ФОРМИРОВАНИЕ УЯЗВИМОГО УЗЛА «ADOBE COLDFUSION DESERIALIZATION OF UNTRUSTED DATA VULNERABILITY»

Конев А. А.[1], Репкин В. С.[2], Семёнов Г. Ю.[3], Сермавкин Н.И.[4]

DOI: 10.21681/2311-3456-2024-1-75-81

Цель исследования: *разработка уязвимого узла, что включает в себя анализ исследуемой уязвимости, реализацию её автоматизированной эксплуатации, формализацию процесса атаки, описание способов обнаружения, а также мер защиты.*

Методы исследования: *системный анализ, формализация процесса эксплуатации уязвимости с помощью методологии моделирования Meta Attack Language (MAL).*

Результат исследования: *в данной научной публикации представлен подробный анализ уязвимости «Adobe ColdFusion Deserialization of Untrusted Data Vulnerability» (CVE-2023-26360) формальное описание процесса ее эксплуатации с использованием MAL. Работа включает в себя описание структуры формируемого уязвимого узла и потенциальных угроз. Кроме того, статья представляет практический сценарий автоматизированной атаки, осуществляемой с использованием Python и фреймворка Metasploit, который может быть использован специалистами для определения защищенности собственной информационной системы. На основе проведенного исследования, в работе приводятся меры защиты и рекомендации для снижения риска эксплуатации уязвимости, включая установку обновлений безопасности и отключение компонентов, представляющих уязвимость.*

Практическая значимость: *результаты исследования можно использовать при создании и формализации сценариев атак, отмеченные меры защиты и детальное описание уязвимости могут быть использованы для обеспечения безопасной разработки на языке ColdFusion, представленный в работе код может быть применен в тестировании систем на проникновение. В данной научной статье не только анализируется уязвимость, но и демонстрируются все шаги её эксплуатации, что позволяет разработать более эффективные методы защиты информационных систем от подобных атак.*

Вклад авторов: *Конев А. А. выполнил постановку задачи и определил методы исследования. Сермавкин Н. И. разработал и настроил сетевую инфраструктуру, провел анализ уязвимости. Семенов Г. Ю. реализовал атаку, эксплуатирующую уязвимость с помощью Metasploit Framework, формализовал атаку с помощью MAL. Репкин В. С. реализовал автоматизированную атаку с помощью Pymetasploit, определил меры защиты.*

Ключевые слова: *информационная безопасность, обучение специалистов, автоматизированная эксплуатация, меры защиты, тестирование на проникновение, имитация атаки, киберполигон, Metasploit, Remote Code Execution, Meta Attack Language.*

FORMATION OF VULNERABLE NODE «ADOBE COLDFUSION DESERIALIZATION OF UNTRUSTED DATA VULNERABILITY»

Konev A. A.[5], Repkin V. S.[6], Semenov G. Yu.[7], Sermavkin N. I.[8]

The purpose of the article: *development of a vulnerable node, which includes the analysis of the vulnerability under study, implementation of its automated exploitation, formalization of the attack process, description of detection methods, as well as protection measures.*

1 Конев Антон Александрович, кандидат технических наук, доцент, ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР), г. Томск, Россия. E-mail: kaa@fb.tusur.ru

2 Репкин Владимир Сергеевич, техник, Центр компетенций Национальной технологической инициативы «Технологии доверенного взаимодействия» (ЦК НТИ ТДВ), г. Томск, Россия. E-mail: repkin_vova@mail.ru

3 Семёнов Григорий Юрьевич, техник, Центр компетенций Национальной технологической инициативы «Технологии доверенного взаимодействия» (ЦК НТИ ТДВ), г. Томск, Россия. E-mail: semenov.g.749-1@e.tusur.ru

4 Сермавкин Никита Игоревич, техник, Центр компетенций Национальной технологической инициативы «Технологии доверенного взаимодействия» (ЦК НТИ ТДВ), г. Томск, Россия. E-mail: iis.vseverske@mail.ru

5 Anton A. Konev, Ph.D., Associate Professor, Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia. E-mail: kaa@fb.tusur.ru

6 Vladimir S. Repkin, Technician, Center of Competences of the National Technological Initiative «Trusted Interaction Technologies», Tomsk, Russia. E-mail: repkin_vova@mail.ru

7 Grigory Y. Semenov, Technician, Center of Competences of the National Technological Initiative «Trusted Interaction Technologies», Tomsk, Russia. E-mail: semenov.g.749-1@e.tusur.ru

8 Nikita I. Sermavkin, Technician, Center of Competences of the National Technological Initiative «Trusted Interaction Technologies», Tomsk, Russia. E-mail: iis.vseverske@mail.ru

Research method: *system analysis, formalization of the vulnerability exploitation process using Meta Attack Language (MAL) modeling methodology.*

The result: *this scientific publication presents a detailed analysis of the vulnerability «Adobe ColdFusion Deserialization of Untrusted Data Vulnerability» (CVE-2023-26360) and a formal description of the process of its exploitation using MAL. The paper includes a description of the structure of the vulnerability node being formed and the potential threats. In addition, the paper presents a practical scenario of an automated attack carried out using Python and the Metasploit framework, which can be used by specialists to determine the security of their own information system. Based on the research conducted, the paper provides protective measures and recommendations to reduce the risk of vulnerability exploitation, including installing security updates and disabling components that present the vulnerability.*

Practical significance: *the results of the study can be used in the creation and formalization of attack scenarios, the noted protection measures and a detailed description of the vulnerability can be used to ensure secure development in the ColdFusion language, the code presented in the paper can be applied in penetration testing of systems. This research paper not only analyzes the vulnerability, but also demonstrates all the steps of its exploitation, which allows us to develop more effective methods of protecting information systems from such attacks.*

Keywords: *information security, specialist training, automated operation, protection measures, penetration testing, attack simulation, cyberpolygon, Metasploit, Remote Code Execution, Meta Attack Language.*

Введение

На данный момент в области кибербезопасности существует серьезная проблема, связанная с нехваткой практических навыков в обучении специалистов[9] по выявлению и предотвращению инцидентов информационной безопасности [1, 2]. Обычно учебные программы ориентированы на теоретическое обучение, что, безусловно, важно в данной сфере, но недостаточно для эффективного противодействия современным кибератакам. Эта проблема актуальна как для начинающих, так и для более опытных специалистов, поскольку постоянное обновление практических и теоретических знаний, следование последним тенденциям и готовность к новым векторам атак имеют ключевое значение.

Для решения этой задачи существует киберполигон Ampire[10], который представляет собой учебно-тренировочную площадку для проведения массовых киберучений. Основой этой платформы являются имитации реальных кибератак. Ampire позволяет специалистам разрабатывать и оттачивать свои навыки в условиях, максимально приближенных к реальным угрозам и атакам, что делает его важным инструментом для обучения и поддержания актуальности знаний в области кибербезопасности. Для проведения тренировок используются уязвимые узлы. Уязвимый узел – это компьютерная система, которая состоит из двух виртуальных машин, связанных в сети. Одна из этих машин является хостом злоумышленника и используется для проведения автоматизированных атак на вторую машину. Под атакой понимается эксплуатация имеющейся уязвимости в предустановленном программном обеспечении, сервисах или операционной системе второй виртуальной машины. Уязвимый узел используется в обучении и тестировании в области кибербезопасности с целью оценки и усовершенствования защиты информационных систем.

Увеличение количества таких узлов способствует повышению разнообразия изучаемых уязвимостей, что в свою очередь обогащает образовательный процесс и делает его более реалистичным. Это помогает специалистам в области кибербезопасности получать более широкий опыт и быть готовым к новейшим вызовам в области кибербезопасности.

Обзор исследований

Современным методам подготовки специалистов по информационной безопасности уделяется много внимания в научных и исследовательских работах [3–5]. В статье [3] предлагается оборудовать профильные высшие учебные заведения специальными пентест-лабораториями. В работах [4,5] подтверждается важность наличия у специалиста по информационной безопасности готовности принимать активные действия по нейтрализации угрозы. Таким образом, можно понять, что ключевой задачей в области обучения профильных специалистов является получение практических навыков.

Невозможность работы начинающих или еще обучающихся специалистов с реальными инцидентами информационной безопасности обусловила появление новых методов обучения, а именно получения

9 Теории недостаточно: о важности практических навыков при обучении сотрудников кибербезопасности [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/importance-of-practical-skills-in-cybersecurity-training (дата обращения: 16.10.2023).

10 Киберполигон Ampire [Электронный ресурс]. URL: https://amonitoring.ru/ampire-po/ (дата обращения: 29.09.2023).

практических навыков с помощью киберполигонов и соревнований типа Capture the Flag (CTF) [6–8]. В работах [7, 8] целью исследования является изучение соревнований CTF и виртуальных лабораторий как инструментов для получения практических навыков и прикладных умений. В статье [6] выявляется преимущество использования киберполигонов, так как киберполигоны могут быть созданы по образу объектов критической информационной инфраструктуры и больше нацелены на развитие навыков защиты, в то время как CTF предполагает еще и атакующие действия. Киберполигоны зачастую основываются либо на статических шаблонах сетевой инфраструктуры, либо на динамических шаблонах, состоящих из «уязвимых узлов». Здесь же стоит отметить преимущество киберполигонов – доступность обучения. Для тренировки не нужно организовывать мероприятие с двумя командами, а достаточно лишь браузера и нескольких программ (например, для работы с удаленным рабочим столом).

Не менее важным аспектом становится описание и моделирование узлов и сетей, подверженных уязвимостям, а также соответствующих атак. Методам и нотациям формального описания компьютерных атак посвящено немалое количество научных работ [9–14]. В работах [10, 11] объясняется важность выбора правильной методологии для описания угроз информационным системам, в работах [12–14] предлагаются различные подходы к описанию угроз кибербезопасности. Предложенные подходы сравниваются в статье [9], в заключении которой упоминается удобство использования MAL для описания сценариев кибератак.

Реализация уязвимого узла и автоматизированной атаки на него представлена в научной работе [15]. В статье описан механизм исследуемой уязвимости, проведено формальное описание потенциальной компьютерной атаки на узел, а также приведен программный код, позволяющий злоумышленнику провести автоматизированную атаку с помощью модуля из фреймворка Metasploit [16–19]. В работах [16, 17] рассматриваются возможности среды Metasploit Framework, а в работах [18, 19] предлагается использовать фреймворк как средство для автоматизированного пентеста. Таким образом, Metasploit является мощным инструментом и позволяет реализовывать эксплуатации уязвимостей с готовой полезной нагрузкой.

Опубликованные исследования и научные работы позволяют понять, что актуальные уязвимости и соответствующие им атаки возможно описать с помощью существующих методов формального описания, а затем смоделировать автоматизированную атаку на уязвимую систему с помощью фреймворка Metasploit.

Формирование уязвимого узла

В данной работе для создания уязвимого узла используется уязвимость «Adobe ColdFusion Deserialization of Untrusted Data Vulnerability» (CVE-2023-26360), которая была обнаружена 14 марта 2023 года. Adobe опубликовала рекомендации по безопасности с описанием уязвимости, затрагивающей ColdFusion 2021 Update 5 и ColdFusion 2018 Update 15. CVE-2023-26360 – это уязвимость десериализация ненадёжных данных, которая позволяет злоумышленнику удаленно выполнить произвольный код в уязвимой системе. Уязвимость оценивается как критическая, поскольку для её использования не требуется взаимодействие с пользователем [20]. Злоумышленник может использовать эту уязвимость для направления различных полезных нагрузок как на систему в целом, так и на сервер веб-приложения, и делать это без необходимости прохождения проверки аутентификации. Это означает, что атакующий может удалённо выполнить произвольный код на уязвимой системе или сервере без участия или согласия пользователя, а также без необходимости получения прав привилегированного пользователя на сервере [21]. Уязвимости, позволяющие злоумышленникам выполнить код на удаленной системе, считаются одними из наиболее опасных и актуальных в области кибербезопасности.

Суть уязвимости заключается в том, как ColdFusion производит десериализацию ненадежных данных. Для эксплуатации данной уязвимости злоумышленник может отправить на сервер ColdFusion специально сгенерированный запрос, содержащий ненадежные данные, которые в последствии будут десериализованы и выполнены в виде кода. Ход эксплуатации уязвимости зависит от того, какой тип файла используется для обработки. Так, для удаленного выполнения произвольного кода на уязвимой системе злоумышленник может внедрить вредоносные CFML-теги, например, в лог-файл, записи из которого будут преобразованы компилятором NeoTranslator в соответствующие инструкции для выполнения вредоносного кода.

Предварительно, с использованием программного продукта виртуализации VirtualBox, были настроены две виртуальные машины (табл. 1).

Для наглядности конечной целью эксплуатации уязвимости будет являться получение хостом злоумышленника возможности удаленно выполнять код с помощью командной оболочки уязвимого хоста, то есть получение Meterpreter-сессии через TCP-соединение.

Это возможно путем выполнения HTTP-запроса с данными, содержащими произвольные теги CFML. Содержимое этих данных будет записываться в файл журнала ColdFusion. После перевода coldfusion-out.log

Таблица 1

Конфигурация уязвимого узла

Хосты / Компоненты	Злоумышленник	Виртуальная машина с уязвимостью
Операционная система	Kali GNU/ Linux 6.1.0	Ubuntu 22.04.2 LTS
Сетевая конфигурация	inet 10.0.2.11 netmask 255.255.255.0 broadcast 10.0.2.255	inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
Программное обеспечение	msfconsole 6.3.25-dev python 3.11	Adobe ColdFusion 2021 Update 5

файла в формат CFML, выполнятся инструкции, указанные в произвольных тегах CFML, которые после осуществления запроса будут присутствовать в файле журнала.

Для получения Meterpreter-сессии необходимо сгенерировать два HTTP-запроса к серверу. Первый запрос организует точку для подключения на уязвимом узле (удалённо создаст полезную нагрузку и эксплуатирует её, используя оболочку bash). Второй запрос – переведёт файл журнала в формат CFML, что является эксплуатацией уязвимости.

Таким образом, если злоумышленник предварительно запустил хэндлер (программу, ожидающую соединения от жертвы по определённому сокету) – между жертвой и злоумышленником установится вредоносная сессия.

Для оптимизации процесса эксплуатации был выбран такой инструмент для выполнения эксплойтов, как Metasploit[11]. На момент написания статьи в базе знаний Metasploit Framework уже существует модуль «exploit/multi/http/adobe_coldfusion_rce_cve_2023_26360», который содержит в себе код эксплуатации уязвимости на языке Ruby. Для корректной эксплуатации уязвимости необходимо настроить определенные параметры модуля:

1. CFC_ENDPOINT – путь до запрашиваемого целевого CFC-файла.
2. CF_LOGFILE – путь до целевого файла журнала.
3. RHOSTS – адрес уязвимого хоста.
4. RPORT – TCP порт, на котором установлен уязвимый сервер. В рамках представленной эксплуатации подключение к серверу осуществляется по порту 8500.
5. LHOST – адрес локального узла, IP-адрес машины злоумышленника.
6. LPORT – локальный порт. Именно этот порт будет прослушивать злоумышленник, в ожидании установления обратного соединения с жертвой.
7. TARGET – цель для эксплуатации. Выбор цели зависит в основном от целевой ОС и возможностях сессии, получаемой после эксплуатации.

Эксплойт предоставляет возможность получить Meterpreter-сессию через готовый payload, без повышения уровня сессии через shell-соединение. В качестве загружаемой и эксплуатируемой полезной нагрузки был выбран модуль java/meterpreter/reverse_tcp.

В ходе эксплуатации, на машине злоумышленника запускается хэндлер и ждёт входящего подключения по сокету 10.0.2.11:4444. Удалённому серверу будет отправлен POST-запрос к файлу по пути: /cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/iedit.cfc с тэгом method=fxyhppau&_cfclient=true. Это запрос на получение файла iedit.cfc, содержащий некорректные CFML-тэги.

В параметре _variables был передан CFML-код, который создает объект java.net.URL класса Java и инициирует его с заданным адресом. Затем создается массив и класс java.net.URLClassLoader, который загружает класс metasploit.Payload.

Второй запрос преобразует некорректные CFML-тэги в исполняемый код. В результате выполнения этого кода на удаленном сервере эксплуатируется полезная нагрузка «meterpreter/reverse_tcp». Далее, устанавливается связь с TCP-обработчиком на 10.0.2.11:4444. В конечном итоге, между уязвимым сервером и злоумышленником будет установлена Meterpreter-сессия.

Для большей понятности и структурированности при описании эксплуатации уязвимости в данной работе применяется формализация с помощью MAL. Формальное описание способствует более эффективному анализу и обучению, а также упрощает коммуникацию между специалистами разных областей. На рис. 1 представлен мета-граф, который включает в себя следующие элементы [22]:

11 Metasploit Framework [Электронный ресурс]. URL: https://www.metasploit.com/ (дата обращения: 29.09.2023).

1. Активы в системе (большие синие круги): обозначают используемые ресурсы в системе, такие как базы данных компании, рабочая станция администратора и так далее.
2. Логические шаги типа И (красные квадраты): показывают переход между активами и представляют этапы, на которых злоумышленник достигает своих целей, например, несанкционированная регистрация нового пользователя или извлечение информации из базы данных компании.
3. Логические шаги типа ИЛИ (маленькие круги): описывают факторы, благодаря которым атака злоумышленника была успешной, такие как захват прав администратора компьютера или неправильная работа механизма миграции в системе контроля версий Gitea.
4. Шаги защиты (треугольники): отражают возможные меры по предотвращению или противодействию атаке, например, настройка групповой политики безопасности или брандмауэра.
5. Используемые системы (нижние круги оранжевого цвета): указывают на конкретные операционные системы, используемые при успешной атаке, такие как Ubuntu или Astra Linux.

Автоматизированная эксплуатация уязвимости

В рамках выполнения работы стояла задача автоматизации процесса эксплуатации уязвимости. Metasploit Framework состоит из Ruby-скриптов, то есть не поддерживает выполнение Python-скриптов через свою оболочку.

Для решения этой задачи была использована библиотека Pymetasploit. С её помощью можно связываться с Metasploit в программном коде по API с использованием протокола RPC через специализированную службу msfrpcd.

Ниже представлено описание кода для эксплуатации уязвимости и автоматизации действий атакующего на языке Python. В процессе разработки использовался Python 3.11.

Импорт библиотек и установка соединения с msfrpc.

```
import time
from pymetasploit3.msfrpc
import MsfRpcClient, ShellSession, MsfConsole
client = MsfRpcClient 'password', port=55553,
ssl=True)
```

Объявления глобальных переменных. Указанные значения будут использоваться для указания параметров в msfconsole. Если выбранный эксплойт использует корректные параметры по умолчанию – в коде их можно не изменять.

```
RHOSTS = '10.0.2.15'
LHOST = '10.0.2.11'
LPORT = '4444'
```

Объявление и написание функции эксплуатации уязвимости. Здесь происходит организация процесса эксплуатации и настройка параметров msfconsole.

```
def exploit_adobe_cve(config) -> bool:
   exploit = client.modules.use('exploit'
'multi/http/adobe_coldfusion_rce_cve_2023_
26360')
   exploit['RHOSTS'] = 'RHOSTS'
   tries = 5
   pload = client.modules.use('payload', 'java/
meterpreter/reverse_tcp')
   pload['LHOST'] = 'LHOST'
   pload['LPORT'] = 'LPORT'
   for i in range(tries):
      if i >= 1:
         time.sleep(10)
      count = len(client.sessions.list)
```

Рис. 1. – Формальное описание эксплуатации уязвимости с помощью методологии моделирования MAL

```
        exploit.execute(payload=pload)
        if len(client.sessions.list) > count:
            return True
    print('Ошибка эксплуатации')
```

После успешного выполнения скрипта между злоумышленником и уязвимой виртуальной машиной будет установлена Meterpreter-сессия. После этого злоумышленник сможет развивать свой вектор атаки в любом направлении и проводить разнообразные манипуляций как с сервером, так и с самой системой.

Меры защиты

Уязвимости «Adobe ColdFusion Deserialization of Untrusted Data Vulnerability» подвержены системы с функционирующими на них серверами ColdFusion 2021 Update 5 и ColdFusion 2018 Update 15, а также более ранние версии. Одной из мер защиты будет являться установка обновлений безопасности с официального сайта продукта (ColdFusion 2021 Update 6, либо ColdFusion 2018 Update 16 и более поздние версии). В случае, если установка обновлений невозможна или требует времени, можно предпринять самостоятельные меры по усилению безопасности ColdFusion. Одной из таких мер является добавление переменной allowNonCFCDeserialization в код класса JSONUtils.java и добавление проверки на расширение «.cfc» Это реализуемый подход, но требует опыта в разработке и понимания кода ColdFusion.

Второй мерой защиты является отключение компилятора NeoTranslator. Отключение компилятора NeoTranslator не позволит ColdFusion переводить страницы в классы Java.

Предложенные меры защиты относятся к методам защиты от веб-уязвимостей на основе намерений, где под «намерением» подразумевается функциональность, которая должна быть заложена в приложении с учетом целей и решаемых задач [23].

Стоит понимать, что предложенные в данной научной статье меры не являются официальными рекомендациями разработчика и могут ограничивать функциональность ColdFusion. Соответственно, при первой возможности рекомендуется установить обновления от разработчика, которые выпущены специально для устранения критической уязвимости CVE-2023-26360.

Заключение

В результате исследования была детально проанализирована и описана уязвимость «Adobe ColdFusion Deserialization of Untrusted Data Vulnerability» (CVE-2023-26360). Эта уязвимость представляет серьезную угрозу для информационной безопасности, так как позволяет злоумышленникам удаленно выполнять произвольный код на уязвимых серверах ColdFusion. Эксплуатация уязвимости была формально описана с помощью методологии моделирования MAL, что позволит многим специалистам понять последовательность шагов злоумышленника, какие он использовал ресурсы и какие меры противодействия можно предпринять.

Была реализована автоматизированная эксплуатация уязвимости с использованием языка программирования Python и фреймворка Metasploit. Это позволило создать уязвимый узел, который является ценным ресурсом, обеспечивая комплексное и актуальное обучение в киберполигоне. Также практический сценарий атаки может быть использован для оценки уровня защиты системы от подобных угроз. Кроме того, в работе были изложены рекомендации по усилению защиты и описана стратегия для предотвращения атак на Adobe ColdFusion.

Киберполигоны представляют собой перспективное направление в области информационной безопасности, поскольку они играют ключевую роль в повышении уровня подготовки персонала и тестировании на защищенность. Вклад в развитие киберполигонов способствует увеличению компетентных экспертов и приводит к повышению общей безопасности, сокращению успешных кибератак и более надежной защите информационной инфраструктуры.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2023–2025 гг. (проект № FEWM-2023-0015).

Литература

1. *Карпов, Д. С. Повышение качества подготовки специалистов по направлению подготовки «Информационная безопасность» / Д. С. Карпов, А. А. Микрюков, П. А. Козырев // Открытое образование. – 2019. – Т. 23, № 6. – С. 22–29. – DOI 10.21686/1818-4243-2019-6-22-29. – EDN YEMKVN.*
2. *Harjinder L. et al. Pedagogic Challenges in Teaching Cyber Security--a UK Perspective //arXiv preprint arXiv:2212.06584. – 2022.*
3. *Аверьянов, В. С. Pentest – лаборатория для обучения специалистов направления подготовки информационная безопасность / В. С. Аверьянов, И. Н. Карцан // Актуальные проблемы авиации и космонавтики : Сборник материалов VI Международной научно-практической конференции, посвященной Дню космонавтики. В 3-х томах, Красноярск, 13–17 апреля 2020 года / Под общей редакцией Ю. Ю. Логинова. Том 2. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2020. – С. 198–200.*

4. Серпенинов, О. В. Система компетентно-ориентированного обучения специалистов в области информационной безопасности / О. В. Серпенинов // Научный вектор: Сборник научных трудов магистрантов / Под научной редакцией А. У. Альбекова. Том Выпуск 4. – Ростов-на-Дону: Ростовский государственный экономический университет «РИНХ», 2018. – С. 199–202.
5. Меньшенина, С. Г. Структура готовности к профессиональной деятельности специалистов по информационной безопасности / С. Г. Меньшенина // Вестник Самарского государственного технического университета. Серия: Психолого-педагогические науки. – 2018. – № 1(37). – С. 100–107.
6. Ciuperca E., Stanciu A., Cîrnu C. Postmodern education and technological development. Cyber range as a tool for developing cyber security skills //INTED2021 proceedings. – IATED, 2021. – С. 8241–8246.
7. Kornegay M. A., Arafin M. T., Kornegay K. Engaging underrepresented students in cybersecurity using Capture-the-Flag (CTF) competitions (experience) //2021 ASEE Virtual Annual Conference Content Access. – 2021.
8. Karampidis K. et al. Digital Training for Cybersecurity in Industrial Fields via virtual labs and Capture-The-Flag challenges //2023 32nd Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE). – IEEE, 2023. – С. 1–6.
9. Методы формализации описания сценариев кибератак / А. Ю. Якимук, С. А. Устинов, Т. П. Лазарев, А. С. Коваленко // Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. – 2022. – № 1-2. – С. 73–76.
10. A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats / A. Konev, A. Shelupanov, M. Kataev [et al.] // Symmetry. – 2022. – Vol. 14, No. 3. – DOI 10.3390/sym14030549.
11. Computer network threat modelling / A. Novokhrestov, A. Konev, A. Shelupanov, A. Buymov // Journal of Physics: Conference Series, Tomsk, 20–22 ноября 2019 года. – Tomsk, 2020. – P. 012002. – DOI 10.1088/1742-6596/1488/1/012002.
12. Xiong W. et al. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix //Software and Systems Modeling. – 2022. – Т. 21. – №. 1. – С. 157–177.
13. Johnson P., Lagerström R., Ekstedt M. A meta language for threat modeling and attack simulations //Proceedings of the 13th International Conference on Availability, Reliability and Security. – 2018. – С. 1–8.
14. Xiong W., Lagerström R. Threat modeling–A systematic literature review //Computers & security. – 2019. – Т. 84. – С. 53–69.
15. Уязвимость «Gitea Git Fetch Remote Code Execution»: анализ, формализация автоматизированной эксплуатации, меры защиты / А. А. Конев, А. С. Коваленко, В. С. Репкин, Г. Ю. Семенов // Вестник УрФО. Безопасность в информационной сфере. – 2023. – № 2(48). – С. 67–73. – DOI 10.14529/secur230207.
16. Ромейко, Д. А. Обзор возможностей среды Metasploit Framework / Д. А. Ромейко, Т. И. Паюсова // Математическое и информационное моделирование : материалы Всероссийской конференции молодых ученых, Тюмень, 18–23 мая 2022 года / Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Институт математики и компьютерных наук. Том Выпуск 20. – Тюмень: ТюмГУ-Press, 2022. – С. 318–325.
17. Khera Y. et al. Analysis and impact of vulnerability assessment and penetration testing //2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). – IEEE, 2019. – С. 525–530.
18. Valea O., Oprişa C. Towards pentesting automation using the metasploit framework //2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP). – IEEE, 2020. – С. 171–178.
19. Raj S., Walia N. K. A study on metasploit framework: A pen-testing tool //2020 International Conference on Computational Performance Evaluation (ComPE). – IEEE, 2020. – С. 296–302.
20. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments //Energy Reports. – 2021. – Т. 7. – С. 8176–8186.
21. Biswas S. et al. A study on remote code execution vulnerability in web applications //International Conference on Cyber Security and Computer Science (ICONCS 2018). – 2018. – С. 50–57.
22. Wideł W., Mukherjee P., Ekstedt M. Security Countermeasures Selection Using the Meta Attack Language and Probabilistic Attack Graphs //IEEE Access. – 2022. – Т. 10. – С. 89645–89662.
23. Методы защиты веб-приложений от злоумышленников / В. Е. Боровков, П. Г. Ключарев, // Вопросы кибербезопасности – 2023. – № 5(57). – С. 89–99. – DOI 10.21681/2311-3456-2023-5-89-99.