УДК 004.056.5 Вестник УрФО № 2(60) / 2026, с. 68–75

Никонов В.В., Трофимов И.А.

DOI: 10.14529/secur260207

МНОГОУРОВНЕВАЯ ЗАЩИТА КОРПОРАТИВНЫХ СЕТЕЙ: МОДЕЛИ МОНИТОРИНГА И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

Целью исследования является разработка методологических основ и организационно-технического комплекса для непрерывного контроля, раннего выявления и нейтрализации современных киберугроз. На базе системного анализа векторов компрометации (DNS-спуфинг, уязвимости нулевого дня, эксплуатация IoT-сегмента) предложены модели мониторинга сетевого трафика, алгоритмы внедрения криптографической верификации DNS-записей и архитектура многоуровневой защиты. В результате сформирован структурированный регламент реагирования на инциденты и разработана матрица практических мероприятий с распределением зон ответственности, периодичностью контроля и механизмами аудита. Обоснована эффективность интеграции поведенческого анализа, автоматизированных систем обнаружения аномалий и криптографических протоколов для минимизации поверхности атаки. Практическая значимость работы заключается в возможности адаптации предложенного комплекса для внедрения в политики информационной безопасности организаций, что способствует повышению операционной устойчивости, снижению рисков утечки данных и соответствию актуальным нормативным требованиям.

Ключевые слова: *кибербезопасность, методы мониторинга, DNS spoofing, атаки нулевого дня, IoT-устройства, защита сети, системы обнаружения и предотвращения вторжений, многоуровневая система безопасности, информационная безопасность, защита данных, угрозы в компьютерных сетях.*

MULTI-LEVEL PROTECTION OF CORPORATE NETWORKS: MONITORING MODELS AND ORGANIZATIONAL AND TECHNICAL MEASURES TO COUNTER THREATS

The aim of this study is to develop a methodological framework and organizational and technical framework for continuous monitoring, early detection, and mitigation of modern cyberthreats. Based on a systemic analysis of compromise vectors (DNS spoofing, zero-day vulnerabilities, IoT segment exploitation), network traffic monitoring models, algorithms for implementing cryptographic verification of DNS records, and a multi-layered defense architecture are proposed. As a result, a structured incident response procedure has been developed and a matrix of practical measures has been developed, assigning responsibilities, monitoring frequency, and audit mechanisms. The effectiveness of integrating behavioral analysis, automated anomaly detection systems, and cryptographic protocols to minimize the attack surface is substantiated. The practical significance of this work lies in the adaptability of the proposed framework for implementation into organizations' information security policies, which contributes to increased operational resilience, reduced risks of data leakage, and compliance with current regulatory requirements.

Keywords: *cybersecurity, monitoring methods, DNS spoofing, zero-day attacks, IoT devices, network protection, intrusion detection and prevention systems, multi-layered security, information security, data protection, threats in computer networks.*

Введение

В настоящее время в цифровой среде компьютерные сети сталкиваются с множеством опасных киберугроз, которые постоянно совершенствуются и для того, чтобы минимизировать риск атаки на системы необходимо методы защиты и повышать уровень кибербезопасности. Одним из таких видов атак являются DNS spoofing или отравление DNS-кэша.

Данный вид атаки реализуется, когда DNS кэш заполняется фальшивыми данными и в результате чего пользователь попадает на вредоносный сайт. Когда происходит отравление DNS-кэша сервер кэша DNS сохраняет поддельный адрес, который предоставил злоумышленник пользователю, а затем передает его пользователям, которые запрашивают настоящий веб-сайт. Главная опасность DNS спуфинга заключается в том, что его очень трудно обнаружить и он может оказать отрицательное влияние на востребованные веб-сайты с большим количеством зарегистрированных пользователей. Это создает огромный риск для таких сфер, как банковская, электронная коммерция и т. д.

Например, предположим, что злоумышленнику удается изменить DNS-записи и IP-адреса для организации. После этих действий они направляют свой запрос на соседний сервер с поддельным IP-адресом, который контролирует злоумышленник. Пользователь, который захочет получить доступ к настоящему сайту организации, будет перенаправлен на поддельный адрес, который содержит вредоносное программное обеспе-

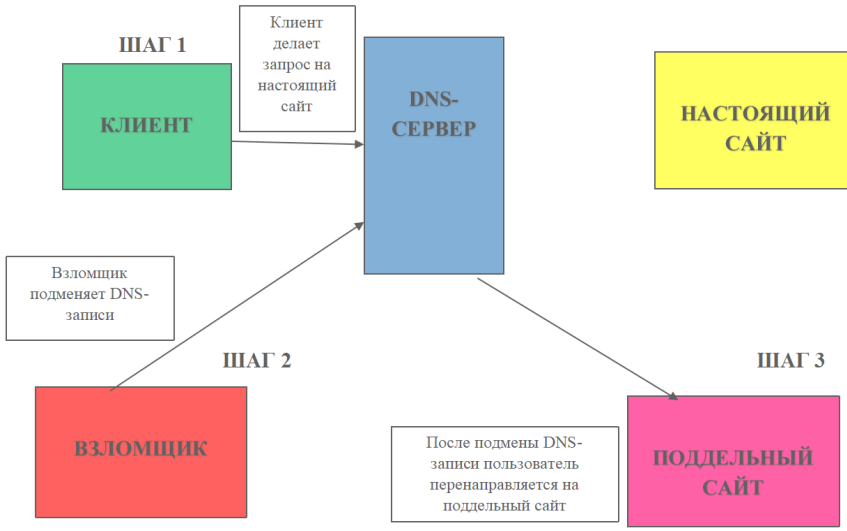

Рис. 1. Процесс реализации DNS-спуфинга

чение для кражи конфиденциальной информации.

Чтобы предотвратить данную атаку необходимо осуществлять мониторинг данных DNS это может помочь установить наличие в трафике отклоняющихся явлений, действий пользователей. Обнаружение отравления DNS-кэшем является сложным процессом, существует несколько мер безопасности, которые необходимо принять, чтобы предотвратить данную атаку. Мера, предотвращающая отравление DNS-кэша, включает в себя использование DNSSEC, отключение рекурсивных запросов и т. д.

DNSSEC (расширения безопасности системы доменных имен) – использует криптографию с открытым ключом для подписи DNS-записей для этого добавляется функция проверки и позволяют системам определять, является ли адрес настоящим или фальшивым. Это поможет проверить и аутентифицировать подлинность запросов и предотвратить подделку.

Отравление кэш-памяти DNS это атака, которую злоумышленник перенаправляет пользователей на вредоносные сайты. Управляемые взломщиками серверы могут ввести в заблуждение пользователей тем самым участники ничего не подозревая скачивают вредоносное программное обеспечение или предоставляют конфиденциальные данные. Чтобы защититься от данной угрозы, необходимо применить методы защиты и обеспечить безопасность DNS-инфраструктуры.

Еще одной из ключевых атак является атака нулевого дня. Атака нулевого дня (zero-day) — это атака, к которой никто не готов. Уязвимость нулевого дня – это ошибка в программном обеспечении, о которой не знает производитель.

Данная уязвимость нулевого дня дает атакующему преимущество во времени. Чтобы реализовать защиту от уязвимостей нулевого дня необходима многоуровневая система защиты, которая включает в себя регулярное обновление программного обеспечения, внедрение систем обнаружения и предотвращения вторжений. Для того, чтобы снизить риск необходимо придерживаться следующих правил.

Схема демонстрирует этапы по предотвращению атаки нулевого дня. Она показывает какие этапы необходимы, чтобы организовать комплексную защиту системы, выявлять уязвимости на ранних этапах и быстро реагировать на угрозы. Каждый ее компонент необходим для создания многоуровневой системы безопасности, которая минимизирует риски эксплуатации нулевых уязвимостей.

Уязвимость нулевого дня – это проверка процессов и архитектуры. При недостаточном анализе процессов, архитектуры и контроля за безопасностью подвергается риску вся инфраструктура. Чтобы минимизировать риск необходимо выполнять следующие этапы - регулярно проводить аудит архитектуры, внедрять многоуровневую защиту, проводить пентесты на уязвимые места и подготовить систему к быстрому реагированию при обнаружении уязвимостей.

Рассмотрим пример атаки на внутренние сети с помощью компрометированных IoT-устройств – это взлом устройств интернета вещей (камеры видеонаблюдения, термоста-

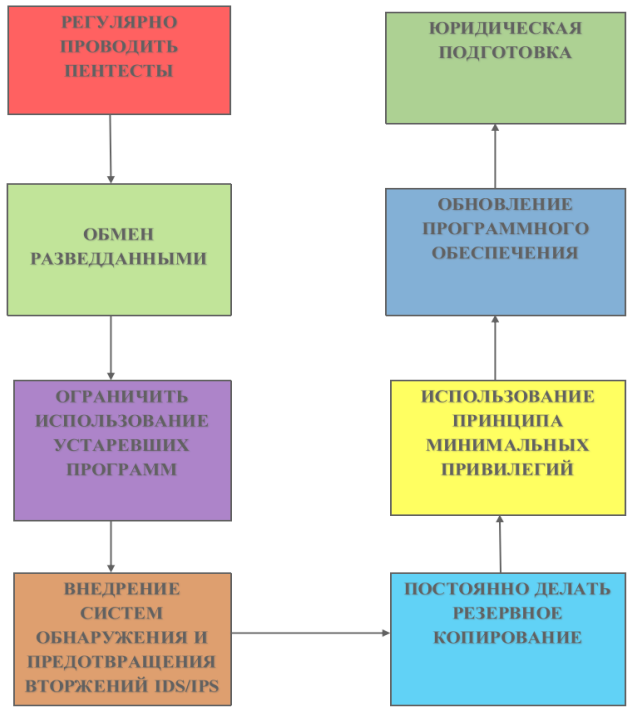

Рис. 2. Этапы, необходимые для минимизации атаки нулевого дня

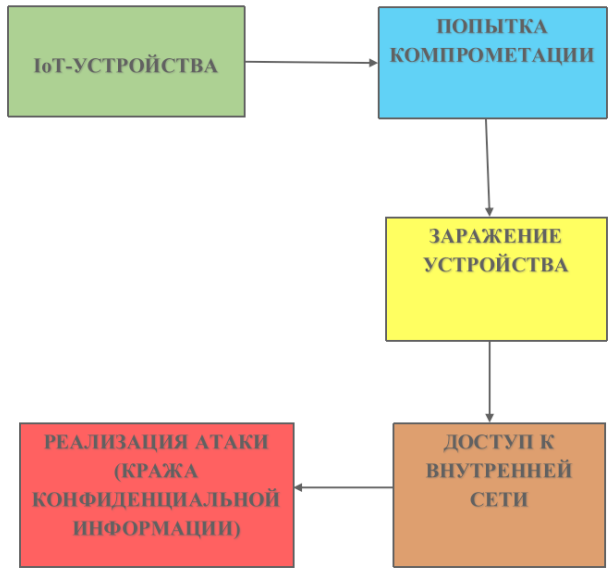

Рис. 3. Этапы атаки с помощью компрометированных IoT-устройств.

ты и другие гаджеты) для получения доступа к корпоративной сети.

Схема предназначена для визуализации процесса угрозы, связанной с использованием IoT-устройств в внутренней сети организации. Она помогает понять, как уязвимости в IoT-устройствах могут привести к серьезным последствиям начиная от взлома и формирования «ботнетов» до получения доступа злоумышленников к внутренним системам.

Данная схема демонстрирует меры защиты сети для обеспечения безопасности IoT-устройств, для организации многоуровневой защиты инфраструктуры и внутренней сети. Она показывает последовательность и взаимосвязь ключевых мер, направленных на снижение рисков и предотвращение атак.

Таким образом, правильная конфигурация каждой из представленных мер позволяют сформировать надежную защиту сети, снизить вероятность успешных атак и быстро реагировать на инциденты. Это обеспечивает

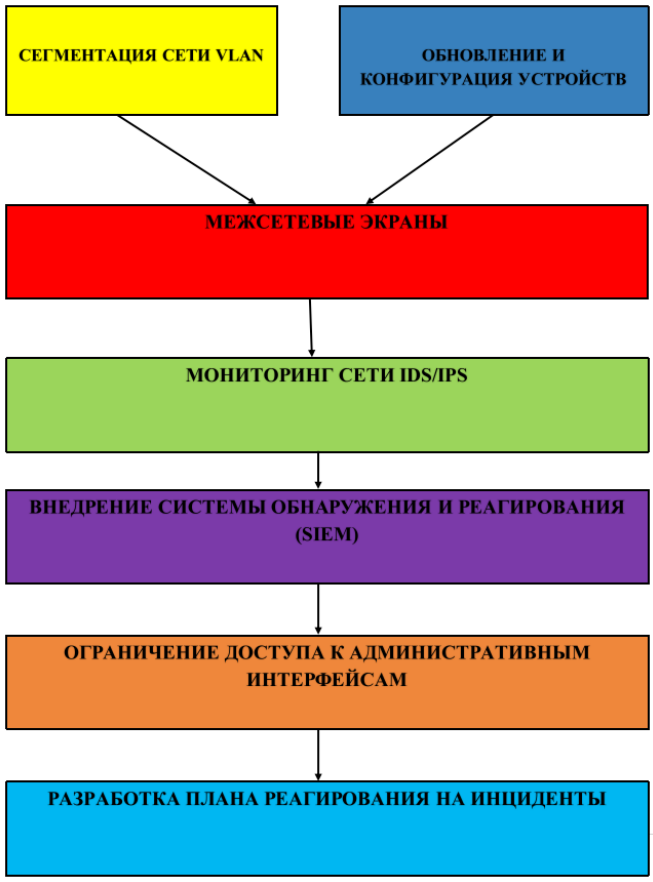

Рис. 4. Меры защиты сети

Таблица 1

Рекомендации для повышения уровня защиты информационной инфраструктуры. План мер по информационной безопасности

РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	ОПИСАНИЕ	ЛИЦА, ОТВЕЧАЮЩИЕ ЗА ВЫПОЛНЕНИЕ РЕКОМЕНДАЦИЙ	ПЕРИОДИЧНОСТЬ ВЫПОЛНЕНИЯ
Внедрение многоуровневой системы защиты	Использование межсетевых экранов, VPN и т. д.	Администраторы сети, инженеры по информационной безопасности	Постоянно, при любых изменениях
Обновление программного обеспечения	Обновление ОС, приложений для минимизации уязвимостей	Системные администраторы и т. д.	Ежемесячно, как только будет совершенно обновление
Проводить пентесты и аудит безопасности	Тестирование уязвимостей	Внутренние специалисты по аудиту, которые помогают устранять внутренние риски, улучшать процессы в соответствии стандартам. Внешние специалисты по аудиту – независимая проверка они обеспечивают независимость и объективность оценки	Раз в полгода

Продол. табл. 1

Разработка и тестирование планов реагирования	Отработка сценариев реагирования на инциденты	Руководитель по ИБ, команда для быстрого реагирования на происшествие	Раз в год после того, как произойдет обновление политики внутреннего контроля и аудита

стабильную работу информационной системы, защищает конфиденциальность данных и способствует выполнению требований безопасности в организации. В результате создается многоуровневая система защиты, которая адаптирована к современным угрозам и обеспечивает высокий уровень безопасности всей инфраструктуры.

Рассмотренные в статье угрозы являются совокупностью атак наиболее опасные и тяжело обнаруживаемые. Для повышения уровня кибербезопасности необходимо разработать и внедрить комплексную политику безопасности, которая включает автоматизацию обновлений программного обеспечения, регулярные тесты и аудит систем, обучение сотрудников, создание планов реагирования на инциденты и постоянный мониторинг инфраструктуры. Внедрение многоуровневых систем защиты поможет снизить риски и обеспечить надежную работу информационной системы, защиту данных и соблюдение требований безопасности.

Рекомендации предназначены для планирования мероприятий, направленных на повышение уровня информационной безопасности организации, где приведены ключевые рекомендации для обеспечения четкого распределения ответственности, контроля сроков и реализации данных мер.

Таким образом, создание и регулярное обновление плана мер по информационной безопасности является ключевым аспектом для комплексной защиты информации организации. Он помогает обеспечить решительный подход к минимизации рисков и повысить уровень защиты данных для обеспечения безопасной работы информационных систем.

Заключение

В результате проведенного исследования были рассмотрены методы и средства мониторинга обнаружения и противодействия атак:

1. Атаки DNS spoofing.

2. Уязвимости нулевого дня.

3. Применение IoT-устройств злоумышленниками.

В результате исследования, были выполнены следующие задачи:

1) разработан комплексный подход к повышению уровня защиты, включающий внедрение многоуровневых систем безопасности;

2) Рассмотрены методы использования криптографических технологий для организации регулярных тестов и аудитов;

3) создан безопасный план реагирования на инциденты.

Таким образом, данный комплексный подход к обеспечению информационной безопасности и предложенные практические рекомендации по созданию надежных систем защиты, что является актуальным и необходимым для корпоративных организаций в настоящее время.

Литература

1. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие: в 3-х ч. / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. – Тамбов: Издательский центр ФГБОУ ВО «ТГТУ» 2023.

2. Информационная безопасность: учеб. пособие / авт.-сост. И74 И. Б. Тесленко [и др.] / под общ. ред. проф. И. Б. Тесленко; Владим. гос. ун-т им. А. Г и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2023 – 212 с. – ISBN 978-5-9984-1783-2.

3. ГОСТ Р 50922-96. Защита информации. Основные требования и определения.

4. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

5. ГОСТ Р 51275-99. Объекты информатизации. Факторы, воздействующие на информацию.

6. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем базовая эталонная модель. Часть 2. Архитектура защиты информации.

7. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения.

8. ГОСТ Р ИСО/МЭК 15408-2002. Информационные технологии. Методы и средства обеспечения безопасности. Критерии безопасности информационных технологий.

9. Келдыш, Наталья Всеволодовна К 34 Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022 – Сетевое издание. Режим доступа: https://izd-mn.com/PDF/43MNNPU22.pdf – Загл. с экрана.

10. Закон РФ «Об информации, информатизации и защите информации».

11. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф.Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2022 – 592 с.

12. Международный стандарт ITU-T Rec. X.816 – «Модель оценки уровня безопасности».

13. Международный стандарт ITU-T Rec. X.813 – «Модель управления безопасностью».

14. Международный стандарт ITU-T Rec. X.800 «Рекомендуемые практики по обеспечению безопасности сетей».

15. Международный стандарт ITU-T Rec. X.814 – «Модель защиты сети».

16. Актуальные вопросы выявления сетевых атак. Александр Астахов. CISA. Информационный бюллетень Jet Info, № 3 (106) – Москва, 2022.

References

1. Programmno-apparatnyye sredstva zashchity informatsii [Elektronnyy resurs]: uchebnoye posobiye: v 3-kh ch. / V. A. Gridnev, YU. A. Gubskov, A. S. Deryabin, A. V. Yakovlev. – Tambov: Izdatel'skiy tsentr FGBOU VO «TGTU» 2023.

2. Informatsionnaya bezopasnost': ucheb. posobiye / avt-sost. I74 I. B. Teslenko [i dr.] / pod obshch. red. prof. I. B. Teslenko; Vladim. gos. un-t im. A. G i N. G. Stoletovykh. – Vladimir: Izd-vo VlGU, 2023 – 212 s. – ISBN 978-5-9984-1783-2.

3. GOST R 50922-96. Zashchita informatsii. Osnovnyye trebovaniya i opredeleniya. 4. GOST R 51188-98. Zashchita informatsii. Ispytaniya programmnykh sredstv na nalichiye komp'yuternykh virusov. Tipovoye rukovodstvo.

5. GOST R 51275-99. Ob"yekty informatizatsii. Faktory, vozdeystvuyushchiye na informatsiyu.

6. GOST R ISO 7498-2-99. Informatsionnaya tekhnologiya. Vzaimosvyaz' otkrytykh sistem bazovaya etalonnaya model'. Chast' 2. Arkhitektura zashchity informatsii.

7. GOST R 51624-2000. Zashchita informatsii. Avtomatizirovannyye sistemy v zashchishchennom ispolnenii. Obshchiye polozheniya.

8. GOST R ISO/MEK 15408-2002. Informatsionnyye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Kriterii bezopasnosti informatsionnykh tekhnologiy.

9. Keldysh, Natal'ya Vsevolodovna K 34 Sistemnaya zashchita informatsii komp'yuternykh setey. Uchebnoye posobiye – M.: Mir nauki, 2022 – Setevoye izdaniye. Rezhim dostupa: https://izd-mn.com/PDF/43MNNPU22.pdf – Zagl. s ekrana.

10. Zakon RF «Ob informatsii, informatizatsii i zashchite informatsii».

11. Shan'gin V.F. Kompleksnaya zashchita informatsii v korporativnykh sistemakh: ucheb. posobiye / V.F.Shan'gin. – M.: ID «FORUM»: INFRA-M, 2022 – 592 s.

12. Mezhdunarodnyy standart ITU-T Rec. X.816 – "Model' otsenki urovnya bezopasnosti".

13. Mezhdunarodnyy standart ITU-T Rec. X.813 – "Model' upravleniya bezopasnost'yu".

14. Mezhdunarodnyy standart ITU-T Rec. X.800 "Rekomenduyemyye praktiki po obespecheniyu bezopasnosti setey".

15. Mezhdunarodnyy standart ITU-T Rec. X.814 – "Model' zashchity seti".

16. Aktual'nyye voprosy vyyavleniya setevykh atak. Aleksandr Astakhov. CISA. Informatsionnyy byulleten' Jet Info, № 3 (106) – Moskva, 2022.

НИКОНОВ Вячеслав Викторович, кандидат технических наук, доцент кафедры «Интеллектуальные системы информационной безопасности» Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА. 107996, г. Москва, ул. Стромынка, д. 20. E-mail: nikonov_v@mirea.ru