УДК 004

Фатеев Р.Р., Шигапов А.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНЫХ УГРОЗ СО СТОРОНЫ ВНУТРЕННИХ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ИХ ДЕЙСТВИЙ И ИСТОРИИ РАБОТЫ

Аннотация. В статье рассматривается методика выявления потенциальных угроз информационной безопасности, исходящих от внутренних пользователей организации. Основное внимание уделяется анализу их поведенческой активности, мониторингу действий и истории работы в корпоративной системе. Применение поведенческих моделей и систем выявления аномалий позволяет своевременно обнаруживать подозрительную активность, предотвращая утечки данных и внутренние атаки. Также обсуждаются современные программные решения, направленные на усиление защиты от инсайдерских угроз и формирование профилей пользователей на основе их цифрового поведения.

Ключевые слова: инсайдерские угрозы, информационная безопасность, поведенческий анализ, мониторинг активности, выявление аномалий.

Выявление потенциальных угроз со стороны внутренних пользователей требует систематического мониторинга их действий в информационных системах с использованием специализированных инструментов. Например, системы SIEM (Security Information and Event Management) собирают и анализируют логи активности, такие как попытки входа в систему, запросы к базам данных, копирование файлов на внешние носители или отправка данных через корпоративную почту [1]. Аномалии выявляются через сравнение текущей активности с историческими данными: если сотрудник из отдела маркетинга, обычно работающий с клиентскими презентациями, начинает обращаться к финансовым базам данных, это фиксируется как подозрительное поведение. Дополнительно используются метрики, такие как объем скачиваемых данных (например, более 1 ГБ за сессию) или частота доступа к критическим системам вне рабочего времени. Ключевым инструментом является анализ поведения на основе систем UEBA (User andEntityBehavior Analytics) [2].

Для повышения точности детекции угроз интеграция с системами DLP (Data LossPrevention) позволяет отслеживать действия, непосредственно связанные с утечкой данных. Например, DLP-правила могут автоматически фиксировать инциденты по шаблонам: «копирование более 10 файлов, помеченных как конфиденциальные, за 24 часа» или «пересылка документов с ключевыми словами «коммерческая тайна» через личную почту». Дополнительный уровень контроля обеспечивают системы PAM (Privileged Access Management), которые мониторят действия администраторов, имеющих доступ к критическим ресурсам, и блокируют несанкционированные изменения настроек, такие как модификация прав доступа [3].

На этом этапе устанавливаются критерии для оценки и классификации переменных, необходимых для анализа риска, а также критерии самой оценки рисков. Методы, используемые для этого, уже на стадии определения контекста задаются в общих чертах. Согласно действующим стандартам ISO, термин «оценка риска» включает три подпроцесса: идентификацию риска, анализ риска и оценку риска. Процесс оценки рисков повторяется и улучшается по мере поступления новой информации. Это может привести к расширению области применения или изменению контекста, если будут выявлены новые типы рисков [4].

Рассмотрим работу нейронной сети для решения задачи выявления потенциальных угроз на примере датасета, содержащего информацию о сотрудниках, их действиях и психометрических характеристиках.

Датасет содержит информацию:

- о сотрудниках (уникальный идентификатор пользователя, роль в организации (например, ITAdmin, Engineer), отдел (например, Finance, R&D), проекты, в которых участвует пользователь);
- о событиях входа и выхода пользователей из системы (идентификатор пользователя, дата и время события, тип активности, идентификатор компьютера);

- о веб-активностях сотрудников (идентификатор пользователя, дата и время запроса, посещенный URL, тип активности, содержимое запроса);
- об операциях с файлами (идентификатор пользователя, дата и время операции, имя файла, тип действия, флаг записи на съемный носитель);
- о подключении внешних устройств (идентификатор пользователя, дата подключения, путь к данным на устройстве, тип действия);
- о личностных характеристиках пользователей (Открытость, Добросовестность, Экстраверсия, Доброжелательность, Невротизм);
- о доступе к файлам-ловушкам (идентификатор пользователя, имя файла-приманки).

Для обнаружения аномалий использовалсяавтоэнкодер - нейронная сеть, которая обучается воссоздавать нормальное поведение пользователей. После обучения вычисляется среднеквадратичная ошибка восстановления (MSE) для каждого пользователя, классифицируя тех, чья ошибка превышает 97-й перцентиль, как потенциальные угрозы. ИИ также генерирует визуализации: график потерь обучения и диаграмму рассеяния, где аномалии выделены красным, что помогает аналитикам быстро идентифицировать подозрительных пользователей.

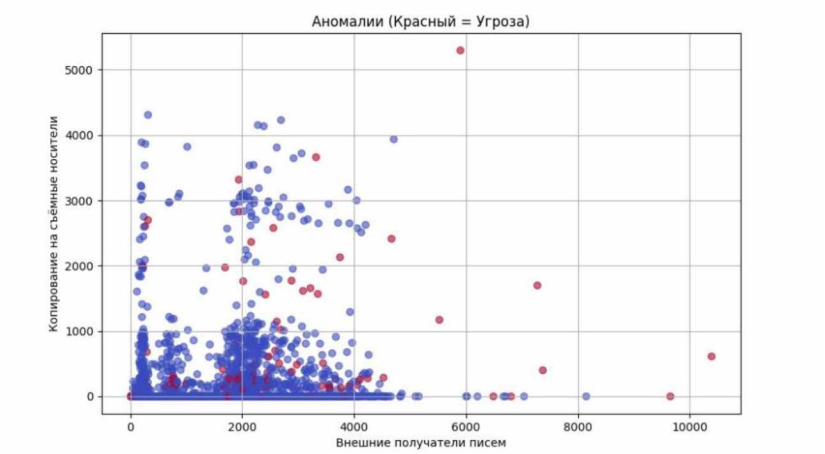

Рис. 1. Тепловая карта собранная по сделанной базе

Нейронная сеть показывает высокую эффективность в нахождении угроз (F1- мера примерно 0,85 на тестовых данных). Внедрение изменений политики безопасности на основе полученных рекомендаций позволяет существенно снизить риски и улучшить защиту данных.

Выявление потенциальных угроз со стороны внутренних пользователей является критически важной задачей в системе обеспечения информационной безопасности любой организации. Применение поведенческого анализа, мониторинга активности и систем обнаружения аномалий позволяет не только своевременно выявлять инсайдерские угрозы, но и снижать риски утечки конфиденциальной информации. Комплексный подход, включающий технологии машинного обучения, постоянную оценку цифровых профилей пользователей и интеграцию средств информационной аналитики, обеспечивает высокий уровень защиты и устойчивость корпоративной среды к внутренним атакам.

Список использованных источников:

1. Исхаков А.Ю., Гайдук К. К вопросу о реализации алгоритмов выявления внутренних угроз с применением машинного обучения // Вестник СибГУТИ. 2022. № 4 (60). URL: https://cyberleninka.ru/article/n/k-voprosu-o-realizatsii-algoritmov-vyyavleniya-vnutrennih-ugroz-s-primeneniem-mashinnogo-obucheniya (дата обращения: 20.04.2025).
2. Корниенко С.В., Пантюхина А.В. Методика выявления потенциальных внутренних нарушителей информационной безопасности // Интеллектуальные технологии на транспорте. 2023. № 2 (34). URL: https://cyberleninka.ru/article/n/metodika-vyyavleniya-potentsialnyh-vnutrennih-narushiteley-informatsionnoy-bezopasnosti (дата обращения: 20.04.2025).
3. Морданов М.А. Система контроллинга как основа эффективного управления рисками деятельности отечественных авиакомпаний // Этап. 2020. № 6. URL: https://cyberleninka.ru/article/n/sistema-kontrollinga-kak-osnova-effektivnogo-upravleniya-riskami-deyatelnosti-otechestvennyh-aviakompaniy (дата обращения: 20.04.2025).
4. Черных Л.В., Горбунова В.Б. Актуальные угрозы обеспечения экономической безопасности в киберпространстве // Вестник молодежной науки. 2022. № 3 (35). URL: https://cyberleninka.ru/article/n/aktualnye-ugrozy-obespecheniya-ekonomicheskoy-bezopasnosti-v-kiberprostranstve(дата обращения: 20.04.2025).

Fateev R.R., Shigapov A.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

DETECTION OF POTENTIAL THREATS FROM INTERNAL USERS BASED ON THEIR ACTIONS AND WORK HISTORY

Abstract. This article presents a methodology for detecting potential information security threats originating from internal users of an organization. The focus is on analyzing behavioral activity, monitoring actions, and evaluating user work history within corporate systems. The use of behavioral models and anomaly detection systems allows for timely identification of suspicious activity, thereby preventing data leaks and internal attacks. The paper also discusses modern software solutions aimed at enhancing protection against insider threats and building user profiles based on their digital behavior.

Keywords: insider threats, information security, behavioral analysis, activity monitoring, anomaly detection.