УДК 004.056

Разработка метода контроля целостности данных системы видеонаблюдения во внутреннем сегменте сети

Шедогубов Н.И. (ИТМО)

Научный руководитель – кандидат технических наук, доцент Коржук В.М. (ИТМО)

Введение. Развитие информационных технологий сфере безопасности данных, включая информацию с систем видеонаблюдения, приводит к увеличению их объема и важности защиты этих данных от киберугроз. Проблема целостности данных в системе видеонаблюдения возникает из-за возможных нарушений или изменений, которые могут оказаться критическими для безопасности банка и его клиентов. На данный момент одними из используемых средств являются хост системы обнаружения вторжений, такой как менеджер событий и система обнаружения вторжений в сеть от SolarWinds Security для монитора сервера и отслеживания сетевого трафика. Однако, основные из недостатков этих систем включают ограниченные возможности обнаружения новых и неизвестных угроз, возможность компрометации в результате атак, а также на сегодня и вовсе приостановлены поставки лицензий и обновлений в Российскую Федерацию. Что подчеркивает важность поиска более надежных, эффективных и рабочих импортозамещающих на территории России методов контроля целостности данных. В исследованиях [1] и [2] осуществлен полный обзор методов анализа журналов событий. [1] подчеркивает широкое использование статистических методов, в то время как [2] выявляет превосходство ансамблевых методов машинного обучения, таких как случайные леса и градиентное усиление, в задачах классификации и обнаружения аномалий.

Основная часть. Для разработки предлагается использовать методы машинного обучения для автоматического контроля журналов целостности в системе видеонаблюдения банка. Этот подход позволит выявлять аномалии и потенциальные нарушения без необходимости ручной проверки. При обнаружении аномалий система автоматически отправляет уведомление администратору, обеспечивая оперативную реакцию на потенциальные угрозы безопасности. Такой подход снижает риски и повышает эффективность контроля за целостностью данных в системе видеонаблюдения банка.

Для проверки эффективности разработанного метода планируется провести эксперименты на данных из реальной системы видеонаблюдения банка. Журналы целостности будут анализироваться как с помощью открытого ПО, так и с применением разработанного метода на основе машинного обучения. Полученные данные позволят сравнить результаты и оценить точность и надежность нового подхода к контролю целостности данных в системе видеонаблюдения.

Выводы. Предполагается, что разработанный метод продемонстрирует высокую точность контроля целостности данных, не ниже инструмента с открытым кодом. Кроме того, ожидается, что он будет оперативнее существующих методов анализа, что ускорит процесс обнаружения аномалий в журналах целостности системы видеонаблюдения банка.

Список использованных источников:

1. Yen S., Moh M. Intelligent log analysis using machine and deep learning//Research Anthology on Artificial Intelligence Applications in Security. – IGI Global, 2021. – С. 1154-1182.
2. Landauer M. et al. Deep learning for anomaly detection in log data: A survey//Machine Learning with Applications. – 2023. – Т. 12. – С. 100470.