

УДК 004.056.5

Д. А. ГОЛУБЕНКО, В. С. ДРОБЫШЕВСКИЙ (ЭМ-21)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. С. ТАТУР

«ШВЕЙЦАРСКИЙ НОЖ» КИБЕРБЕЗОПАСНОСТИ CYBERCHEF

Рассматривается веб-приложение CyberChef с открытым исходным кодом, разработанное в британском центре правительственной связи GCHQ. Описываются полностью клиентская архитектура, обеспечивающая конфиденциальность данных, и основные категории операций (кодирование, криптография, сжатие, извлечение индикаторов). Приводятся практические рецепты для анализа фишинговых писем и расшифровки обфусцированных PowerShell-скриптов. Показывается, что CyberChef сокращает время рутинного анализа в несколько раз и может использоваться как средство обучения. Обосновывается необходимость включения инструмента в арсенал аналитика центра мониторинга информационной безопасности (SOC).

Специалист SOC ежедневно сталкивается с десятками разнородных задач: декодирование Base64, расшифровка сетевого трафика, извлечение IP-адресов из логов, распаковка вложений фишинговых писем. Традиционный подход требует использования множества консольных утилит (Base64, Openssl, Strings) или написания одноразовых скриптов. Это снижает скорость реакции на инциденты и повышает риск ошибок.

В 2016 году аналитик британского центра правительственной связи GCHQ опубликовал на GitHub проект CyberChef – веб-приложение, объединяющее более 300 операций обработки данных в едином интерфейсе. Инструмент быстро получил неофициальное название «кибершвейцарский нож». Цель данной работы – показать возможности CyberChef для практического применения в деятельности аналитика SOC и цифрового криминалиста.

CyberChef создан в рамках «10 % инновационного времени» сотрудника GCHQ. В ноябре 2016 года исходный код был открыт под лицензией Apache 2.0. К 2026 году проект насобирал более 32 тысяч звёзд на GitHub, число уникальных пользователей превысило 1,4 миллиона. Принципиальной особенностью является полностью клиентская архитектура: все операции выполняются в браузере пользователя на JavaScript. Данные не покидают компьютер, что критически важно при работе с конфиденциальной информацией (образцы вредоносного ПО, внутренние логи). CyberChef может работать полностью автономно – достаточно один раз скачать HTML-файл.

Интерфейс состоит из четырёх зон: панель операций (с поиском по

названиям), центральная панель рецепта (цепочка операций), поле ввода и поле вывода. Результат пересчитывается мгновенно (Auto Bake). Рецепт можно сохранить в файл или передать коллеге уникальной ссылкой. Существуют официальный Docker-образ и пакет для Node.js, что позволяет вернуть инструмент в корпоративной среде.

Наиболее востребованы следующие группы.

1 Кодирование/декодирование: Base32/64/85, URL, HTML, шестнадцатеричные представления, конвертация текстовых кодировок (UTF-8, Windows-1251 и др.).

2 Криптография и хеширование: AES (128/192/256 бит, режимы CBC, GCM), Triple DES, RSA, XOR, MD5, SHA-1/256, BLAKE2. Важно: криптооперации предназначены для анализа, а не для защиты реальных данных.

3 Сжатие: Gunzip, Unzip, Raw Inflate, Untar позволяют распаковывать многослойные архивы.

4 Сетевые структуры: парсинг URL, IP-адресов, доменов, email; разбор X.509 сертификатов.

5 Извлечение информации: Strings (аналог Unix), регулярные выражения, извлечение метаданных, стеганография.

6 Magic: автоматический подбор цепочки декодирования из десятков вариантов – идеальный первый шаг при неизвестном формате.

Рассмотрим два типовых сценария.

Анализ фишингового письма. Копируем тело письма в поле ввода. Добавляем операции «Extract URLs» и «Extract Email Addresses» – получаем все индикаторы. Далее находим вложение в кодировке Base64, применяем «From Base64», затем «Detect File Type» (определяем ZIP), затем «Unzip». Финальный шаг – «Hash» (SHA-256) для проверки по базам IOC. Весь цикл занимает менее минуты.

Расшифровка обфусцированного PowerShell. Команда с ключом «-enc» содержит строку Base64. Применяем «From Base64» в режиме выдачи байтов, затем «Decode text» с принудительной кодировкой UTF-16LE. Получаем читаемый скрипт, который может содержать вложенные слои. Ручной разбор такого скрипта занял бы 10–15 минут, в CyberChef – менее минуты.

CyberChef не заменяет полноценные криптографические библиотеки для защиты реальных данных. Работа с файлами более 2 ГБ может быть некомфортна в браузере (лучше использовать Node.js-версию). Однако для повседневных задач SOC и DFIR он заменяет десятки консольных утилит, обеспечивая наглядность и воспроизводимость. Инструмент активно используется в учебных курсах по кибербезопасности: преподаватели в реальном времени демонстрируют действие AES, хеш-функций, стеганографии. Студенты выполняют лабораторные работы без установки дополнительного ПО. CyberChef стал стандартом на соревнованиях CTF (Capture The Flag) для задач многоступенчатого декодирования.

CyberChef – уникальный open-source проект, вышедший из недр спец-

службы и ставший мировым стандартом для быстрой обработки данных в кибербезопасности. Его ключевые преимущества: полная безопасность (клиентская обработка), интуитивность (drag-and-drop рецепты), масштабируемость (от веб-версии до Docker в корпоративном периметре). Разработанные в работе рецепты могут быть непосредственно применены в деятельности SOC, а сам инструмент рекомендован для включения в «джентльменский» набор аналитика информационной безопасности. Попробуйте операцию Magic на первой попавшейся подозрительной строке – и вы поймёте, почему CyberChef называют кибершвейцарским ножом.

СПИСОК ЛИТЕРАТУРЫ

- 1 CyberChef : The Cyber Swiss Army Knife // GitHub. – URL: <https://github.com/gchq/CyberChef> (date of access: 28.04.2026).
- 2 CyberChef Live Demo // GCHQ. – URL: <https://gchq.github.io/CyberChef/> (date of access: 28.04.2026).
- 3 **Давыдова, А.** CyberChef – швейцарский кибер-нож / А. Давыдова // Codeby.net. – 2024. – URL: <https://codeby.net/blogs/cyberchef-shvejsarskij-kiber-nozh/> (дата обращения: 28.04.2026).
- 4 CyberChef – инструмент, который заменяет десятки утилит // Хабр. – URL: <https://habr.com/ru/articles/cyberchef-instrument/> (дата обращения: 28.04.2026).
- 5 SANS Digital Forensics and Incident Response Poster // SANS Institute. – URL: <https://www.sans.org/posters/windows-forensic-analysis/> (date of access: 28.04.2026).

Получено 27.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 621.314

М. Е. ГОНЧАРОВ, В. Ю. АШУРКО (ЭМ-31)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. В. КИСЕЛЕВА

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОЦЕССАХ DEVOPS

Рассматриваются методологические и архитектурные аспекты интеграции технологий искусственного интеллекта в DevOps-практики (концепция AIOps). Проведён анализ стека наблюдаемости, пайплайнов обработки телеметрии и роли MLOps в управлении жизненным циклом моделей. Представлена методология оценки эффективности на основе количественных метрик (FPR, MTTR, TCO). Рассмотрены риски информационной безопасности, связанные с использованием генеративных моделей и систем автоматического реагирования, а также сформулированы требования к качеству данных и верификации алгоритмов.