DOI 10.37882/2223-2966.2024.6-2.24

АНАЛИЗ МЕТОДОВ И ПУТЕЙ РЕШЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

ANALYSIS OF METHODS AND WAYS FOR SOLVING INFORMATION PROTECTION IN INFORMATION AND TELECOMMUNICATION SYSTEMS

A. Kolesnikov

Summary. The article is devoted to current issues related to information security in information and telecommunication systems. Special attention is paid to the problems that the industry faces today in the era of the development of cloud computing and digital technologies. In addition, the research process presents the author's approach to constructing a security architecture for information and telecommunication systems, based on neural network technologies. Significant problems for information protection in ITS are identified. A promising method of protection against moving targets is described, its capabilities and areas of application are outlined.

Keywords: data, protection, information and telecommunication system, network, cloud, attack.

Колесников Антон Александрович
Санкт-Петербургский Политехнический университет Петра Великого
anton.kolesnikov.science@mail.ru

Аннотация. Статья посвящена актуальным вопросам, связанным с защитой информации в информационно-телекоммуникационных системах. Отдельное внимание уделено проблемам, с которыми сегодня сталкивается отрасль в эпоху развития облачных вычислений и цифровых технологий. Кроме того, в процессе исследования представлен авторский подход к построению архитектуры защиты информационно-телекоммуникационных систем, базирующийся на нейросетевых технологиях. Определены значимые проблемы для защиты информации в ИТС. Описан перспективный метод защиты от движущихся целей, обозначены его возможности и сферы применения.

Ключевые слова: данные, защита, информационно-телекоммуникационная система, сеть, облако, атака.

Ограниченные в прошлом нишевыми областями, такими как банковское дело, аэрокосмическая промышленность или военные приложения, безопасность данных и защита информации постепенно и уверенно становятся частью всех областей жизнедеятельности общества и социальных систем. По мере того, как компьютеры и сети приобретают статус неотъемлемого элемента повседневной жизни, о безопасности в информационных сетях говорят уже не только профильные эксперты, но также правительственные структуры и обычные пользователи. Поскольку многие аспекты современной деловой и частной жизни зависят от компьютеров и сетей, крайне важно, чтобы они работали безопасно.

Особую актуальность данная проблематика приобретает для информационно-телекоммуникационных систем. Связано это с тем, что телекоммуникационные компании быстрыми темпами внедряют новые платформы и среды, трансформируя свою инфраструктуру и расширяя возможности. Ожидается, что в период 2024–2027 годов телекоммуникационные корпорации инвестируют в инфраструктуру 5G более 600 миллиардов долларов [1]. Однако 5G — это лишь самая заметная часть трансформации. За кадром происходят еще более масштабные изменения. Мультиоблачность стала реальностью для телекоммуникационных компаний, 80 % телекоммуникационных провайдеров имеют двух или более поставщиков услуг инфраструктуры как сервиса (IaaS), а среднее количество приложений программного обеспечения, используемых ими, составляет 113, по сравнению с 97 для предприятий в целом [2]. Все это повышает сложность и делает защиту данных еще более важной и комплексной задачей.

По данным компании EfficientIP, занимающейся вопросами кибербезопасности, в 2023 году 43 % операторов связи пострадали от атак вредоносного ПО на базе системы доменных имен (DNS), причем 81 % из них потребовалось три дня и более для применения критически важного исправления безопасности после обнаружения утечки данных. В том же отчете отмечено, что в телекоммуникационном секторе похищается больше всего конфиденциальных данных среди всех отраслей: 30 % операторов связи, принявших участие в исследовании, сообщили о краже конфиденциальной информации клиентов [3].

Таким образом, принимая во внимание тот факт, что телекоммуникационная сфера входит в число отраслей-

лидеров, в которых накапливаются самые большие объемы конфиденциальной информации в мире, поскольку миллионы людей делятся с компаниями личной информацией и финансовыми данными, вопросы обеспечения безопасности сетей являются актуальными, теоретически и практически значимыми, что и обусловило выбор темы данной статьи.

Ключевые аспекты и меры, которые следует учитывать для защиты данных и конфиденциальности в информационно-телекоммуникационных системах, рассматривают в своих трудах Кадирманов К.Б., Оразымбетова А.К., Анищенко А.В., Чуприн Д.В., Грозмани Е.С., Yuling Chen, Jing Sun, Yixian Yang.

Над усовершенствованием правил обеспечения безопасности при обработке персональных данных и формирования уведомлений об утечках конфиденциальной информации трудятся Стародубцев Ю.И., Худайназаров Ю.К., Кныш Т.П., Hongsen Zou, Zheng Xiang, Weiping Shang, Josip Milanovic.

Однако, несмотря на имеющиеся труды и наработки, весьма справедливо отмечают эксперты, что ни одна угроза сегодня не может быть устранена изолированно, и что субъекты угроз будут продолжать использовать уязвимости в принятых технологиях для достижения своих целей. Поэтому в перманентной актуализации нуждаются способы защиты данных с учетом постоянно меняющегося ландшафта коммуникаций. Также, отдельного внимания заслуживают методы решения проблемы использования традиционных инструментов сетевой защиты из-за статического характера сервисов и конфигураций информационно-телекоммуникационных сетей.

Итак, цель статьи заключается в проведении анализа подходов к решению защиты информации в информационно-телекоммуникационных системах (ИТС).

Современная защита информации в ИТС основана на таксономии угроз безопасности, которая включает конфиденциальность, целостность, доступность и кражу [4]. Это основные соображения или составляющие современной «компьютерной коммуникационной безопасности». Другими словами, требуется защита от утечки конфиденциальной информации (конфиденциальность), от червей/вирусов, влияющих на работу критически важных приложений (целостность), от ботнетов, выводящих из строя важную систему (доступность), или от кражи личных данных граждан (кража личных данных).

Как уже отмечалось ранее, телекоммуникационная отрасль стремительно развивается, открывая огромные возможности для бизнеса, но в тоже время актуализируя массу новых задач перед сотрудниками служб безопасности. Обозначим ряд наиболее значимых проблем для защиты информации в ИТС.

1. Миграция в облако — переход на облачные сервисы стал одной из основных разрушительных тенденций последних лет, что позволило телекоммуникационным компаниям стать более гибкими. Однако эта трансформация сопряжена с проблемами безопасности, поскольку облачные сервисы зачастую не менее, а то и более уязвимы, чем локальные системы. Чтобы обеспечить защиту своих облачных сервисов, телекоммуникационным компаниям необходимо внедрить надежные протоколы безопасности, комплексное шифрование и передовые системы аутентификации.
2. Безопасность сетей 5G — развитие сетей пятого поколения имеет значительные последствия для сохранности данных. К ним будет подключено больше устройств, чем когда-либо прежде, что сделает их более уязвимыми для атак. Для решения этой проблемы телекоммуникационным компаниям необходимо инвестировать в интегрированные системы безопасности.
3. Растущая тенденция BYOD — поскольку сотрудники все чаще используют для работы собственные устройства, телекоммуникационным компаниям необходимо обеспечить их безопасное подключение к корпоративной сети. Также целесообразно внедрять технологии для защиты конфиденциальных данных и конфиденциальных коммуникаций от компрометации.
4. Положения о защите данных — в связи с появлением многочисленных законов о защите данных, телекоммуникационные компании должны не только соблюдать эти положения, но и обеспечивать безопасность своих данных. Для этого необходимо инвестировать в технологии, повышающие конфиденциальность, такие как шифрование и маскировка данных.
5. Кроссплатформенные возможности. Телекоммуникационные компании часто используют среду смешанных операционных систем. Большинство продуктов безопасности ориентированы на конкретную операционную систему (часто Windows, которая является преобладающей операционной системой на предприятии) и предлагают только урезанные версии для других операционных систем [5].

С учетом вышеизложенного, можно отметить, что, по мнению автора, эффективная стратегия защиты информации ИТС должна быть основана на двух основных концепциях: 1) фокус на предотвращении угрозы, а затем, 2) надежное реагирование и нивелирование угрозы, в случае ее возникновения.

На рис. 1 представлена архитектура защиты данных в ИТС.

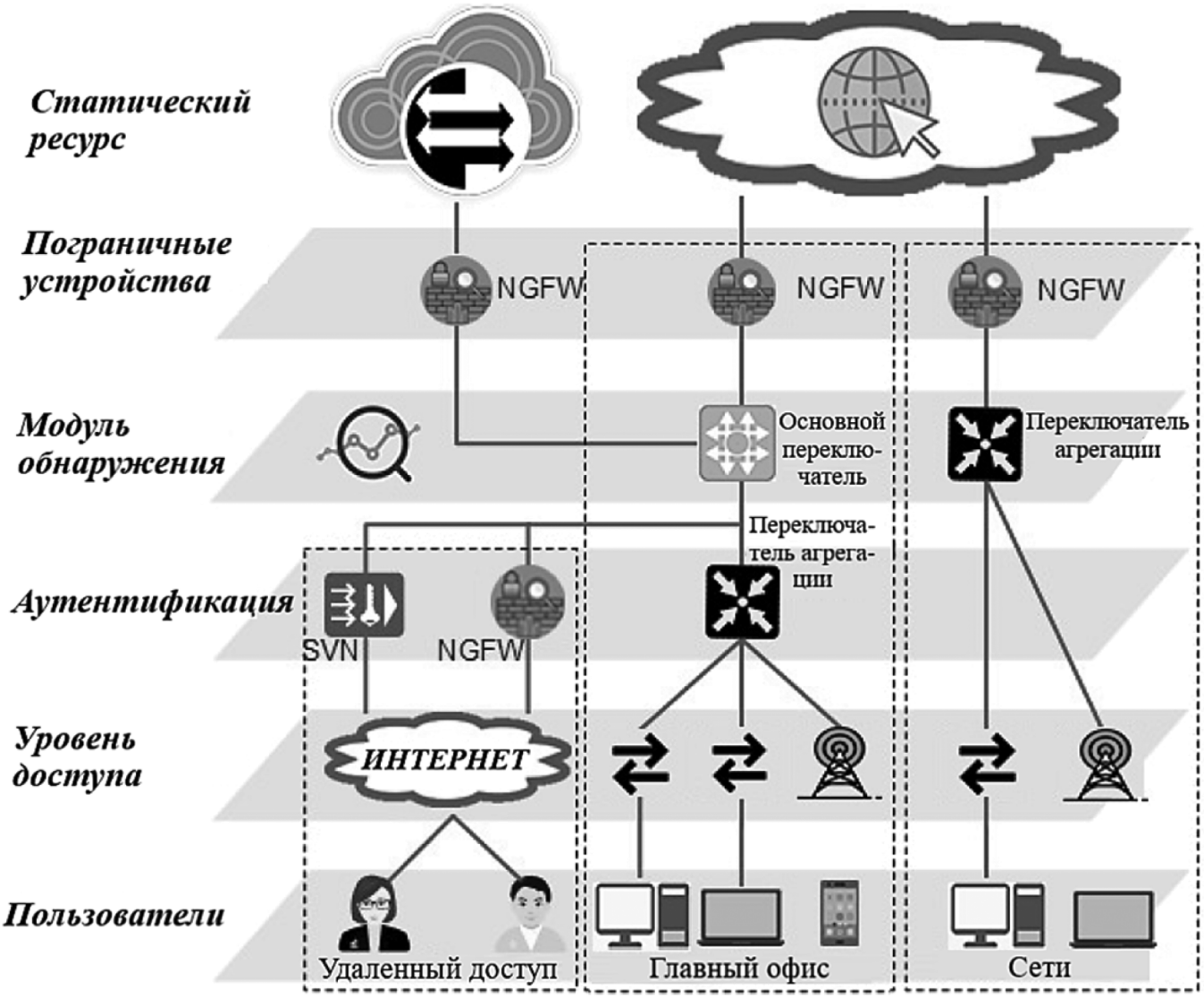

Рис. 1. Архитектура защиты данных в ИТС[1]

В рамках представленной архитектуры модуль обнаружения атак размещается на коммутаторе ядра, что способствует прохождению сетевого трафика. Опишем более подробно как работает данная архитектура, уделив внимание набору данных, предварительной обработке данных, моделям и алгоритмам.

Набор данных. Набор данных, используемый для реализации предлагаемой модели, является простым набором потоковых данных, применяемых для анализа сетевого трафика. Необработанные данные сетевого трафика в формате pcap перехватываются с помощью зеркалирования портов на коммутаторе. Доброкачественный трафик собирается непосредственно при подключении к сети, чтобы убедиться, что он не содержит вредоносных намерений. Набор данных состоит как из обычных экземпляров, так и из сложных угроз (например, Gafgyt, Mirai). Gafgyt и Mirai — это две группы вредоносных программ, которые выполняют Botnet-атаки на различные интеллектуальные устройства [6].

Предварительная обработка данных. Поскольку данные часто собираются из разных источников и доступны в разных форматах, их нецелесообразно напрямую подавать алгоритму для классификации. Есть вероятность столкнуться с некоторыми проблемами в наборе данных из-за человеческих ошибок, ошибок устройства или же недостатков в проблеме сбора. Предварительная обработка данных представляет собой полный процесс преобразования исходных данных в последовательную форму, которая может быть подана классификаторам. Кроме того, она дополнительно снижает сложность экземпляров с точки зрения емкости и времени. Для обеспечения жизнеспособности системы необходимо привести все значения признаков к масштабируемому виду от 0 до 1. Для этого используется скалярная функция

[1] SVN — аутентификация по требованию сервера с кешированием, NGFW — брандмауэр нового поколения

python Standard, позволяющая стандартизировать набор данных. С целью уменьшения количества повторов данных и улучшения целостности информации необходимо провести трансформацию данных, которая устраняет пропущенные, дублирующиеся и нулевые значения. Преобразование выполняется с помощью кодирования меток. Кодирование меток выполняется таким образом, чтобы данные могли быть легко приняты алгоритмом, сохраняющим их первоначальное значение.

Модуль обнаружения. В рамках предлагаемой архитектуры модуль обнаружения базируется на особом виде рекуррентных нейронных сетей, способных обучаться долгосрочным зависимостям, которые делают сеть «умной» в запоминании того, что происходило в прошлом, и поиске закономерностей во времени, чтобы ее следующие предположения имели смысл. Нейронная сеть используется для исследования вредоносного ПО. В результате основу архитектуры безопасности составляет эффективная, мощная и универсальная система идентификации вредоносных программ, которая позволяет выявлять их различные классы. Вид гибридного модуля обнаружения вредоносных программ в ИТС на основе нейронной сети показан на рисунке 2.

Первым этапом схемы обнаружения является предварительная обработка набора данных, который был получен на предыдущем этапе. Второй этап предлагаемой модели — обучение гибридных классификаторов. В процессе обучения обработанные данные передаются классификаторам (т.е. DNN, LSTM), а полученные результаты объединяются для лучшей оптимизации и конечной производительности гибридных классификаторов.

Алгоритмы. Long Short-Term Memory (LSTM) — это алгоритм, принадлежащий к семейству рекуррентных нейронных сетей (RNN) моделей глубокого обучения (DL). LSTM хорошо известен своей потенциальной способностью к обучению длинных последовательностей и сохранению информации в наборе данных. Конволюционная нейронная сеть (CNN) — еще один алгоритм глубокого обучения, который известен своими возможностями извлекать значимые признаки из данных. Глубокая нейронная сеть (DNN) или полностью подключенная нейронная сеть (FNN) — базовая модель в категории глубокого обучения с простыми нейронами, соединенными в многоуровневой архитектуре.

Таким образом, предложенная архитектура представляет собой мощный, адаптируемый и продуктивный метод обнаружения вредоносных программ на основе нейронных сетей для защиты ИТС.

И в завершении исследования представляется целесообразным акцентировать внимание на таком прогрессивном приеме защиты данных в ИТС как метод защиты с использованием движущихся целей (MTD). Данный метод базируется на концепции контроля изменений на разных иерархиях системы с целью повышения неопределенности и кажущейся сложности для злоумышленников, а также для уменьшения окна их возможностей и увеличения затрат на исследования и атаки.

MTD значительно усложняет злоумышленникам разработку и использование инструментов эксплойтов, снижая эффективность автоматизированных атак и делая успешные атаки более трудоемкими и дорогостоящи-

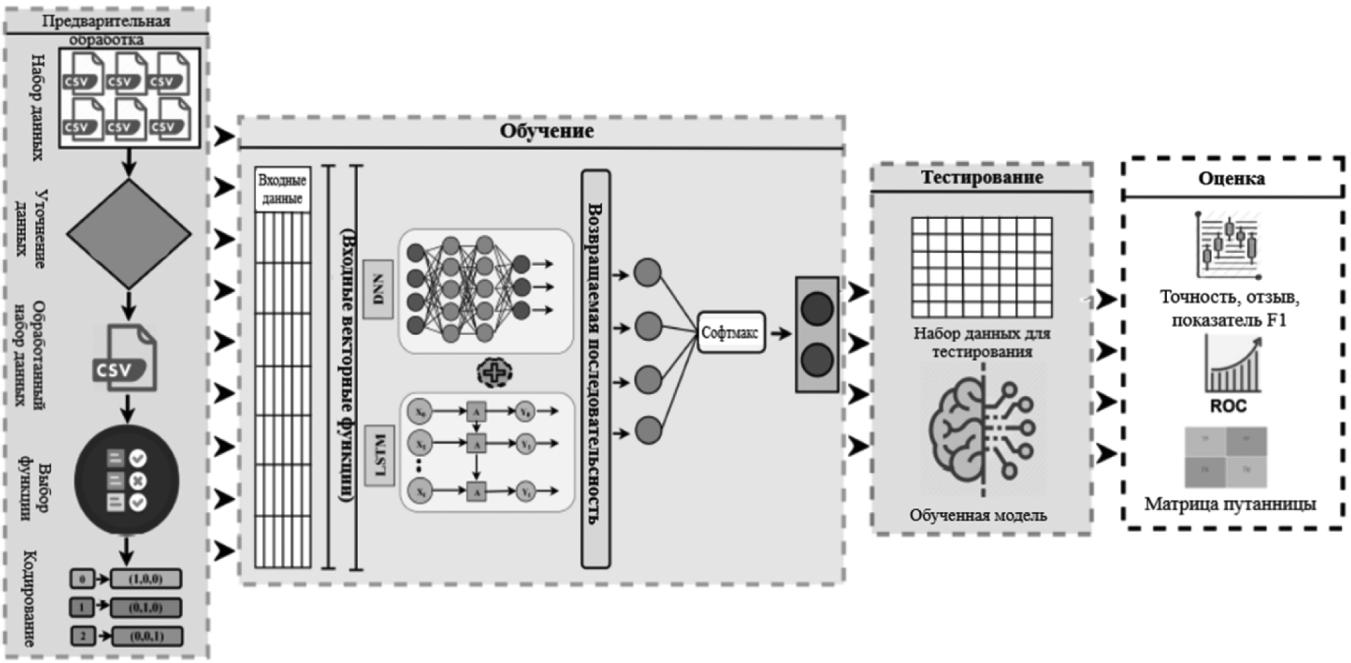

Рис. 2. Предлагаемая гибридная архитектура глубокого обучения нейронной сети для выявления атак на ИТС

ми. Кроме того, защита с использованием движущихся целей делает сложным решение задачи по сохранению устойчивости и контроля над взломанной системой. Таким образом, MTD является очень эффективной техникой для повышения безопасности ИТС.

Один из примеров использования MTD в ИТС — защита сотовых сетей от кибератак. В результате постоянного изменения инфраструктуры сети и протоколов связи, злоумышленникам становится гораздо сложнее проникнуть в сеть и нарушить работу сервиса. Другой пример — развертывание программно-определяемых сетей в телекоммуникационных системах. Методы MTD могут использоваться для динамической реконфигурации топологии сети и перемещения критически важных ресурсов в ответ на обнаруженные угрозы, что затрудняет хакерам поиск конкретных уязвимостей.

Таким образом, подводя итоги, отметим, что в современном взаимосвязанном мире безопасность данных в ИТС имеет первостепенное значение. Понимая значение телекоммуникационной безопасности, проблемы, с которыми она сталкивается, и внедряя передовые методы, организации могут обеспечить безопасность связи, защитить конфиденциальную информацию и сохранить доверие своих клиентов.

В статье представлен авторский подход к построению архитектуры защиты информации в ИТС, который базируется на нейросетевых технологиях. Также подробно описан перспективный метод защиты от движущихся целей, обозначены его возможности и сферы применения.

ЛИТЕРАТУРА

1. Жидко Е.А. Критерий обеспечения безопасности и защиты информации в информационно-телекоммуникационной системе // Воздушно-космические силы. Теория и практика. 2022. № 24. С. 92–103.
2. Баранов В.В. Подход к управлению безопасности информационно-телекоммуникационной сети на основе нейросетевых систем // I-methods. 2021. Т. 13. № 3.
3. Yong Xie Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges // Software: Practice and Experience. 2021. Volume 51, Issue 11. P. 23–29.
4. Будзко В.И. Ключевые системы в больших информационно-телекоммуникационных системах, реализующих технологии распределенных обработки и хранения данных // Системы высокой доступности. 2021. Т. 17. № 3. С. 5–15.
5. Chinnathangam Karthikraja An empirical intrusion detection system based on XGBoost and bidirectional long-short term model for 5G and other telecommunication technologies // Computational Intelligence. 2022. Volume 38, Issue 4. P. 67–72
6. Сиротский А.А. Противодействие утечкам персональных данных из телекоммуникационных систем // REDS: Телекоммуникационные устройства и системы. 2023. Т. 13. № 3. С. 33–40.

Журнал «Современная наука: актуальные проблемы теории и практики»