Программа имеет практико-ориентированный язык: рекомендации формируются как конкретные задания (например, добавьте в форму заказа отдельную пометку для согласия на рассылку). В программе заложен механизм проверки выполнения рекомендации.

Апробация разработанного программного обеспечения показывает, что ее использование позволяет:

- сократить время приведения в соответствие требованиям по защите персональных данных с учетом современного законодательства;
- снизить финансовые затраты на защиту персональных данных за счет минимизации расходов на внешних консультантов, применения недорогих средств защиты, достаточных для выполнения требований, предъявляемых к малым предприятиям;
- реализовать проактивную защиту с учётом возможных изменений в деятельности организации.

Использование программы позволяет выявлять и устранять потенциальные проблемы по защите персональных данных, соответственно выполнять профилактику нарушении в этой области защиты информации.

Минакова Наталья Николаевна, д.ф.м.н., профессор, профессор каф. информационной безопасности, minakova@asu.ru

Мансуров Александр Валерьевич, к.ф.м.н., доцент, зав. каф. информационной безопасности, mansurov@mail.asu.ru

Нам Алина Сергеевна, студ. гр. 5.207-3, nam@mail.asu.ru

УДК 004.056

ПРИМЕНЕНИЕ СЕТЕВЫХ ОТПЕЧАТКОВ УСТРОЙСТВ ДЛЯ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ

И.С. Поздняк, Г.Н. Чифранов
ФБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», г. Самара

Ключевые слова: кибербезопасность, сетевые отпечатки, профилирование устройств, сетевые протоколы.

Важнейшим вопросом кибербезопасности в локальных сетях является предотвращение проникновения в периметр сети злоумышленников путем подключения неконтролируемых устройств. Для усиления безопасности и контроля доступа в локальной сети предлагается использовать механизмы сетевых отпечатков устройств. Внедрение технологий профилирования сетевых устройств представляет собой переход к современной архитектуре, основанной на принципах идентификации и доверии (Identity-Centric Security) [1].

Применение сетевых отпечатков позволяет добавить дополнительные факторы в процессы верификации устройств. Для этого анализируются

характеристики используемых протоколов сетевого стека. Непрерывный анализ отпечатков позволяет динамически оценивать уровень риска и регулировать политики доступа в реальном времени. Также появляется возможность применять дифференцированные политики безопасности, для одинаковых устройств, но с разным типом ПО (например, устаревшим).

Реализация систем для анализа отпечатков позволит решить многие проблемы безопасности локальных сетей. Корреляция MAC-адреса устройства с неизменяемыми характеристиками стека протоколов (DHCP, JA3 хеш и т.д.) обеспечивает целостность процесса идентификации, инициируя блокировку доступа при несовпадении значений с профилем устройства, позволяя предотвратить спуфинг параметров легитимного устройства.

Проблема контроля нелегитимных устройств решается автоматической классификацией на основе пассивного анализа трафика и помещения таких устройств в карантинную подсеть, что предотвращает компрометацию периметра через физические порты доступа. Применение отпечатков JA3 обеспечивает видимость зашифрованного трафика, используя метаданные рукопожатий для определения применяемого ПО, что позволяет детектировать вредоносное ПО и нелегитимные устройства в зашифрованных каналах связи.

Необходимо учитывать тот факт, что при использовании сетевых отпечатков требуются механизмы динамического обновления баз профилей устройств для предотвращения ложных блокировок. Например, обновление ПО и используемого стека протоколов может повлиять на отпечаток устройства.

Применение сетевых отпечатков устройств в системах безопасности локальной сети позволяет организовать динамическое управление доступом, обеспечивает видимость применяемого ПО в зашифрованном трафике и реализует принципы сегментации. Однако эффективность данного подхода зависит от качества корреляции данных, ее актуальности и интеграции с системами автоматизированного реагирования.

В дальнейшем планируется разработка доказательства концепции на базе open-source инструментов, таких как Zeek или Suricata. А также создание дашборда на базе ELK Stack (Elasticsearch + Kibana) для визуализации отпечатков и рисков. Кроме того, допустима реализация автоматизации и ML-улучшений в части внедрения ML-модели для динамического обновления профилей устройств: кластеризация трафика (возможность автоматизированно поддерживать и уточнять профили устройств и выявлять отклонения без ручной обработки нормального и аномального трафика), предикция изменений от обновлений ПО (использование моделей машинного обучения для прогнозирования того, как обновление программного обеспечения (ОС, браузер, драйверы) повлияет на сетевой отпечаток устройства, чтобы избежать ложных блокировок).

Список использованных источников
1. Identity-Centric Cybersecurity Model. URL: https://identitymanagementinstitute.org/identity-centric-cybersecurity-model/ (дата обращения: 11.03.2026).

Поздняк Ирина Сергеевна, к.т.н., доцент, декан фак. кибербезопасности и управления, i.pozdnyak@psuti.ru.
Чифранов Георгий Николаевич, стар. препод. каф. информационной безопасности, chifranov.e@ya.ru.

УДК 004.056; 004.8

МНОГОФАКТОРНЫЙ НЕЙРОСЕТЕВОЙ АНАЛИЗ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ

Е.А. Марченко, С.В. Жуков, В.А. Федосеев
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: DLP‑системы, обнаружение утечки данных, гибридные модели глубокого обучения, поведенческая аналитика.

Современные корпоративные информационные системы генерируют значительные объёмы разнородных данных о действиях пользователей, что усложняет своевременное выявление инсайдерских угроз и подготовительных сценариев утечки конфиденциальной информации. Традиционные подходы, основанные на правилах, и простые статистические методы не позволяют в полной мере учитывать разнообразие поведения конкретного пользователя, динамику его активности и контекст выполняемых операций. В результате возрастает потребность в интеллектуальных UEBA‑решениях, способных проводить именно персонализированный поведенческий анализ и оценивать риск не только на уровне событий, но и на уровне индивидуального профиля пользователя [1, 2].

Целью работы является разработка и экспериментальное обоснование многофакторного персонализированного подхода к поведенческому анализу пользователей на основе комбинации нейросетевых моделей в контексте DLP‑систем.

Для достижения цели предлагается двухуровневый подход, решающий две ключевые задачи:

1. Объективная оценка уровня риска поведения сотрудника.
2. Выявление степени отклонения поведения от индивидуального профиля сотрудника.

Для решения этих задач были сформированы наборы данных, состоящие из 47 признаков, агрегированных на уровне сессии