УДК 004.8

Полышева А.К.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шафиков М.Р.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В рамках данного исследования, акцент сделан на применении технологий искусственного интеллекта для оптимизации задач управления информационной безопасностью. Рассматриваются средства защиты информации отечественного рынка, которые используют в своей работе алгоритмы машинного обучения и искусственного интеллекта. Описываются встроенные модули систем.

Ключевые слова: искусственный интеллект, угроза, безопасность, система защиты информации, машинное обучение.

Реализация эффективной защиты информации сталкивается с серьезными трудностями, поскольку современные кибернетические угрозы характеризуются высоким уровнем сложности, а спектр используемых технологий – большим разнообразием [3]. Все более проблематичным становится выполнение таких важных задач, как постоянный контроль, аналитическая обработка данных и оперативное реагирование на инциденты.

Существуют разнообразные подходы к обнаружению киберугроз, в том числе сигнатурный анализ, а также методы, которые основаны на нейросетях и алгоритмах машинного обучения. Хотя сигнатурный анализ, базирующийся на сравнении с известными образцами, позволяет быстро находить определенные типы атак, он не эффективен против новых угроз [3].

Если сигнатурный анализ основывается на известных признаках угроз, то машинное обучение использует анализ больших данных для обнаружения аномального поведения, которое может свидетельствовать о готовящейся атаке. Нейросети повышают эффективность этого анализа, позволяя распознавать более сложные и адаптивные угрозы.

Тем не менее окончательная оценка ситуации и принятие мер остаются в компетенции человека.

Отечественный сектор IT и информационной безопасности активно внедряет инструменты на основе машинного обучения и искусственного интеллекта.

Для обнаружения и предотвращения кибератак все чаще применяют искусственный интеллект в качестве прогностического инструмента. ИИ используется в антивирусном ПО для автоматизации реагирования на атаки, а также для анализа обширных массивов данных с целью выявления скрытых угроз и реализации множества других функций.

Использует искусственный интеллект и DLP-система «СёрчИнформ КИБ». Система включает программные модули. Можно выделить те, которые отвечают за распознавание лиц и личных устройств. Искусственный интеллект, в частности, для мониторинга активности персонала в сети Интернет и отображаемой на мониторах информации. В общей сложности «СёрчИнформ КИБ» насчитывает одиннадцать модулей [2].

Одним из преимуществ DLP-системы является модуль MonitorController, который позволяет собирать информацию о работающих процессах и посещаемых сайтах в момент создания снимка экрана. Это дает возможность получить полное представление о действиях пользователя за время сбора данных.

Еще одним важным дополнением является функция распознавания лиц, которая позволяет определить, кто именно находился за компьютером в момент потенциального нарушения. Функциональность данной программы позволяет выявлять случаи несанкционированного использования чужих ПК сотрудниками [2]. Программа позволяет установить личность пользователя, осуществившего вход в систему с использованием чужого компьютера, зафиксировать точную дату и время инцидента.

Подход, используемый для анализа данных в «СёрчИнформ КИБ», отличается от подхода InfoWatch. DLP-система InfoWatch для прогнозного анализа собираемых данных использует искусственный интеллект.

Предиктивная аналитика данных, собираемых системой Traffic Monitor, осуществляется с помощью инструмента InfoWatch Prediction. Этот инструмент использует технологии машинного обучения для выявления рискованных паттернов поведения сотрудников, что способствует повышению эффективности управления группами риска. При построении паттерна поведения сотрудника для анализа инструмент использует более 54 параметров и типов событий.

Основной задачей предиктивной аналитики является автоматический анализ данных с целью выявления рискованных паттернов (цепочек событий) и своевременное оповещение о любых отклонениях от нормы. Такой подход позволяет службе безопасности работать на упреждение, прогнозируя риски, а не реагируя на уже произошедшие инциденты.

Согласно статистике, в двух случаях из трех сотрудники, покидающие компанию, копируют данные для последующего использования в новой организации. InfoWatch Prediction автоматически выявляет подобную активность, сопоставляет ее с другими признаками и выдает предупреждение об аномальном поведении.

Алгоритмы машинного обучения анализируют различные параметры, включая активность в рабочей переписке, посещение ресурсов по трудоустройству, время начала и окончания рабочего дня, и информируют о любых отклонениях от стандартного паттерна поведения конкретного работника.

В табл. 1 приведены ключевые характеристики двух решений для проведения сравнительного анализа.

Таблица 1

Сопоставление решений DLP

Характеристика/Система	«СёрчИнформ КИБ»	InfoWatch Traffic Monitor
Сертификат соответствия ФСТЭК	да	да
Реестр отечественного ПО	включен	включен
Возможность интеграции со СКУД системой	да	нет
Просмотр рабочего стола в режиме реального времени	да	нет

SIEM-система MaxPatrol – еще один пример. С помощью поведенческого анализа, который базируется на машинном обучении, такая система способна распознавать даже ранее неизвестные атаки, а также те, которые подразумевают обход стандартных правил корреляции.[1]

Ниже, на рис. 1, изображен процесс обнаружения угроз в MaxPatrol.

Рис. 1. Обнаружение угроз в SIEM-системе MaxPatrol

Определение границ ответственности интеллектуальных систем является ключевым вопросом при разработке искусственного интеллекта. Искусственный интеллект в России пока не признан субъектом права. Как следствие, в законодательстве отсутствуют нормы, регулирующие ответственность за возможные происшествия с его участием [3]. Процесс внедрения машинного обучения и искусственного интеллекта, хотя и управляется разработчиками, может приводить к результатам, которые трудно предугадать.

Ключевым условием для выявления потенциальных ошибок в функционировании искусственного интеллекта является эффективный контроль. Для этого процесс принятия решений должен быть понятен и прозрачен [3]. Высокое качество работы во многом зависит от анализа метаданных. В связи с этим, ключевым приоритетом при разработке является создание условий для безопасного хранения данных и предотвращения их несанкционированного использования, а также защиты от неправомерного доступа.

Список использованных источников:

1. Зачем SIEM-системе машинное обучение: реальные сценарии использования // ITSec.Ru: [сайт]. URL: https://www.itsec.ru/articles/zachem-siem-sisteme-mashinnoe-obuchenie-realnye-scenarii-ispolzovaniya (дата обращения: 06.03.2025).

2. Обзор DLP-системы «Контур информационной безопасности SearchInform» // Компания «Безопасность бизнеса» – Создание комплексных систем безопасности предприятий и объектов: [сайт]. URL: https://www.bugshunt.ru/info/articles/obzor-dlp-sistemy-kontur-informatsionnoy-bezopasnosti-searchinform-chast-1-osnovnye-funktsii-sistemy/ (дата обращения: 19.03.2025).

3. Повышение уровня безопасности ИТ-систем с помощью технологий ИИ // Secuteck.Ru: [сайт]. URL: https://www.secuteck.ru/articles/povyshenie-urovnya-bezopasnosti-it-sistem-s-pomoshchyu-tekhnologij-ii (дата обращения: 21.03.2025).

Polysheva A.K.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shafikov M.R.
Ufa University of Science and Technology, Ufa

USING MODERN TECHNOLOGIES WITH MACHINE LEARNING ALGORITHMS TO IMPROVE THE EFFECTIVENESS OF THE INFORMATION PROTECTION SYSTEM

Abstract. In the context of this article, the focus is on the application of artificial intelligence technologies to optimize information security management tasks. It considers information security tools of the Russian information security products, which use machine learning and artificial intelligence algorithms in their work. It describes the built-in modules of the systems.

Keywords: artificial intelligence, threat, security, information protection system, machine learning.