УДК 004.056:005.942 Вестник УрФО № 2(56) / 2025, с. 74–79

Новиков Г. А., Кузьмин А. А., Кузьмина У. В. DOI: 10.14529/secur250208

ПРИМЕНЕНИЕ МЕТОДОВ ХАОС-ИНЖИНИРИНГА В ИНФРАСТРУКТУРЕ ОТДЕЛА ИБ ПРЕДПРИЯТИЯ

Статья посвящена исследованию применения хаос инжиниринга в контексте информационной безопасности. На основе созданного цифрового двойника бизнес-процесса обеспечения информационной безопасности организации проводится тестирование реакций систем защиты. В статье описана методика развертывания тестовой среды, сбор метрик и проведения ручных тестов с последующей автоматизацией инцидентов. Результаты исследования демонстрируют потенциал использования данного подхода для повышения устойчивости систем безопасности.

Ключевые слова: *хаос инжиниринг, информационная безопасность, цифровой двойник, SIEM, IPS/IDS, DLP.*

Novikov G. A., Kuzmin A. A., Kuzmina U. V.

THE USE OF CHAOS ENGINEERING METHODS IN THE INFRASTRUCTURE OF THE INFORMATION SECURITY DEPARTMENT OF THE ENTERPRISE

The article is devoted to the study of the application of chaos engineering in the context of information security. Based on the created digital twin of the organization's information security business process, the reactions of security systems are being tested. The article describes the methodology for deploying the test environment, collecting metrics and conducting manual tests with subsequent incident automation. The results of the study demonstrate the potential of using this approach to increase the stability of security systems.

Keywords: *chaos engineering, information security, digital twin, SIEM, IPS/IDS, DLP.*

Введение

Современные информационные системы имеют сложную распределенную архитектуру. Традиционные методы тестирования и аудита безопасности часто не способны обнаружить скрытые уязвимости, которые могут быть выявлены лишь в условиях реальных инцидентов. Хаос инжиниринг, зародившийся для тестирования распределенных систем (на примере Chaos Monkey от Netflix), сегодня активно применяется для имитации отказов и проверки реакции систем в условиях неопределенности. В данной статье предлагается концепция применения хаос инжиниринга в области информационной безопасности, когда наряду с техническими сбоями моделируются атаки, утечки данных и иные инциденты, способные проверить работоспособность технических средств защиты.

Особое внимание уделяется необходимости создания цифрового двойника – виртуальной копии бизнес-процесса обеспечения информационной безопасности организации, где моделируются все ключевые процессы. Такой цифровой двойник позволяет проводить тесты и эксперименты без риска для боевой инфраструктуры.

В контексте информационной безопасности такой подход может помочь не только оценить настройку технических средств защиты, но и протестировать оперативную реакцию ИБ-команды на инциденты [1]. Цифровой двойник по-зволяет проводить испытания, не подвергая риску реальную инфраструктуру [2].

Цель исследования – оценка эффективности тестовых сценариев хаос инжиниринга на основе разработанной методологии создания тестовой среды цифрового двойника отдела информационной безопасности.

Задачи исследования:

1. Разработка методологии развертывания цифрового двойника отдела информационной безопасности.

2. Развертывание тестовой среды цифрового двойника бизнес-процесса обеспечения информационной безопасности организации.

3. Проведение ручного тестирования и оценка реакции системы на атаку.

В данной статье рассмотрим разработку методологии развертывания цифрового двойника отдела информационной безопасности. Перед развертыванием цифрового двойника необходимо определить его архитектуру, функциональные требования и цели тестирования. Основные вопросы, которые следует учитывать:

- Какие бизнес-процессы должны быть смоделированы?
- Какие компоненты инфраструктуры необходимо включить?
- Какие инциденты будут тестироваться?
- Какие метрики будут собираться?

Методология развертывания цифрового двойника включает в себя несколько ключевых этапов, одним из которых является определение границ моделируемой системы. Важно отметить, что для создания адекватного цифрового двойника не требуется полное воспроизведение всей инфраструктуры организации. Современные компании, особенно крупные предприятия, обладают разветвленной IT-инфраструктурой, включающей в себя множество взаимосвя-занных сервисов, сетевых сегментов и вычислительных мощностей. Однако для успешного функционирования цифрового двойника достаточно включить в его состав только те элементы, которые непосредственно задействованы в функционировании одного или нескольких ключевых бизнес-процессов. Такой подход позволяет оптимизировать вычислительные ресурсы, снизить затраты на развертывание и управление двойником, а также сосредоточиться на моделировании именно тех аспектов системы, которые имеют наибольшее значение для анализа и тестирования.

Поэтому была выделены основная функциональная область:

• Мониторинг активности пользователей, анализ логов, сработки систем защиты (SIEM, IDS/IPS, DLP) и реакцию системы на выявленные угрозы.

Многие современные корпоративные сервисы изначально проектируются и разворачиваются в виртуальных средах, будь то частные облака, контейнерные платформы или традиционные гипервизоры. Это означает, что создание цифрового двойника может быть реализовано путем репликации уже имеющихся виртуальных машин и контейнеров, что существенно снижает временные и финансовые затраты на его построение.

Цифровой двойник построен с учетом принципов сегментирования сети, многоуровневой защиты и контроля доступа и состоит из следующих компо-нентов (см. рисунок 1):

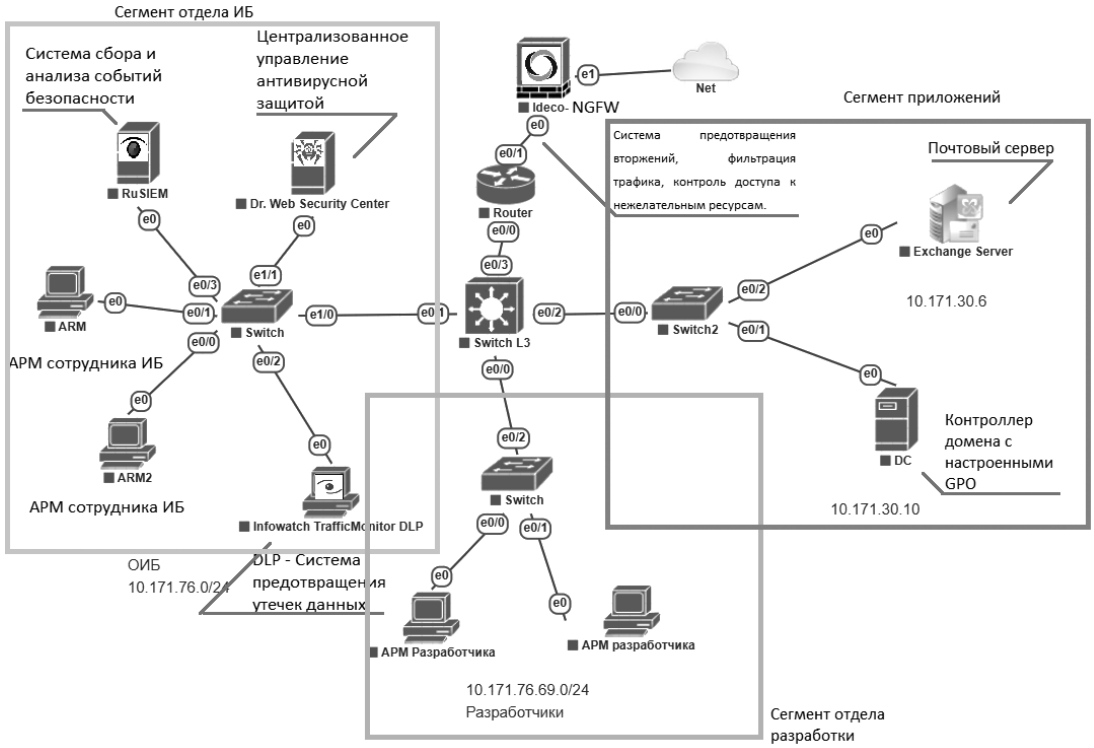

Рис. 1. Схема сети цифрового двойника

Для тестовой среды выделена изолированная сеть с подсетью 10.171.0.0/16, в которой размещены все компоненты цифрового двойника. Такое решение позволяет отслеживать сетевую активность, моделировать атаки и анализировать их последствия без риска воздействия на рабочую инфраструктуру. [3]

Для оценки эффективности защиты в тестовой среде определены сле-дующие сценарии атак:

• Тестирование механизма предотвращения утечек данных с использованием InfoWatch DLP.

• Анализ сработок IDS/IPS при моделировании аномального сетевого трафика.

• Проверка работы антивирусных решений при загрузке вредоносных файлов.

• Тестирование срабатывания правил SIEM и отображения событий.

•

Основные этапы разработанной методологии тестирования инцидентов на основе хаос-инжиниринга:

• Описывается сценарий инцидента. Например, симуляция заражения сети «червем» или утечка данных посредством генерации большого объема исходящего трафика.

• Формируются ожидания от эксперимента. Например, сработки или несработки, ожидания от реакции системы.

• Определяются метрики реакции. Задаются ключевые показатели: время обнаружения инцидента (фиксируется системой SIEM), скорость восстановления системы, число ложных срабатываний и эффективность оповещений.

• Проводится имитация инцидента вручную. Администратор вручную запускает сценарий, наблюдая за работой системы и сбором метрик через интегрированный центр.

• Проверка ожидаемого результата и реального, если вдруг что-то пошло не так, это выявит аномалию.

•

Ход эксперимента:

В рамках исследования устойчивости корпоративной инфраструктуры к целевым атакам смоделирован сценарий компрометации сети через легитимные учетные данные с последующим запуском вируса-шифровальщика. Эксперимент проводился в изолированном тестовом окружении, повторяющем инфраструктуру организации, фазы атаки и реакция систем безопасности представлены на рисунке 2.[4]

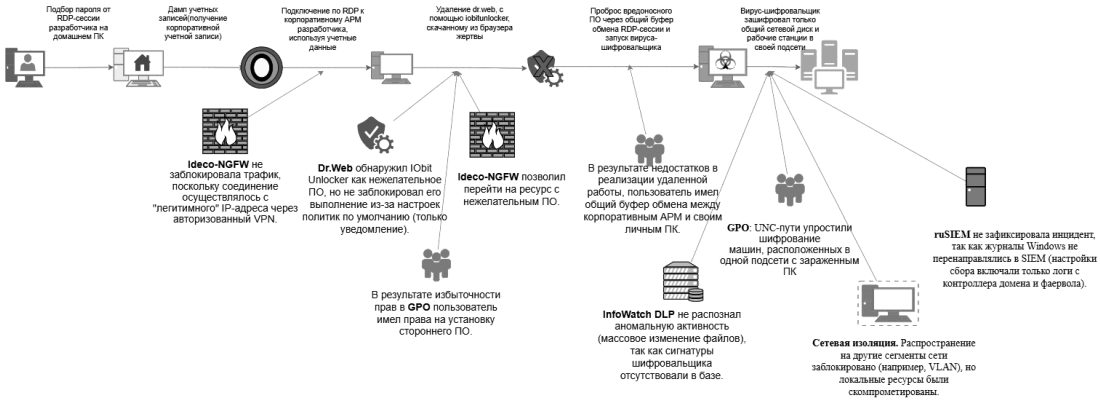

Рис. 2. Фазы атаки и реакция систем защиты

В ходе эксперимента были выявлены следующие критические уязвимости инфраструктуры:

• Антивирусная защита продемонстрировала недостаточную эффективность: продукт Dr.Web функционировал на базовых политиках, не настроенных на блокировку потенциально нежелательных приложений (PUA).

• Конфигурация групповых политик (GPO) содержала ряд ошибок. В частности, политики безопасности разрешали установку неподписанного программного обеспечения, включая такие утилиты, как IObit Unlocker. Активация общего буфера обмена между локальными и удалёнными машинами при под-ключении через RDP создала канал для передачи вредоносного кода. Дополнительным риском стало отсутствие двухфакторной аутентификации для RDP-сессий, что упростило несанкционированный доступ.

• Системы мониторинга не обеспечили должного уровня контроля. Платформа ruSIEM не агрегировала логи с рабочих станций, что сделало невидимыми ключевые события: удаление антивирусного ПО, запуск шифроваль-щика и очистку журналов. Решение InfoWatch DLP не отслеживало аномальные паттерны доступа к данным, включая массовое изменение тысяч файлов, что позволило злоумышленникам действовать без обнаружения.

• Сетевая архитектура также имела существенные недостатки. Наличие открытых SMB-ресурсов (включая административные шары типа C$) упростило горизонтальное перемещение внутри сети. Система Ideco не блокировала загрузку подозрительных утилит, так как исключения для «ресурсов разработчиков» отсутствовали в правилах фильтрации. Кроме того, неконтролируемые VPN-сессии не разрывались при длительном простое, создавая дополнительные векторы для атак.

Результаты:

• Частичный успех защиты: Сетевая изоляция предотвратила катастрофическое распространение шифровальщика, а зашифрованные данные удалось восстановить из бекапов.

• Ложная легитимность: Действия злоумышленника (использование валидных учетных данных, штатных утилит) не вызывали подозрений у большинства систем.

• Несоответствие политик: GPO, разрешающие управление службами и установку ПО, противоречили принципу минимальных привилегий.

• Как можно увидеть в результате проведенного эксперимента, шифрования избежать не удалось, хотя злоумышленника можно было отсечь на каждом из этапов, эти несовершенства СЗИ были выявлены, благодаря эксперименту в виртуальной среде, что позволило усилить безопасность организации, поскольку были обозначены дыры в безопасности.

Основные преимущества методологии.

Цифровой двойник отдела информационной безопасности предоставляет уникальную возможность для проведения тестовых сценариев без риска для реальной инфраструктуры. Среди основных преимуществ можно выделить:

• Безопасность эксперимента.
• Комплексное тестирование процессов.
• Гибкость и масштабируемость.

Заключение

В статье представлена комплексная методология применения хаос инжи-ниринга для обеспечения информационной безопасности с использованием цифрового двойника и интегрированного центра сбора метрик. На основе которой проведено дальнейшее развертывание тестовой среды, имитирующей работу бизнес-процесса обеспечения информационной безопасности организации, которая позволяет проводить эксперименты по моделированию различных ин-цидентов, таких как заражение вредоносным ПО, утечка данных, DoS-атаки и фишинговые атаки.

Для развертывания тестовой среды была использована виртуализационная платформа PNetLab, которая позволила создать изолированное окружение и минимизировать влияние экспериментов на рабочие системы. Для обеспечения гибкости и отказоустойчивости реализована возможность быстрого восстановления (rollback) тестовой среды после проведения экспериментов.

Таким образом, применение хаос инжиниринга в сфере информационной безопасности представляет собой перспективное направление, способное повысить уровень защиты корпоративных систем за счет выявления скрытых уязвимостей, оптимизации процессов реагирования и непрерывного совершенствования мер безопасности.

Литература

1. Розенталь Кейси, Джонс Нора Хаос-инжиниринг / К. Розенталь, Н. Джонс - 1-е изд. – Москва: Изд-во ДМК Пресс, 2021. - 284 с.

2. Digital Twin — цифровая копия физической системы // Хабр URL: https://habr.com/ru/articles/887936/ (дата обращения: 05.02.2025).

3. Афанасьева С.В., Кузьмина У.В. Основные проблемы при создании и обслуживании центров мониторинга информационной безопасности // Безо-пасность информационного пространства: сборник научных трудов XXI Все-российской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2023. С. 29-31.

4. Chaos Engineering: искусство умышленного разрушения. Часть 1 // Хабр URL: https://habr.com/ru/companies/flant/articles/460367/ (дата обращения: 02.02.2025).

5. Кузьмина У.В., Абзалутдинов Д.Р., Бараков К.Я. Создание модуля киберполигона, имитирующего компьютерные атаки // Актуальные проблемы современной науки, техники и образования. 2023. Т. 14. № 1. С. 54-57.

References

1. Keysi Rozental', Nora Dzhons Khaos-inzhiniring. - 1 izd. - DMK Press, 2021. - 284 s.

2. Digital Twin — tsifrovaya kopiya fizicheskoy sistemy // Khabr URL: https://habr.com/ru/articles/887936/ (data obrashcheniya: 05.02.2025).

3. Afanas'eva S.V., Kuz'mina U.V. Osnovnye problemy pri sozdanii i ob-sluzhivanii tsentrov monitoringa informatsionnoy bezopasnosti // Bez-opasnost' in-formatsionnogo prostranstva: sbornik nauchnykh trudov XXI Vse-rossiyskoy nauch-no-prakticheskoy konferentsii studentov, aspirantov i molo-dykh uchenykh. Ekate-rinburg, 2023. S. 29-31

4. Chaos Engineering: iskusstvo umyshlennogo razrusheniya. Chast' 1 // Khabr URL: https://habr.com/ru/companies/flant/articles/460367/ (data obrashche-niya: 02.02.2025).

5. Kuzmina U.V., Abzalutdinov D.R., Barakov K.Ya. Creation of a cyber range module simulating computer attacks // Actual problems of modern science, technology and education. 2023. Vol. 14. No. 1. P. 54-57.

КУЗЬМИН Александр Андреевич, студент кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: kuzminsa2002@gmail.com

НОВИКОВ Глеб Александрович, студент кафедры информатики и ин-формационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Лени-на, 38. E-mail: glebbuns@gmail.com

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: Ylianapost@gmail.com

KUZMIN Alexander Andreevich, student of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. No-sov". 455000, Magnitogorsk, Lenin Ave., 38. Email: kuzminsa2002@gmail.com

NOVIKOV Gleb Alexandrovich, student of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. No-sov". 455000, Magnitogorsk, Lenin Ave., 38. Email: glebbuns@gmail.com

KUZMINA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. Nosov". 455000, Magnitogorsk, Len-in Ave., 38. Email: Ylianapost@gmail.com