УДК 004.056.53

Бянкина Е.Е.
студент
ФГБОУ ВО «Тихоокеанский государственный университет»
г. Хабаровск, Россия
Матафонова А.Н.
ст. преподаватель
ФГБОУ ВО «Тихоокеанский государственный университет»
г. Хабаровск, Россия

Применение методов машинного обучения для обеспечения безопасности интеллектуальной собственности и прогнозирования ее утечек

Аннотация. В статье рассматриваются возможности применения методов машинного обучения для обеспечения безопасности интеллектуальной собственности и прогнозирования ее утечек в корпоративных информационных системах. Анализируются основные причины возникновения внутренних угроз, особенности поведения инсайдеров и современные подходы к выявлению аномальной активности пользователей. Рассматриваются алгоритмы классификации и обнаружения аномалий, используемые для анализа действий сотрудников и оценки вероятности инцидентов информационной безопасности. Особое внимание уделяется интеграции технологий машинного обучения с системами DLP и UEBA. Показаны преимущества интеллектуального анализа данных для повышения уровня защиты конфиденциальной информации, а также существующие ограничения, связанные с качеством данных, ложными срабатываниями и необходимостью постоянного обновления моделей.

Ключевые слова: машинное обучение, интеллектуальная собственность, утечка данных, инсайдерская угроза, информационная безопасность, анализ поведения пользователей, обнаружение аномалий, прогнозирование, DLP, UEBA.

Byankina E.E.
Student
Pacific State University
Khabarovsk, Russia
Matafonova A.N.
Senior Lecturer
Pacific State University
Khabarovsk, Russia

Applying machine learning methods to predict intellectual property leaks

Annotation. The article explores the potential applications of machine learning techniques to safeguard intellectual property and anticipate its unauthorized disclosure within corporate information systems. It delves into the primary sources of internal threats, the behavioral characteristics of insiders, and contemporary methods for identifying unusual user behavior. The paper reviews classification and anomaly detection algorithms employed to scrutinize employee activities and gauge the probability of information security incidents. Particular emphasis is placed on integrating machine learning technologies with DLP and UEBA systems. The benefits of intelligent data analysis for enhancing the protection of sensitive information are outlined, along with existing constraints related to data quality, false alarms, and the necessity for ongoing model refinements.

Keywords: machine learning, intellectual property, data leakage, insider threat, information security, user behavior analysis, anomaly detection, forecasting, DLP, UEBA.

В современных условиях цифровизации интеллектуальная собственность становится одним из наиболее ценных ресурсов организации. К интеллектуальной собственности относятся программные продукты, техническая документация, результаты научных исследований, коммерческие разработки и иные сведения, представляющие стратегическую ценность для компании. Потеря такой информации способна привести не только к финансовым убыткам, но и к утрате конкурентных преимуществ.

Одной из наиболее серьезных проблем информационной безопасности являются внутренние утечки данных, связанные с действиями сотрудников организации. В отличие от внешних атак, инсайдерские угрозы сложнее выявлять, поскольку пользователь обладает легальным доступом к информации и использует корпоративные ресурсы в рамках своих полномочий. Традиционные методы защиты информации, основанные на фиксированных правилах и сигнатурном анализе, не всегда позволяют своевременно обнаруживать подозрительную активность. В связи с этим возрастает интерес к использованию методов машинного обучения, способных анализировать большие объемы данных и выявлять скрытые закономерности поведения пользователей [1].

Большинство современных систем информационной безопасности фиксируют огромное количество событий: входы пользователей в систему, операции с файлами, передачу данных по сети, использование внешних устройств и обращение к корпоративным сервисам. Анализ подобной информации вручную становится практически невозможным, особенно в крупных организациях. Именно поэтому методы машинного обучения рассматриваются как перспективный инструмент автоматизации процессов выявления угроз [2].

Одним из наиболее распространенных подходов является анализ поведения пользователей. Система формирует модель нормальной активности сотрудника, учитывая время работы, частоту обращения к определенным файлам, объем передаваемых данных и используемые приложения. Если действия пользователя начинают существенно отличаться от привычного поведения, система определяет это как потенциальную угрозу [3].

Например, сотрудник может внезапно начать копирование большого количества технической документации на внешний носитель либо отправлять корпоративные файлы через сторонние облачные сервисы. Подобные действия сами по себе не всегда являются прямым доказательством утечки информации, однако машинное обучение позволяет оценить совокупность признаков и определить вероятность возникновения инцидента.

Для решения подобных задач применяются различные алгоритмы машинного обучения. В исследованиях российских авторов часто рассматриваются методы классификации, включая Random Forest, Support Vector Machine и XGBoost. Такие алгоритмы позволяют разделять действия пользователей на безопасные и потенциально опасные на основе заранее подготовленных обучающих выборок. При этом качество работы модели напрямую зависит от полноты и достоверности данных, используемых в процессе обучения [2].

Отдельное внимание уделяется методам обнаружения аномалий. Их преимущество заключается в способности выявлять неизвестные ранее сценарии утечек информации. В отличие от классических сигнатурных систем, ориентированных на заранее известные шаблоны угроз, модели обнаружения аномалий способны реагировать на нетипичное поведение даже в тех случаях, когда конкретный способ утечки ранее не встречался [4].

В последние годы активно развиваются технологии «User and Entity Behavior Analytics» (UEBA), основанные на комплексном анализе действий пользователей и объектов информационной системы. Подобные решения используются совместно с DLP-системами и позволяют значительно повысить эффективность обнаружения внутренних угроз. Машинное обучение помогает снизить нагрузку на специалистов по информационной безопасности, автоматически выделяя наиболее подозрительные события среди большого количества ежедневных операций [1].

Несмотря на очевидные преимущества, использование машинного обучения в задачах информационной безопасности связано с рядом проблем. Одной из них является высокая вероятность ложных срабатываний. Иногда система может классифицировать обычные действия сотрудника как подозрительные, что приводит к дополнительной нагрузке на отдел безопасности. Кроме того, злоумышленники могут пытаться адаптировать свое поведение таким образом, чтобы обходить интеллектуальные системы обнаружения [5].

Еще одной важной проблемой является необходимость постоянного обновления моделей. Поведение пользователей и способы взаимодействия с информационными системами постепенно меняются, поэтому алгоритмы требуют регулярного переобучения. В противном случае точность прогнозирования угроз может снижаться.

Тем не менее развитие технологий искусственного интеллекта делает применение машинного обучения все более эффективным. Современные исследования показывают, что сочетание анализов поведения, методов обнаружения аномалий и интеллектуальной обработки данных позволяет существенно повысить уровень защиты интеллектуальной собственности в корпоративных системах [2].

Таким образом, методы машинного обучения являются перспективным направлением развития систем информационной безопасности, предназначенных для прогнозирования утечек интеллектуальной собственности. Использование интеллектуального анализа поведения пользователей позволяет своевременно выявлять потенциальные угрозы и снижать риск потери конфиденциальной информации.

Несмотря на существующие ограничения, связанные с качеством данных, ложными срабатываниями и необходимостью постоянного обучения моделей, применение машинного обучения уже сегодня демонстрирует высокую эффективность в задачах обнаружения инсайдерских угроз. В дальнейшем развитие искусственного интеллекта и технологий анализа данных будет способствовать созданию более точных и адаптивных систем защиты информации.

Список источников

1. Гайдук, К. А. К вопросу о реализации алгоритмов выявления внутренних угроз с применением машинного обучения / К. А. Гайдук, А. Ю. Исхаков // Вестник Сибирского государственного университета телекоммуникаций и информатики. – 2022. – № 3. – С. 45–52.

2. Стрижков, В. А. Application of machine learning methods to counter insider threat to information security / В. А. Стрижков // Информационные технологии и телекоммуникации. – 2023. – Т. 11, № 2. – С. 34–41.

3. Золотухина, М. А. Определение параметров скрытых угроз раннего обнаружения в информационных системах для задач машинного обучения / М. А. Золотухина, С. В. Зыков // Научно-технический вестник информационных технологий, механики и оптики. – 2023. – Т. 23, № 4. – С. 712–719.

4. Баранов, А. В. Методы анализа поведения пользователей в системах информационной безопасности / А. В. Баранов, И. С. Кудинов // Информационная безопасность регионов. – 2021. – № 2. – С. 58–64.

5. Исследование состязательных атак на классические модели машинного обучения в контексте обнаружения сетевых угроз // Научно-технические ведомости Санкт-Петербургского политехнического университета. Информатика. Телекоммуникации. Управление. – 2025. – Т. 18, № 1. – С. 96–105.

6. Адаменко П. А., Цибульникова В. Ю., Нужина И. П. Применение машинного обучения и искусственного интеллекта при управлении предпринимательскими рисками в малом бизнесе// Журнал прикладных исследований.-2023.-№10-С.66-72.

7. Рашникова Ю. Е. Искусственный интеллект в инновационных разработках// Актуальные вопросы современной экономики, 2024. №8. URL: http://www.авсэ.рф. С. 349-356