Список использованных источников
1. UM1924. User manual. STM32 crypto library. ST, 2015. [Электронный ресурс] – URL: https://www.st.com/resource/en/user_manual/dm00215061-stm32-crypto-library-stmicroelectronics.pdf (дата обращения: 26.10.2022).
2. Мартин Моц. Кибербезопасность на уровне микроконтроллеров. [Электронный ресурс] – URL: https://controleng.ru/wp-content/uploads/8370.pdf pdf (дата обращения: 26.10.2022).

Чарикова Полина Вячеславовна, студент гр. 6271-110401D, charikova99@gmail.com.
Лофицкий Игорь Вадимович, к.т.н., доцент каф. радиотехники, ivl60@mail.ru.

УДК 004.056.52; 004.891.3

## ПОСТРОЕНИЕ DLP-СИСТЕМ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

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

**Ключевые слова:** DLP-системы, системы контроля, нейронные сети, нейросетевые технологии.

Предотвращение потери данных (Data Loss Prevention) - мера безопасности, предназначенная для защиты бизнес-информации и предотвращения потери, кражи и искажения важных или конфиденциальных данных путем предотвращения перемещения ключевой информации конечными пользователями за пределы сети. Технология использует программные или аппаратные инструменты, позволяющие сетевому администратору отслеживать данные, которые используются и передаются конечными пользователями.

DLP-система – программное решение либо набор инструментов, защищающая сетевые информационные структуры организации. Такая система позволяет анализировать данные защищаемого цифрового периметра безопасности на внешних носителях и т.п.

Искусственные нейронные сети (ИНС) обладают способностью к обучению, которое заключается в изменении весов и порогов сети. Самой распространённой из огромного множества различных вариаций ИНС является многослойная нейронная сеть прямого распространения (рисунок 1).

Сеть состоит из нескольких слоев и каждый из них состоит из искусственных нейронов, при этом выходы нейронов предыдущего слоя являются входами для нейронов последующего слоя. Она может моделировать функцию практически любой степени сложности, причем число слоев и число элементов в каждом слое определяют сложность функции.

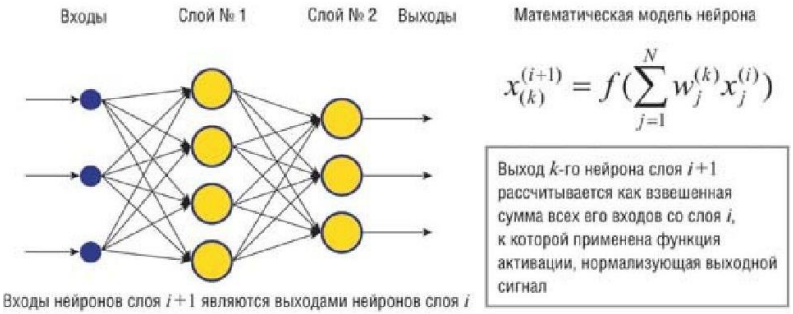


Рисунок 1 – Многослойная нейронная сеть прямого распространения

Цель использования искусственного интеллекта в решении DLP состоит в успешном симбиозе новых технологий с людьми, чтобы активно усиливать соответствующие сильные стороны других. Компании используют навыки экспертов по нейронным сетям и машинному обучению для выбора, создания и применения инновационных методологий и решений, основанных на данных, в сочетании с уже существующими традиционными решениями DLP.

Идентификация поврежденных данных и подозрительной активности стала проще благодаря ИИ, поскольку записи о предыдущих атаках на данные автоматически регистрируются и учитываются при принятии решений в будущем. Решения DLP на основе нейронных сетей могут автоматически блокировать или отключать определенного пользователя с высоким уровнем риска на основе использования или моделей поведения, предотвращая нарушение или утечку данных. Шаблоны данных также можно сканировать по регионам, отделам или процессам в режиме реального времени, что позволяет компаниям выявлять слабые места и сосредоточивать усилия на укреплении безопасности в этих областях.

При работе с большими данными искусственный интеллект может одновременно просеивать и анализировать огромные объемы данных, чтобы обнаруживать события угроз быстрее и точнее, чем любое традиционное решение DLP. На самом деле, чем больше данных доступно, тем больше шаблонов нейронная сеть может обнаружить и изучить, чтобы обнаружить аномальную активность или угрозы в обычном потоке шаблонов. Искусственный интеллект отслеживает действия пользователей, считающиеся нормальными, такие как время входа в систему и местоположение устройства человека, активность этого устройства и многое другое. Любые отклонения от обычной деятельности пользователя, такие как вход в систему из другого места, немедленно помечаются и могут быть заблокированы или приостановлены до тех пор, пока не будет

предоставлена проверка. Затем эта новая информация может быть учтена в будущем поведении пользователя.

Список использованных источников

1. Айдинян А.Р., Цветкова О.Л., Черняков П.В., Сокол Д.С., Методики интеллектуального выбора и оценки DLP-системы для решения проблем информационной безопасности/ Молодой исследователь Дона. Донской государственный технический университет - 2018. - № 1 (10). - С. 1-4.
2. Алексеев И.В., Митрохин М.А., Кольчугина Е.А., Программная реализация модуля DLP-системы для мониторинга и анализа трафика корпоративной сети с использованием машинного обучения/ Безопасность информационных технологий - 2020. – Том № 27 (№ 1). - С. 28-39.
3. Писаренко Игорь, Нейросетевые технологии в безопасности, Информационная безопасность - 2009 - № 4 - С. 34
4. Валерий Естехин**,** ИИ как предсказатель утечек данных**,** Информационная безопасность - 2020. - № 6

Марченко Екатерина Александровна, студент гр. 6203-010302D, katyushenkamarchenko@mail.ru.
Жуков Семен Викторович, ассистент каф. геоинформатики и информационной безопасности, zhukovsv91@inbox.ru.

## ЭКСПЛУАТАЦИЯ РАДИОЭЛЕКТРОННОГО ОБОРУДОВАНИЯ И СРЕДСТВ ДИАГНОСТИКИ АВИАЦИОННОЙ ТЕХНИКИ

УДК 629.7.064.3

# ИСПОЛЬЗОВАНИЕ МОДУЛЬНЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОЦЕНКИ ТЕХНИЧЕСКОГО СОСТОЯНИЯ УЗЛОВ АВИАЦИОННОЙ ТЕХНИКИ

А.Б. Деста
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

**Ключевые слова:** системы встроенного контроля, диагностика, упреждающее техническое обслуживание.

Цель работы – предложить подход к оценке технического состояния узлов авиационной техники, основанный на дедуктивном анализе данных,