СИСТЕМА ЗАЩИТЫ В СИСТЕМЕ ВОЛОКОННОЙ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Анваржон Хабибуллаевич Расулов
Тошкент ахборот технологиялари университети Фарғона филиали
E-mail: anvarx@inbox.ru

Мохинур Хасанова
Тошкент ахборот технологиялари университети Фарғона филиали
E-mail: butterflytatu@gmail.com

АННОТАЦИЯ

Одним из наиболее актуальных и востребованных вопросов сегодня в условиях повсеместной трансформации и цифровизации сфер человеческой деятельности является информационная безопасность и обеспечение целостности данных. Основные исследования и разработки в области информационной безопасности направлены на повышение эффективности и рационализацию. Одним из основных средств передачи данных и эксплуатации информационных комплексов являются волоконно-оптические системы. На сегодняшний день имели место случаи незаконного проникновения и кражи информации, проходящей через данный вид связи. Таким образом, на сегодняшний день существует проблема, связанная с недостаточной защитой информации в волоконно-оптических системах передачи данных. Одним из наиболее эффективных инструментов противодействия актам незаконного вмешательства в системы являются искусственный интеллект и криптографические алгоритмы защиты информации. Именно симбиоз этих двух инструментов позволяет качественно повысить уровень защиты информации в волоконно-оптических системах передачи данных. Таким образом, авторы данной статьи преследуют цель, связанную с описанием инновационной системы защиты информации от нарушений в волоконно-оптических системах передачи данных, основанной на интеграции интеллектуальных криптографических алгоритмов.

Ключевые слова: Волоконно-оптическая связь, криптография, информационная безопасность, искусственный интеллект, информация, система передачи данных.

ВВЕДЕНИЕ

В работе рассматривается основная информация, актуальность и эффективность, связанные с темой исследования. Это исследование выполняет работу посредством применения статистических данных и информации, а также эмпирических и теоретических методов исследования. В данной статье использованы публикации и материалы отечественных и зарубежных источников для более полного раскрытия темы и получения достоверных данных.

В каждой из вышеперечисленных работ авторы проводят исследования, имеющие большое значение в области информационной безопасности на сегодняшний день. Так, например, исследуются вопросы сценариев подключения к оптоволоконным кабелям и защиты от несанкционированного перехвата информации в каналах связи, способы защиты информационного сигнала от несанкционированного доступа, современные угрозы информационной безопасности и многое другое.

Искусственный интеллект (ИИ) и технологии машинного обучения уже широко используются в информационных системах для повышения производительности труда, увеличения продаж и обучения. Их использование в защите от кибератак становится одним из ключевых направлений информационной безопасности.

Суммарные инвестиции в компании, создающие продукты ИБ с использованием технологий ИИ, составляют на конец 2019 года 3749 млн долларов. При этом мировой рынок продуктов ИБ с использованием технологий ИИ к 2025 году достигнет 30 млрд долларов с ежегодным приростом в 23 %.

На данный момент количество атак растет, а ландшафт угроз меняется молниеносно. Например, продукты «Лаборатории Касперского» отражают более 700 млн онлайн-атак в квартал (данные за второй квартал 2019 года) по всему миру, а Cisco утверждает, что блокирует 20 млрд сетевых атак в день (более 7 трлн атак в 2018 году). Очевидно, что при таких объемах вредоносной активности киберпреступники активно используют средства автоматизации кибератак, в том числе используют технологии искусственного интеллекта и машинного обучения для их улучшения и трансформации, а также для обхода известных средств защиты. Например, известный троянец Emotet является эффективным прототипом. Основным каналом его распространения является спам-фишинг, и группа, стоящая за созданием Emotet, может легко использовать ИИ для усиления атаки, встраиваясь в разговоры естественным образом и используя анализ текста на естественном языке.

Еще одна возможная область злонамеренного использования искусственного интеллекта — лучший подбор пароля или обход двухфакторной аутентификации. Два года назад исследователи создали бота, который смог обходить проверки CAPTCHA с эффективностью 90% с помощью технологий искусственного интеллекта. Используя огромное количество различных источников данных в даркнете для формирования базы знаний искусственного интеллекта, злоумышленники могут сделать атаки на людей по-настоящему эффективными.

Чтобы справиться с растущим объемом атак, поставщики систем безопасности также начинают активно внедрять технологии искусственного интеллекта, машинного обучения и глубокого обучения (ML/DL) для обнаружения, прогнозирования и реагирования на киберугрозы в режиме реального времени. В целом, по данным Webroot (https://www-cdn.webroot.com), около 85% специалистов по безопасности считают, что злоумышленники используют технологии ИИ в своих атаках.

АКТУАЛЬНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ

Долгое время считалось, что волоконно-оптические линии связи обладают максимальной защищенностью и скрытностью информации, но современные исследования показали, что существуют способы снятия излучения с оптических волокон, таким образом, передаваемая по ним информация может быть скомпрометирована, удалена или заблокирована. В соответствии с Федеральным законом «О связи» операторы связи обязаны обеспечивать тайну связи и защиту средств и средств связи от несанкционированного доступа к ним. Несанкционированный доступ к средствам связи и передаваемой с их помощью информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность.

Вопреки мнению о том, что в ВОЛС невозможен скрытый вывод информации, способы такого подключения существуют и их внедрение возможно на каждом из предприятий, использующих в передаче данных оптические технологии. Также в этой статье мы рассмотрим методы защиты от этих незаконных подключений. Рассматривая второй тип угроз - перехват речевой информации, можно сделать вывод, что утечка речевой информации может происходить не только в действующих, но и в нерабочих, но проложенных ВОЛС, если злоумышленник искусственно вводит сигнал, который будет модулируется акустическими волнами в кабель [2].

Следует отметить, что используемое злоумышленником оборудование не обязательно должно быть специализированным для несанкционированного сбора данных, это может быть различное общедоступное стандартное оборудование, например, для прокладки линий связи. Основные методы защиты трафика от утечки в ВОЛС можно разделить на три основные группы методов защиты от перехвата такой информации злоумышленником:

1. Физические средства защиты информации;
2. Аппаратные средства защиты информации;
3. Криптографическая защита информации.

Защита информации обеспечивается не воздействием на параметры канала утечки, а вероятностным преобразованием информации перед ее передачей по каналу связи. Невозможность восстановления информации злоумышленником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем обычный канал пользователя. Метод шифрования выбирается таким образом, чтобы количество ошибок, возникающих в канале утечки, сильно увеличивалось, обеспечивая эффект шумовой передачи сигнала, в то время как основной канал обеспечивал надежное соединение. Криптографический метод включает в себя метод, который делает информацию для злоумышленника мало полезной - это является квантовая криптография, которая нашла свое отражение как раз в волоконно-оптической технологии. Квантовая криптография основана на принципе неопределенности Гейзенберга — невозможно измерить один параметр фотона, не исказив другой. Поэтому нарушитель не сможет изменить состояние передаваемых фотонов, так как это может привести к его засветке, по факту дополнительных помех на принимающей стороне.

Анализ интеграции искусственных нейронных сетей для повышения эффективности криптографических алгоритмов защиты информации

Интеллектуальные технологии, в частности искусственные нейронные сети (ИНС), обладающие огромным потенциалом в решении различных сложных вычислительных задач, наиболее активно изучаются и интегрируются в современные системы защиты информации. Колоссальная актуальность интеграции искусственного интеллекта в эти задачи является одной из самых высоких в современном мире в рамках области исследования. Этот фактор связан с тем, что интеллектуальные технологии используются не только для решения задач математического и инженерного характера, но и успешно зарекомендовали себя при решении задач из области информационной безопасности, шифрования, дешифрования и других процессов.

ИНС достаточно прочно входят в жизнь современного человека при решении разного рода задач, а также используются там, где примитивные

алгоритмы являются малоэффективным или вообще невозможным инструментом. В перечень задач, решение которых основано на использовании нейронных сетей, входят: распознавание текста, контекстная реклама на сайтах, фильтрация спама, мониторинг подозрительных транзакций в банковской системе, восстановление изображений и многие другие [3].

Искусственные нейронные сети являются ключевым направлением развития из области искусственного интеллекта для решения задач информационной безопасности. ИНС представляют собой математическую модель, имеющую собственную реализацию на программно-аппаратном уровне. Рис. 1 иллюстрирует схему простой искусственной нейронной сети:

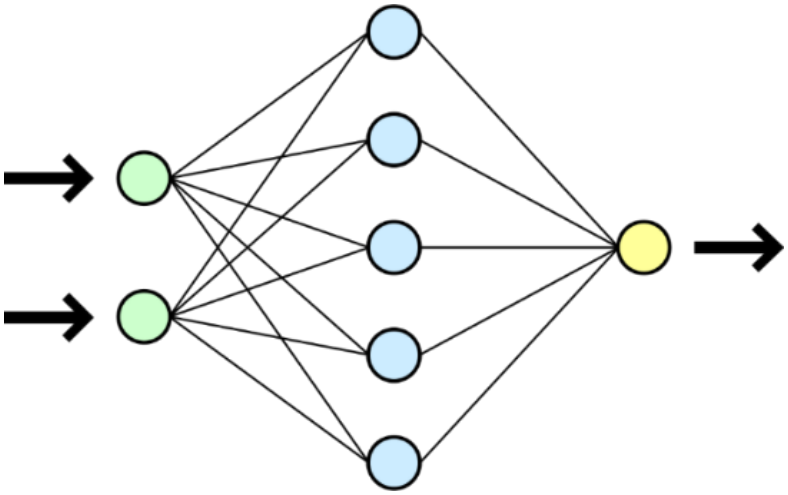

Рис. 1. Принципиальная схема простой нейронной сети. Зеленый - входные нейроны; синий - скрытые нейроны; желтый - выходной нейрон

Рассмотрим математический смысл искусственных нейронных сетей. В математической интерпретации ИНС представляются как нелинейная функция. При w он характеризуется связями, именно через них сигналы одних нейронов поступают на входные сигналы других нейронов. Каждый нейрон искусственной нейронной сети имеет один выход, называемый синапсом. Следует отметить, что каждый выход нейрона связан (или может быть соединен) с неограниченным числом выходов других нейронов (рис. 2). Для понимания представлена следующая математическая модель искусственного нейрона:

$$y = f\left(\sum_{i=1}^{n}(w_i \cdot x_i + b_i)\right), \qquad (1)$$

Где: w_i– представляют веса соответствующих входов;

x_i - представляют собой сигналы на входах нейрона;

b_i - представляет вход и вес нейрона смещения.

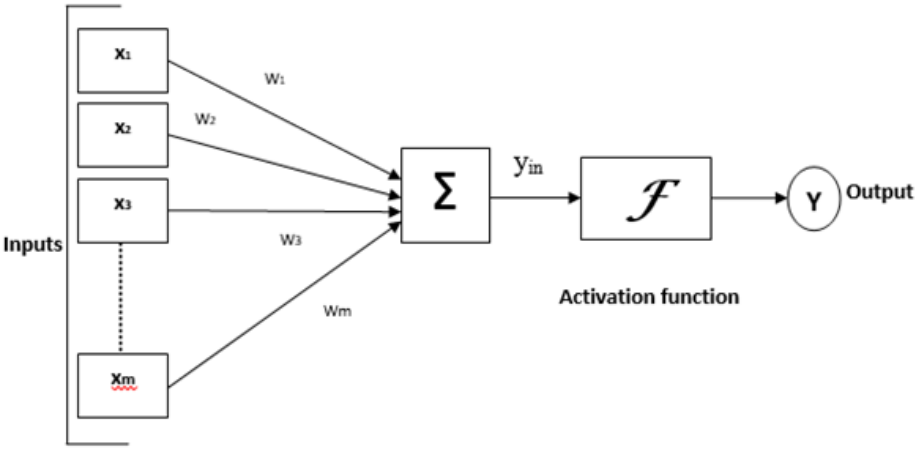

Рис. 2. Схема искусственного нейрона

Отличительной особенностью криптографии по сравнению с другими методами защиты информационных потоков является концентрация алгоритмической работы на физических процессах и методах. Информация и шифры, полученные с помощью физических методов, могут быть переданы и сформированы на основе объектов квантовой механики. Все процессы в целом при этом методе шифрования информации происходят посредством исполнения физических методов. Одним из примеров работы квантово-криптографических алгоритмов является движение некоторого количества электронов в электрическом поле или фотонов в волоконно-оптических линиях связи. Такая схема включает в себя квантовый канал и специальное оборудование, размещенное на обоих концах системы. На рис. 3 схематически изображен принцип работы такой схемы передачи информационных потоков [4].

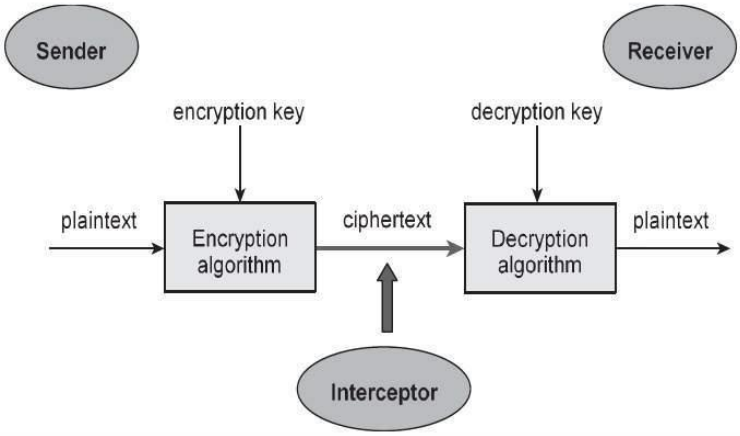

Рис. 3. Криптографический алгоритм защиты информации

Как видно из диаграммы, ключевым принципом работы квантово-криптографических алгоритмов является неопределенность поведения квантовой системы. Основная идея этого принципа заключается в том, что нет

возможности выразить одновременно координату и импульс одной частицы без параллельного искажения другой.

С помощью работы квантовых процессов в настоящее время широко внедряются и разрабатываются различные системы связи и средства передачи информационных потоков, обладающие способностью стопроцентного обнаружения подслушивания и перехвата информации. Эта способность достигается за счет следующего фактора: любая попытка измерения взаимосвязанных параметров квантовой системы вносит в нее возмущения, параллельно уничтожая исходные данные.

В последние годы активно ведутся исследования в области построения методов защиты информации с использованием теории криптографии и помехоустойчивого кодирования и именно эти системы наиболее активно подвергаются компьютерным атакам. Традиционно существующие системы защиты информации не имеют возможности самообучения и используют лишь определенные правила, заложенные в их программном или аппаратном обеспечении. Создание перспективных систем защиты информации в последнее время определяется с использованием интеллектуальных инструментов, таких как: экспертные системы, системы нечеткой логики, нейронные сети, генетические алгоритмы. Эти подходы реализуют эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта специалистов по информационной безопасности в виде системы нечетких правил, доступных для анализа [5].

Возрастающее появление нежелательного (вредоносного) программного обеспечения, использующего новые уязвимости, повысило требования к современным системам защиты информации и привело к использованию систем искусственного интеллекта. Интеллектуальные средства активно используются для решения задач информационной безопасности. Классификация и кластеризация являются основными задачами, решаемыми интеллектуальными средствами защиты информации (ИБ) каналов телекоммуникаций в космической связи, поскольку требуется постоянный мониторинг системных уязвимостей и полей угроз каналов [6].

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПРИНЦИПА ИНТЕЛЛЕКТУАЛЬНОЙ КРИПТОГРАФИИ

ИИ оказывает значительное влияние на многие сферы нашего общества и экономики (например, прогнозирование полиции, правосудия, точной

медицины, маркетинга, политической пропаганды). Отраслевые приложения ИИ характеризуются различными проблемами и не могут быть должным образом рассмотрены в этом отчете, в котором представлен общий обзор основных вопросов, связанных с взаимодействием между защитой данных и ИИ. Таким образом, этот последний раздел кратко затрагивает только две основные области: государственный сектор и рабочее место. В частности, в большинстве случаев внедрение технологий ИИ в систему информационной безопасности организации сокращает время на выявление проблем и реагирование на инциденты, а также затраты на управление персоналом. Операторы отмечают повышение эффективности обнаружения неизвестных угроз, а также скорости анализа и обнаружения вредоносной активности на конечных точках и в приложениях [8].

Применение ИИ увеличивает количество специфических вопросов при использовании в государственном секторе, во многом из-за дисбаланса власти между гражданами и администрацией и предоставляемых необходимых услуг. Более того, принятие всеобъемлющих и нечетких решений ИИ со стороны правительств и их агентств свидетельствует о том, что им сложнее выполнять свои обязательства по подотчетности, причем не только в отношении данных, находящихся в обработке [9].

Такое положение дел, по-видимому, оправдывает принятие более жестких гарантий, кроме передачи специальных комиссий или ревизии. Защита также должна включать процесс оценки, который критически оценивает потребность в предлагаемых решениях ИИ и их пригодность для предоставления услуг государственными учреждениями или частными компаниями, действующими от их имени. Этот процесс требует, чтобы «по крайней мере они [приложения ИИ] были доступны для публичного аудита, тестирования и рассмотрения, а также в соответствии со стандартами подотчетности».

Для достижения этой цели процедуры государственных закупок могут налагать определенные обязательства по обеспечению прозрачности и предварительной оценки поставщиков ИИ.

ВЫВОД

Обзор состояния сегмента искусственного интеллекта в информационной безопасности позволяет сделать следующие выводы:

Основные методы защиты трафика от утечки в ВОЛС можно разделить на три основные группы методов защиты от перехвата такой информации злоумышленником:

1. Физические средства защиты информации;

2. Аппаратные средства защиты информации;

3. Криптографическая защита информации.

Искусственные нейронные сети являются ключевым направлением развития из области искусственного интеллекта для решения задач информационной безопасности.

Все процессы в целом при этом методе шифрования информации происходят посредством исполнения физических методов. Одним из примеров работы квантово-криптографических алгоритмов является движение некоторого количества электронов в электрическом поле или фотонов в волоконно-оптических линиях связи. Такая схема включает в себя квантовый канал и специальное оборудование, размещенное на обоих концах системы. Искусственный интеллект вносит заметный вклад в борьбу с современными информационными угрозами.

В результате работы видно, что технологии ИНС являются одними из самых инновационных и прорывных достижений науки на сегодняшний день. Эти средства широко внедряются практически во все сферы жизни современного человека, начиная от бытовых и заканчивая профессиональными. В данной работе более подробно были рассмотрены вопросы, связанные с интеграцией искусственных нейронных сетей в системы защиты информации.

ЛИТЕРАТУРА

1. Artificial Intelligence and Autonomy in Russia. — CNA Report. - May. 2021. Режим доступа: https://www.cna.org/CNA_files/ centers/CNA/sppp/fsp/russia-ai/Russia-Artificial-lntelligence-Autonomy- Military.pdf

2. Guaranteeing Al Robustness Against Deception (GARD). Режим доступа: https://darpa.mil/program/guaranteeing-ai-robustness- against-deception.

3. A Taxonomy and Terminology of Adversarial Machine Learning. Draft NISTIR 8269, October 2019. Режим доступа: https://doi. org/10.6028/NIST.IR.8269-draft

4. Adversarial ML Threat Matrix. December 2020. Режим доступа: https://github.com/mrtre/advmlthreatmatrix.

5. Грибунин. В.Г. Беэопасность систем машинного обучения. Защищаемые активы уязвимости, модель нарушителя и угроз. таксономия атак. / В.Г. Грибунин, В.Г., РЛ Гришаненко. А.П. Лабазников. А.А. Тимонов // Известия института инженерной физики. — Серпухов. - 2021 г. — №3. — С.65-71.

6. Vadillo J.. Santana R. Universal adversarial examples in speech command classification. - Preprint. - 2021. - Режим доступа: https://arxiv.org/pdf/1911.10182.pdf

7. Chakraborty A. A survey on adversarial attacks and defences. /A.Chakraborty, M.AJam. V.Dey, A.Chattopadhyay. D.Mukhopadhyay//CAA1 Transactions on Intelligence Technology. - 2021. — v.6. — P.25-45.

8. Machado G.R. Adversarial Machine Learning Image classification: A Survey Towards the Defender's Perspective/G.R. Machado. E. Silva, R. R. Goldschmidt // Preprint — September. 2020. Режим доступа: httpsy/arxjv.org'pdf/2009.0372vl.

9. Moosavi-Dezfooh S. DeepFool: a simple and accurate method to fool deep neural networks / S.Moosavi-Dezfooli. A.Fawzi. P.Frossard. // Preprint — July. 2016. Режим доступа: https://arxiv.org/ pdf/1511.04599v3.

10. Machado G. Adversarial Machine Learning in Image Classification: A Survey Towards the Defender's Perspective. /G. Machado. E.Silva, R.Goldschmidt Preprint - September 2020. - Режим доступа: https://arxiv.org/pdf/2009.0372v1