поведения и контекста создают надежные барьеры перед угрозами «нулевого дня», обнаруживая аномалии и предупреждая о потенциальных атаках [20,21]. Проактивное обнаружение уязвимостей позволяет заметить слабые места до того, как они станут объектом атак. Использование децентрализованных систем и блокчейна добавляет сложности для злоумышленников, а разработка адаптивных систем обеспечивает гибкую защиту в постоянно меняющейся угрозовой среде.

Однако важно понимать, что борьба с угрозами «нулевого дня» - это непрерывный и динамичный процесс. С каждым новым технологическим прорывом, киберпреступники находят новые пути атаки. Поэтому разработка методов нейтрализации угроз «нулевого дня» должна быть постоянной и систематической. Кроме того, не менее важным фактором является взаимодействие и обмен опытом между специалистами в области кибербезопасности, так как это способствует более эффективной адаптации к новым угрозам.

Все это свидетельствует о необходимости продолжения исследований и инноваций в области кибербезопасности.

Вывод. Современный мир, пронизанный информационными технологиями, требует высокого уровня кибербезопасности, который может устоять перед постоянно меняющимися угрозами. В наше время, когда киберпреступники постоянно стремятся к новым методам и техникам атак, разработка методов нейтрализации угроз «нулевого дня» становится неотъемлемой частью стратегии обеспечения безопасности информационных систем. Разработка методов нейтрализации угроз «нулевого дня» - это ключевой элемент в обеспечении стабильной и безопасной киберсреды, которая позволит современному обществу развиваться и процветать в век информационных технологий.

Библиографический список:

1. Journal of Information Security and Applications // Volume 46 June 2019 Pages 164-172
2. Huang, L., Joseph, A., Nelson, H., & Rubinstein, B. Adversarial machine learning // Proceedings of the 4th ACM workshop on Security and artificial intelligence. ACM, 2011. Pp. 43-58.
3. Rieck, K., Trinius, P., Willems, C., Holz, T., & Bos, H. Automatic analysis of malware behavior using machine learning // Journal of Computer Security, 19(4), 639-668.
4. DDoS-атаки. Причины возникновения, классификация и защита от DDoS-атак [Электронный ресурс]. URL: http://efsol.ru/articles/ddos-attacks.html (дата обращения 19.07.2023).
5. Флёнов М. Linux глазами хакера. - СПб.:БХВ-Петербург, 2010.- 480 с.
6. High-Tech Crime Trends 2017. Group-IB Report. – URL: https://www.group-ib.ru/resources/threat-research/2017-report.html. (Accessed: 18.03.18).
7. Topical Cyber-threats 2017. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/webinar_290218.pdf (Accessed: 14.03.18).
8. Meicong Li, Wei Huang. The Study of APT Attack Stage Model. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7550947&tag=1 (Accessed: 18.03.18).
9. Targeted Attack Anatomy. Kaspersky Lab. — URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (Accessed: 15.03.18). (In Russ).
10. B. B. Gupta, Aakanksha Tewari. Fighting against phishing attacks: state of the art and future challenges. – URL: https://link.springer.com/content/pdf/10.1007%2Fs00521-016-2275-y.pdf (Accessed: 25.03.18).
11. Spear-Phishing Attacks. Why they are successful and how to stop them. FireEye Report. – URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (Accessed: 25.03.18).
12. How social engineering opens a door to your organization. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf (Accessed: 16.04.2018). (in Russian).
13. Topical Cyberthreats 2017— Trends and forecasts. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (Accessed: 15.03.18). (in Russian).
14. Tzipora Halevi, Nasir Memon, Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742 (Accessed: 16.04.2018).
15. Scott Donnelly. Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals. RecordedFuture Report. – URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf (Accessed: 16.04.2018).
16. Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits. RecordedFuture Report. — URL: https://www.recordedfuture.com/top-vulnerabilities-2015/ (Accessed: 16.04.2018).
17. New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.] Recorded Future Report. – URL: https://www.recordedfuture.com/top-vulnerabilities-2016/ (Accessed: 16.04.2018).
18. Daniela Oliveira Harold Rocha Huizi Yang. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. – URL: https://dl.acm.org/citation.cfm?id=3025831(Accessed: 16.04.2018).
19. Thomas, J. E. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727 (Accessed: 16.04.2018).
20. Zhurin S.I., Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider. ICT Res. Appl., Vol. 8, No. 3, 2015, p. 230 – 248.
21. Zhurin S.I. Basics of countermesuares against insider threats. Tutorial for students. MEPhI, 2014. p. 262.

References

1. Journal of Information Security and Applications. June 2019; 46:164-172

2. Huang, L., Joseph, A., Nelson, H., & Rubinstein, B. Adversarial machine learning. *Proceedings of the 4th ACM workshop on Security and artificial intelligence. ACM*, 2011; 43-58.
3. Rieck, K., Trinius, P., Willems, C., Holz, T., & Bos, H. Automatic analysis of malware behavior using machine learning. *Journal of Computer Security*, 19(4), 639-668.
4. DDoS attacks. Causes of occurrence, classification and protection from DDoS attacks [Electronic resource]. URL: http://efsol.ru/articles/ddos-attacks.html (accessed 07.19.2023).
5. Flenov M. Linux through the eyes of a hacker. - St. Petersburg:BHV-Petersburg, 2010; 480. (In Russ).
6. High-Tech Crime Trends 2017. Group-IB Report. – URL: https://www.group-ib.ru/resources/threat-research/2017-report.html. (Accessed: 18.03.18).
7. Topical Cyber-threats 2017. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/webinar_290218.pdf (Accessed: 14.03.18).
8. Meicong Li, Wei Huang. The Study of APT Attack Stage Model. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7550947&tag=1 (Accessed: 18.03.18).
9. Targeted Attack Anatomy. Kaspersky Lab. — URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (Accessed: 15.03.18). (in Russ.).
10. B. B. Gupta, Aakanksha Tewari. Fighting against phishing attacks: state of the art and future challenges. – URL: https://link.springer.com/content/pdf/10.1007%2Fs00521-016-2275-y.pdf (Accessed: 25.03.18).
11. Spear-Phishing Attacks. Why they are successful and how to stop them. FireEye Report. – URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (Accessed: 25.03.18).
12. How social engineering opens a door to your organization. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf (Accessed: 16.04.2018). (In Russ).
13. Topical Cyberthreats 2017 Trends and forecasts. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (Accessed: 15.03.18). (In Russ).
14. Tzipora Halevi, Nasir Memon, Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742 (Accessed: 16.04.2018).
15. Scott Donnelly. Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals. RecordedFuture Report. – URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf (Accessed: 16.04.2018).
16. Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits. RecordedFuture Report. — URL: https://www.recordedfuture.com/top-vulnerabilities-2015/ (Accessed: 16.04.2018).
17. New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.] Recorded Future Report. – URL: https://www.recordedfuture.com/top-vulnerabilities-2016/ (Accessed: 16.04.2018).
18. Daniela Oliveira Harold Rocha Huizi Yang. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. – URL: https://dl.acm.org/citation.cfm?id=3025831(Accessed: 16.04.2018).
19. Thomas, J. E. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727 (Accessed: 16.04.2018).
20. Zhurin S.I., Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider. ICT Res. Appl., 2015; 8(3): 230 – 248.
21. Zhurin S.I. Basics of countermesuares against insider threats. Tutorial for students. MEPhI, 2014; 262.

Сведения об авторах:

Дубровина Ангелина Игоревна, ассистент, кафедра «Вычислительные системы и информационная безопасность»; adubrovina@yug.gkovd.ru

Алкорди Мустафа Хельми Муса, студент, кафедра «Вычислительные системы и информационная безопасность»; ministrelia69@yandex.ru.

Information about authors:

Angelina I. Dubrovina, Assistant, Department of Computer Systems and Information Security; adubrovina@yug.gkovd.ru

Alkordi Mustafa Helmi Musa, Student, Department of Computer Systems and Information Security; ministrelia69@yandex.ru.

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 27.10.2023.

Одобрена после рецензирования/ Reviced 16.11.2023.

Принята в печать/ Accepted for publication 16.11.2023.