

ПРОГНОЗНАЯ МОДЕЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ¹

Авраменко В.С.², Саенко И.Б.³, Котенко И.В.⁴

Ключевые слова: безопасность информации, прогнозирование, показатель защищенности, машинное обучение, оценка точности.

Аннотация

Цель работы: разработка прогнозной модели защищенности информации в инфокоммуникационных системах (ИКС) на основе рекуррентных нейронных сетей, обеспечивающей высокую точность прогнозов значений показателей защищенности информации.

Методы исследования: системный анализ, классификация, моделирование, машинное обучение с помощью искусственных нейронных сетей.

Результаты исследования: разработана прогнозная модель защищенности информации в ИКС на основе рекуррентной нейронной сети; проведена экспериментальная оценка точности прогнозирования защищенности информации; обоснована целесообразность использования комплексных показателей защищенности информации в качестве прогнозных величин и рекуррентных нейронных сетей для прогнозирования их значений.

Практическая ценность: уточнены концептуальные положения по прогнозированию защищенности информации в ИКС.

DOI: 10.24412/1994-1404-2025-2-140-147

Введение

Проблема защиты информации в инфокоммуникационных системах (ИКС) относится к классу постоянных, требует регулярного исследования с учетом изменений в защищаемой системе и ландшафта угроз безопасности информации. В настоящее время публикуемые статистические данные свидетельствуют о росте количества компьютерных инцидентов безопасности в ИКС различного назначения, в том числе относящихся к объектам критической инфраструктуры. Помимо традиционных факторов, связанных с появлением новых уязвимостей, средств и технологий реализации компьютерных атак, в том числе и с использованием технологий искусственного интеллекта [1], увеличение количества атак обусловлено сложившейся геополитической обстановкой.

Следует отметить, что объектом компьютерных атак становятся и модели машинного обучения, все чаще используемые в различных сферах деятельности, что требует разработки и внедрения соответствующих методов и технологий защиты [2—4]. В целом ситуация характеризуется значительным повышением нагрузки на системы защиты информации в ИКС, необходимостью привлечения дополнительных сил и средств для обработки возрастающего количества инцидентов безопасности и реагирования на них. В таких условиях возрастает актуальность задачи прогнозирования угроз безопасности информации и уровня защищенности информации в ИКС в целом с целью своевременного проведения мероприятий по предотвращению перехода ИКС в незащищенное состояние.

¹ Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.

² **Авраменко Владимир Семенович**, кандидат технических наук, доцент, профессор Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-2452-0380.

E-mail: vsavr@yandex.ru

³ **Саенко Игорь Борисович**, доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-9051-5272.

E-mail: ibsaen@comsec.spb.ru

⁴ **Котенко Игорь Витальевич**, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), заслуженный деятель науки РФ, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0001-6859-7120.

E-mail: ivkote@comsec.spb.ru

В системах защиты информации ИКС функция прогнозирования защищенности информации в автоматическом режиме практически не реализуется. Основными причинами проблемы прогнозирования защищенности информации является недостаточно высокая результативность прогнозных аналитических и статистических моделей защищенности и низкий уровень автоматизации существующих решений по прогнозированию защищенности.

Одним из путей решения повышения эффективности прогнозирования защищенности информации в ИКС является применение технологий машинного обучения, в частности, — рекуррентных нейронных сетей, хорошо зарекомендовавших себя в задачах прогнозирования временных последовательностей в различных предметных областях [5, 6].

Данная работа посвящена исследованию возможностей рекуррентных нейронных сетей для повышения точности прогнозирования уровня защищенности информации в ИКС. Новизна работы заключается в применении рекуррентных нейронных сетей для прогнозирования комплексных показателей защищенности информации, в отличие от известных, совместно учитывающих зависимости процессов нарушений безопасности и восстановления защищенности информации.

Обзор исследований

Исследования в области применения технологий искусственного интеллекта для решения задач защиты информации, в том числе для прогнозирования уязвимостей, атак, угроз и состояния защищенности информации в ИКС, ведутся достаточно активно. В частности, в [7] рассматривается влияние архитектуры искусственной нейронной сети на эффективность обнаружения сетевых атак, обсуждаются преимущества и недостатки различных архитектур, а также проблемы, связанные с их использованием. В [8] предложена модель прогнозирования ситуации на основе темпоральной сверточной сети, которая фокусируется на проблеме долгосрочного прогнозирования временных рядов. В [9] представлен обзор методов прогнозирования в области защиты информации, обсуждается задача прогнозирования следующего шага или намерения злоумышленника, предсказания предстоящих кибератак и прогнозирования безопасности всей сети. В [10] предлагается метод прогнозирования сетевой безопасности, основанный на модели LSTM-XGBoost, в котором модель сети LSTM используется для прогнозирования сетевых вторжений, а XGBoost применяется для оценки ситуации на основе прогнозируемых данных. В [11] рассматривается методика прогнозирования показателей защищенности информации в автоматизированных системах на основе статистических методов. В [12] для прогнозирования безопасности защищенных систем предлагается нейро-нечеткая сеть, обеспечивающая возможность использования слабо формализованных данных и обучение в режиме реального време-

ни. В [13] предложен метод прогнозирования ситуации безопасности в программно-определяемой сети. В [14] исследованы методы предотвращения, прогнозирования и распознавания угроз информационной безопасности, которые направлены на снижение ущерба из-за недостатков существующих подходов управления рисками. В [15] для прогнозирования атак UDP-flood используются модели экспоненциального сглаживания и нейросетевого прогнозирования. В [16] обсуждается прогнозирование и распознавание намерений при многоэтапной или постоянной сетевой атаке. В [17] предложены стохастические модели прогнозирования ущерба от инцидентов безопасности в информационных системах, учитывающие статистику временных и объемных характеристик ущерба. В [18] представлен метод прогнозирования рисков сетевой информационной безопасности, основанный на сверточной нейронной сети. В [19] описаны взаимосвязанные модели и методы, систематизированные для использования при планировании и реализации стандартизованных процессов системной инженерии. Их применение позволяет осуществлять анализ влияния защищенности информации в терминах прогнозируемых рисков. В [20] исследуется влияние функции потерь в нейронных сетях на эффективность прогнозирования и производится сравнение статистических методов и нейронных сетей при прогнозировании осведомленности о ситуации сетевой безопасности. Делается вывод, что нейронные сети более точны для прогнозирования ситуации в области сетевой безопасности. В [21] предложена модель прогнозирования инцидентов информационной безопасности на основе метода ближайшего соседа.

Таким образом, обзор исследований показывает, что прогнозирование защищенности информации является актуальной задачей защиты информации в ИКС, для решения которой используются как традиционные статистические методы, так и методы машинного обучения с использованием нейронных сетей. Предлагаемый в работе подход к прогнозированию отличается применением рекуррентных нейронных сетей для прогнозирования значений комплексных показателей защищенности информации в ИКС в целом.

Концептуальные положения по прогнозированию защищенности информации в ИКС

Под прогнозом защищенности информации в ИКС понимается предположение о возможных состояниях защищенности ИКС в будущем и (или) о путях и сроках перехода в эти состояния. Прогнозирование защищенности информации может выполняться как отдельная функция управления защитой и (или) частная функция планирования, контроля (мониторинга) защищенности. Целью прогнозирования защищенности информации в ИКС является получение оценок состояния защищенности информации ИКС в будущем для обеспечения своевременного проведения мероприятий

упреждающего характера на возможное нарушение защищенного состояния ИКС. Прогнозировать защищенность целесообразно как при проектировании ИКС, так и в ходе ее функционирования.

Методы и модели прогнозирования защищенности определяются задачами защиты информации в ИКС, полнотой и степенью неопределенности имеющейся информации о состоянии защищенности в прошлом, условиями функционирования ИКС, требованиями к показателям эффективности прогнозирования. По характеру информации, на основе которой осуществляется прогнозирование защищенности, можно выделить фактографические, экспертные и комбинированные методы. При наличии достоверных статистических данных для прогнозирования защищенности целесообразно использовать фактографические методы, основанные на анализе динамических (временных) рядов характеристик (параметров) защищенности информации.

Эффективность прогнозирования защищенности определяется точностью, оперативностью и ресурсоемкостью прогнозирования. На точность прогноза в первую очередь влияют выбранные методы прогнозирования, а также данные из источников, которые должны быть достоверны, сопоставимы, представительны, однородны и устойчивы. Такими источниками могут быть различного рода журналы событий аппаратных и программных средств построения ИКС и средств защиты информации, консолидированные данные из собственных и внешних центров мониторинга информационной безопасности, информация об уязвимостях и компьютерных атаках как из публичных, так и из собственных источников, заключения экспертов.

Ключевой задачей прогнозирования является разработка прогнозной модели защищенности. Под прогнозной моделью защищенности ИКС понимается модель системы защиты информации ИКС, исследование которой позволяет получить совокупность данных о возможных состояниях защищенности ИКС в будущем и (или) путях и сроках их осуществления.

В общем виде прогнозная модель защищенности информации в ИКС по аналогии с классическими моделями имеет следующий вид:

$$y_3(t) = tr(t) + S(t) + I(t) + \varepsilon \quad (1)$$

где $y_3(t)$ — прогнозное значение характеристики или показателя защищенности, $tr(t)$ — тренд, представляющий собой плавно изменяющуюся составляющую, отражающую влияние оказывающих долговременное воздействие факторов на процессы защиты информации; $S(t)$ — циклическая составляющая, отражающая регулярную повторяемость процессов защиты во времени (в течение года, недели, суток и др.); $I(t)$ — интервенции (резкие изменения уровня защищенности под влиянием факторов, которые практически сложно локализовать во времени с точки зрения возможности предвидения); ε — нерегулярная составляющая.

При отсутствии объективных предпосылок для цикличности основных процессов защиты и непредвиденных воздействий может использоваться упрощенная прогнозная модель защищенности:

$$y_3(t) = tr(t) + \varepsilon \quad (2)$$

Для формирования прогноза защищенности как случайного нестационарного процесса необходимо произвести декомпозицию исходного процесса на регулярную (тренд) и нерегулярную составляющие. Тренд описывает устойчивые тенденции изменения значений показателей защищенности информации. Нерегулярная составляющая характеризует случайную непрогнозируемую часть и возможные отклонения фактических значений показателей защищенности от тренда. Выделенный в результате декомпозиции тренд может в дальнейшем использоваться в качестве основы прогнозной модели защищенности.

Прогнозная модель защищенности должна обеспечить требуемую точность и достоверность прогноза, но при этом минимизировать значения показателей оперативности и ресурсоемкости прогнозирования.

В качестве показателя точности прогноза комплексных показателей защищенности может использоваться средняя абсолютная ошибка прогноза в процентах (Mean Absolute Percentage Error, MAPE).

В качестве показателя оперативности прогноза защищенности целесообразно использовать время, затраченное на разработку прогноза. С учетом направленности исследования на реализацию прогнозирования защищенности ИКС в автоматизированном режиме в качестве показателя ресурсоемкости может применяться коэффициент использования вычислительных ресурсов, отражающий загруженность процессора и оперативной памяти. Могут использоваться также финансово-экономические показатели.

Другой вариант постановки задачи на прогнозирование защищенности может быть сформулирован следующим образом: прогнозная модель должна обеспечить максимально возможную точность прогноза при заданных ограничениях на значения показателей оперативности и ресурсоемкости прогнозирования. При определении требований к оперативности прогноза следует учитывать время, необходимое на анализ результатов прогнозирования и проведение мероприятий по реагированию.

Можно выделить два основных направления решения задачи разработки прогнозной модели значений показателей защищенности информации в рамках модели временных рядов: на основе

- статистических моделей (регрессии, экспоненциального сглаживания и т. д.) и
- структурных моделей (цепи Маркова, классификационные деревья, нейронные сети и другие).

С учетом результатов исследований в данной области перспективным направлением решения задачи прогнозирования показателей защищенности информации в ИКС является использование рекуррентных нейронных сетей.

Прогнозная модель защищенности информации на основе рекуррентных сетей

Первоочередной задачей прогнозирования защищенности информации в ИКС является определение целей прогнозирования и прогнозируемых показателей защищенности. В интересах управления защитой информации в ИКС могут использоваться прогнозы как единичных, так и комплексных показателей защищенности информации. В качестве единичных могут использоваться такие показатели, как интенсивность появления уязвимостей, интенсивность нарушений безопасности информации, величина ущерба, интенсивность восстановления защищенности информации. Но для прогнозирования уровня защищенности информации в ИКС в целом целесообразно использовать комплексные показатели защищенности информации, учитывающие характеристики как процесса нарушения безопасности, так и восстановления защищенного состояния. В частности, в качестве прогнозной величины может быть использован коэффициент защищенности информации K_3 , определяемый следующим образом:

$$K_3 = \frac{\mu_{вз}}{\lambda_{нб} + \mu_{вз}} \quad (3)$$

где $\lambda_{нб}$ — интенсивность нарушений безопасности в ИКС; $\mu_{вз}$ — интенсивность восстановления защищенности информации в ИКС.

Показатель $\mu_{вз}$ отражает возможности системы защиты информации по восстановлению защищенности информации, включающее задачи обнаружения и диагностирования нарушений безопасности, а также реагирования на них.

Более точно оценить защищенность информации в ИКС возможно при учете процессов нарушения безопасности и восстановления защищенности для каждого защищаемого ресурса ИКС. При наличии возможности восстановления защищенности только одного ресурса для расчета коэффициента защищенности информации в ИКС может использоваться следующая формула:

$$K_3 = 1 / \sum_{i=0}^{N_{зр}} A_{N_{зр}}^i \left(\frac{\lambda_{нб,i}}{\mu_{вз,i}} \right)^i \quad (4)$$

где $N_{зр}$ — количество защищаемых ресурсов в ИКС; $A_{N_{зр}}^i = \frac{N_{зр}!}{(N_{зр}-i)!}$ — число размещений из $N_{зр}$ по i .

При условно неограниченных возможностях по восстановлению защищенности ресурсов расчетное выражение следующее:

$$K_3 = \prod_{i=1}^{N_{зр}} \frac{\mu_{вз,i}}{\lambda_{нб,i} + \mu_{вз,i}} \quad (5)$$

Из известных апробированных моделей машинного обучения для прогнозирования защищенности целесообразно использовать рекуррентные нейронные сети (Recurrent Neural Network, RNN), хорошо зарекомендовавшие себя в задачах прогнозирования временных рядов. Наиболее распространенными являются RNN Элмана, LSTM-сети и Gated Recurrent Units (GRU) [5]. Ос-

новным преимуществом сетей LSTM и GRU является решение проблемы исчезающего градиента, характерной для простейшей рекуррентной нейронной сети. В [5] показано, что в задачах прогнозирования временных рядов LSTM демонстрирует более высокую точность, чем GRU и RNN Элмана. Но для относительно небольших наборов данных или коротких последовательностей GRU может быть более эффективна, чем LSTM, так как способна обучаться на таких данных с меньшими вычислительными затратами без потери в точности.

Обобщенная прогнозная модель защищенности включает наборы нейронных сетей для прогнозирования единичных показателей защищенности и блок расчета прогнозных значений комплексного показателя защищенности (рис. 1).

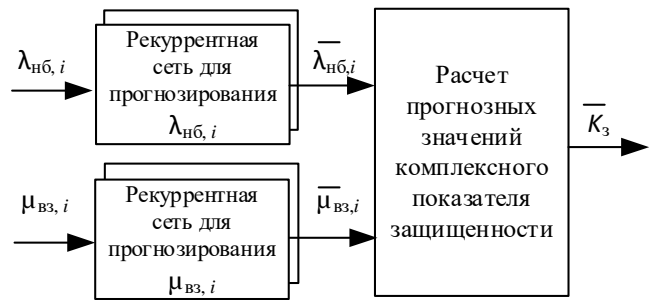


Рис. 1. Прогнозная модель защищенности информации в ИКС на основе рекуррентных сетей

На входы рекуррентных сетей подаются последовательности значений интенсивностей нарушений безопасности $\lambda_{нб}$ и интенсивностей восстановления защищенности $\mu_{вз}$ для каждого i -го защищаемого ресурса, рассчитываемых на основе исходных статистических данных. На выходе рекуррентных сетей формируются прогнозные значения единичных показателей защищенности. Далее рассчитываются прогнозные значения комплексного показателя защищенности \bar{K}_3 .

Пример прогнозирования защищенности информации в ИКС

Для прогнозирования показателей защищенности информации была создана система LSTM-сетей с использованием языка программирования Python и общедоступных библиотек.

Для прогнозирования интенсивности нарушений безопасности в качестве входных данных для нейросетей использовались временные ряды интенсивностей нарушений безопасности, построенные на основе статистических данных за несколько лет, полученных из базы данных уязвимостей National Vulnerability Database (NVD).

Для обучения нейросети и прогнозирования защищенности информации в ИКС необходимо использовать статистические данные о функционировании системы защиты. В наихудшем для системы защиты информации случае, когда нарушитель имеет высокую квалификацию, постоянно отслеживает появление но-

вых уязвимостей, а также имеет возможность оперативно использовать их для реализации нарушения безопасности, интенсивность нарушений безопасности соответствует интенсивности появления уязвимостей.

Исходя из принятого допущения, в качестве примера были построены динамические (временные) ряды интенсивностей нарушений безопасности для ОС Linux (ядро Debian) на основе данных за несколько лет, полученных из базы данных NVD. Построенные временные ряды соответствовали типовым интервалам планирования защиты информации в ИКС (неделя, месяц и год). Далее была проведена подготовка данных, включающая выявление повторяющихся и незаполненных значений, аномалий и выбросов, нормализацию данных.

Для обучения LSTM-сети использовался алгоритм обратного распространения ошибки.

В ходе испытания программного макета автоматизированной системы прогнозирования защищенности информации в ИКС на выходе нейросетей формировались прогнозные значения интенсивности нарушений безопасности $\lambda_{нб,t}$ с заданным прогнозным периодом. В контрольном примере прогнозирования защищенности было сделано допущение о неизменности значения интенсивности восстановления защищенности в исследуемый период функционирования (структура и характеристики системы защиты не изменяются).

Оценка интенсивности восстановления защищенности была получена на основе статистической обработки данных о возможностях системы защиты типовой ИКС. Далее рассчитывались прогнозные значения комплексного показателя защищенности информации по формуле (3).

Аналогичный эксперимент был также проведен для прогнозной модели на основе GRU-сетей.

В качестве показателя точности прогноза защищенности использовалась средняя абсолютная процентная ошибка прогноза, рассчитываемая по формуле

$$MAPE = \frac{1}{n} \sum_{t=1}^n \frac{|e_t|}{x_t} \cdot 100, \quad (8)$$

где $e_t = x_t - \bar{x}_t$ — ошибка прогноза; x_t — фактическое значение; \bar{x}_t — прогнозное значение; n — количество прогнозных значений.

Для сравнительного анализа методов прогнозирования на основе рекуррентных сетей и традиционных статистических методов прогнозирования были рассчитаны прогнозные значения показателей защищенности на основе методов скользящего среднего и экспоненциального сглаживания с использованием тех же исходных данных, что и для нейросетей.

Результаты оценки точности прогнозов представлены в таблице 1.

Таблица 1

Результаты оценки точности прогнозов защищенности

Используемый метод прогнозирования	MAPE (%)		
	на 1 год	на 1 месяц	на 1 неделю
На основе LSTM-сети	4,6	6,8	10,4
На основе GRU-сети	5,3	7,7	11,2
Скользящего среднего	8,5	17,53	21,2
Экспоненциального сглаживания	26,3	32,7	40,9

По результатам сравнительного анализа методов прогнозирования защищенности информации, представленных в таблице 1, можно сделать вывод о том, что метод прогнозирования на основе LSTM-сети точнее, чем на основе GRU-сети, и существенно точнее классических статистических методов прогнозирования. Также очевидна закономерность увеличения точности прогноза с увеличением прогнозного периода.

Для достижения максимальной точности прогноза защищенности информации в ИКС и наличии достаточно полных и достоверных исходных данных за длительные периоды времени предпочтительным представляется использование LSTM-сетей. В условиях ограниченности статистических данных о функционировании ИКС данных в прошлом или жестких ограничений на вычислительные ресурсы целесообразно использовать GRU-сети.

Программное средство прогнозирования защищенности информации в ИКС на основе рекуррентных

сетей может использоваться как администраторами безопасности ИКС для обеспечения упреждающего оперативного реагирования, так и сотрудниками, ответственными за организацию защиты информации в ИКС, при долгосрочном планировании защиты информации. В качестве исходных данных для прогнозирования могут использоваться как имеющиеся статистические данные о процессах защиты в ИКС, так и данные об уязвимостях и угрозах из внешних источников информации.

Заключение

Использование представленной прогнозной модели защищенности информации на основе рекуррентных сетей может использоваться как разработчиками системы защиты информации ИКС, так и должностными лицами по защите информации ИКС на стадии эксплуатации для обеспечения своевре-

менного проведения мероприятий упреждающего характера по поддержанию требуемого уровня защищенности. При этом разработка и внедрение автоматизированной системы прогнозирования защищенности информации не требует существенных затрат.

Дальнейшие исследования направлены на повышение эффективности прогнозирования защищенности за счет более детального учета в прогнозной модели защищенности характеристик процессов нарушения безопасности информации, структуры и характеристик системы защиты информации, повышения степени автоматизации процесса прогнозирования.

Рецензент: **Липатников Валерий Алексеевич**, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, старший научный сотрудник научно-исследовательского центра Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия.
E-mail: lipatnikovanl@mail.ru

Литература

1. Намиот Д.Е. О кибератаках с помощью систем искусственного интеллекта // International journal of open information technologies. 2024. Т. 12. № 9. С. 132—141.
2. Котенко И.В., Саенко И.Б., Лаута О.С., Васильев Н.А., Садовников В.Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований // Вопросы кибербезопасности. 2024. № 1 (59). С. 24—38. DOI: 10.21681/2311-3456-2023-6-2-19 .
3. Kotenko I., Saenko I., Lauta O., Vasiliev N., Iatsenko D. Attacks Against Machine Learning Systems: Analysis and GAN-based Approach to Protection. Proceedings of the 7th International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’23). IITI 2023. Lecture Notes in Networks and Systems. Vol. 777. Springer, Cham. 2023. Pp. 49–59. DOI: 10.1007/978-3-031-43792-2_5 .
4. Zhou Sh., Liu Ch., Ye D., Zhu T., Zhou W., Yu Ph.S. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys. 2022. Vol. 55. No. 8. Article 163. 39 p. DOI: 10.1145/3547330.
5. Hewamalage H., Bergmeir C., Bandara K. Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. International Journal of Forecasting. 2021. Vol. 37. No. 1. Pp. 388–427. DOI: 10.1016/j.ijforecast.2020.06.008 .
6. Kotenko I., Lauta O., Kribel K., Saenko I. LSTM Neural Networks for Detecting Anomalies Caused by Web Application Cyber Attacks. Frontiers in Artificial Intelligence and Applications. Vol. 337: New Trends in Intelligent Software Methodologies, Tools and Techniques. 2021. Pp. 127–140. DOI: 10.3233/FAIA210014 .
7. Xoliyarov F.T., Gulomov S.R., Bozorov S.M. The Impact of Artificial Neural Network Architecture on Network Attack Detection. The International Conference on Future Networks and Distributed Systems (ICFNDS ’23). 2023. 9 p. DOI: 10.1145/3644713.3644792 .
8. Yin K., Yang Y., Yao C., Yang J. Long-Term Prediction of Network Security Situation Through the Use of the Transformer-Based Model. IEEE Access. 2022. Vol. 10. Pp. 56145–56157. DOI: 10.1109/ACCESS.2022.3175516 .
9. Liu H., Jiang R., Zhou B., Rong X., Li J., Li A. A Survey of Cyber Security Approaches for Prediction. 2021 IEEE 6th International Conference on Data Science in Cyberspace (DSC). 2021. Pp. 439–444. DOI: 10.1109/DSC53577.2021.00069 .
10. Gao F., Xia J., Wu D., Wang W., Wang C., Song C. Network security situation prediction based on LSTM. 2023 2nd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE). 2023. Pp. 350–354. DOI: 10.1109/CBASE60015.2023.10439145 .
11. Авраменко В.С. Методика прогнозирования защищенности информации в инфокоммуникационных системах // Перспективные направления развития отечественных информационных технологий. Материалы VI межрегиональной научно-практической конференции. 2020. С. 235—236.
12. Sklyarov V. Forecasting Performance of Security Information for Protected Systems Based on Hybrid Artificial Neural Networks. Proceedings of the 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). 2020. Pp. 1–3. DOI: 10.1109/FarEastCon50210.2020.9271334 .
13. Sheng M., Liu H., Yang X., Wang W., Huang J., Wang B. Network Security Situation Prediction in Software Defined Networking Data Plane. Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA). 2020. Pp. 475–479. DOI: 10.1109/AEECA49918.2020.9213592 .
14. Grishaeva S.A., Borzov V.I. Information Security Risk Management. Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020. Pp. 96–98. DOI: 10.1109/ITQMIS51053.2020.9322901 .
15. Тумбинская М.В., Волков В.В., Загидуллин Б.Г. Применение статистических методов для прогнозирования UDP-FLOOD атак // Вестник Дагестанского государственного технического университета. Технические науки. 2020. Т. 47. № 2. С. 108—122. DOI: 10.21822/2073-6185-2020-47-2-108-122 .

16. Buchta R., Gkoktsis G., Heine F., Kleiner C. Advanced Persistent Threat Attack Detection Systems: A Review of Approaches, Challenges, and Trends. *Digital Threats*. 2024. Vol. 5. No. 4. Article 39. Pp. 1–37. URL: <https://doi.org/10.1145/3696014>
17. Saurenko T.N., Anisimov V.G., Anisimov E.G., Kasatkin V.V., Los' V.P. Information Security Incident Forecasting. *Automatic Control and Computer Sciences*. 2021. Vol. 55. No. 8. Pp. 903–907. DOI: 10.3103/S0146411621080277 .
18. Li W. Prediction and Analysis of Network Information Security Risk Based on Convolutional Neural Network. 2021 4th International Conference on Information Systems and Computer Aided Education (ICISCAE 2021). 2021. Pp. 2819–2823. DOI: 10.1145/3482632.3487522 .
19. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // *Вопросы кибербезопасности*. 2022. № 6(52). С. 71—82. DOI: 10.21681/2311-3456-2022-6-71-82 .
20. Staňa R., Pekarčík P., Gajdoš A., Sokol P. Network Security Situation Awareness Forecasting Based on Neural Networks. *Theory and Applications of Time Series Analysis and Forecasting. ITISE 2021. Contributions to Statistics*. 2023. Pp. 255–270. DOI: 10.1007/978-3-031-14197-3_17 .
21. Беляева Т.А., Микрюков А.А. Нейросетевое прогнозирование инцидентов информационной безопасности // *Международный студенческий научный вестник*. 2023. № 6. С. 30—36.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

A PROGNOSTIC MODEL OF INFORMATION PROTECTION IN INFORMATION COMMUNICATION SYSTEMS BASED ON A RECURRENT NEURAL NETWORK

*Vladimir Avramenko, Ph.D. (Technology), Associate Professor, Professor at the Military Academy of the Signal Corps, Saint Petersburg, Russian Federation. ORCID: 0000-0002-2452-0380.
E-mail: vsavr@yandex.ru*

*Igor' Saenko, Dr.Sc. (Technology), Professor, Principal Researcher at the Laboratory for Computer Security Problems of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint Petersburg, Russian Federation. ORCID: 0000-0002-9051-5272.
E-mail: ibsaen@comsec.spb.ru*

*Igor' Kotenko, Dr.Sc. (Technology), Professor, Principal Researcher and Head of the Laboratory for Computer Security Problems of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Honoured Figure of Science of the Russian Federation, Saint Petersburg, Russian Federation. ORCID: 0000-0001-6859-7120.
E-mail: ivkote@comsec.spb.ru*

Keywords: *information security, forecasting, protection indicator, machine learning, accuracy evaluation.*

Abstract

Purpose of the study: developing a prognostic model of information protection in information communication systems (ICS) based on recurrent neural networks which ensures a high accuracy of forecasts for the values of information protection indicators.

Methods used in the study: system analysis, classification, modelling, machine learning using artificial neural networks.

Study findings: a prognostic model of information protection in ICS based on a recurrent neural network was developed. An experimental evaluation of accuracy for information protection forecasting was carried out. A justification was given for the advisability of using integrated information protection indicators as prognostic values, and recurrent neural networks for forecasting their values.

Practical value: conceptual provisions for information protection forecasting in ICS were made more specific.

References

1. Namiot D.E. O kiberatakakh s pomoshch'iu sistem iskusstvennogo intellekta. *International journal of open information technologies*. 2024. T. 12. No. 9. Pp. 132–141.

2. Kotenko I.V., Saenko I.B., Lauta O.S., Vasil'ev N.A., Sadovnikov V.E. Ataki i metody zashchity v sistemakh mashin-nogo obucheniia: analiz sovremennykh issledovani. Voprosy kiberbezopasnosti. 2024. No. 1 (59). Pp. 24–38. DOI: 10.21681/2311-3456-2023-6-2-19 .
3. Kotenko I., Saenko I., Lauta O., Vasiliev N., Iatsenko D. Attacks Against Machine Learning Systems: Analysis and GAN-based Approach to Protection. Proceedings of the 7th International Scientific Conference “Intelligent Information Technologies for Industry” (IITI'23). IITI 2023. Lecture Notes in Networks and Systems. Vol. 777. Springer, Cham. 2023. Pp. 49–59. DOI: 10.1007/978-3-031-43792-2_5 .
4. Zhou Sh., Liu Ch., Ye D., Zhu T., Zhou W., Yu Ph.S. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys. 2022. Vol. 55. No. 8. Article 163. 39 p. DOI: 10.1145/3547330.
5. Hewamalage H., Bergmeir C., Bandara K. Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. International Journal of Forecasting. 2021. Vol. 37. No. 1. Pp. 388–427. DOI: 10.1016/j.ijforecast.2020.06.008 .
6. Kotenko I., Lauta O., Kribel K., Saenko I. LSTM Neural Networks for Detecting Anomalies Caused by Web Application Cyber Attacks. Frontiers in Artificial Intelligence and Applications. Vol. 337: New Trends in Intelligent Software Methodologies, Tools and Techniques. 2021. Pp. 127–140. DOI: 10.3233/FAIA210014 .
7. Xoliyarov F.T., Gulomov S.R., Bozorov S.M. The Impact of Artificial Neural Network Architecture on Network Attack Detection. The International Conference on Future Networks and Distributed Systems (ICFNDS '23). 2023. 9 p. DOI: 10.1145/3644713.3644792 .
8. Yin K., Yang Y., Yao C., Yang J. Long-Term Prediction of Network Security Situation Through the Use of the Transformer-Based Model. IEEE Access. 2022. Vol. 10. Pp. 56145–56157. DOI: 10.1109/ACCESS.2022.3175516 .
9. Liu H., Jiang R., Zhou B., Rong X., Li J., Li A. A Survey of Cyber Security Approaches for Prediction. 2021 IEEE 6th International Conference on Data Science in Cyberspace (DSC). 2021. Pp. 439–444. DOI: 10.1109/DSC53577.2021.00069 .
10. Gao F., Xia J., Wu D., Wang W., Wang C., Song C. Network security situation prediction based on LSTM. 2023 2nd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE). 2023. Pp. 350–354. DOI: 10.1109/CBASE60015.2023.10439145 .
11. Avramenko V.S. Metodika prognozirovaniia zashchishchennosti informatsii v infokommunikatsionnykh sistemakh. Perspektivnye napravleniia razvitiia otechestvennykh informatsionnykh tekhnologii. Materialy VI mezhtsebnogo nauchno-prakticheskoi konferentsii. 2020. C. 235–236.
12. ISklyarov V. Forecasting Performance of Security Information for Protected Systems Based on Hybrid Artificial Neural Networks. Proceedings of the 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). 2020. Pp. 1–3. DOI: 10.1109/FarEastCon50210.2020.9271334 .
13. Sheng M., Liu H., Yang X., Wang W., Huang J., Wang B. Network Security Situation Prediction in Software Defined Networking Data Plane. Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA). 2020. Pp. 475–479. DOI: 10.1109/AEECA49918.2020.9213592 .
14. Grishaeva S.A., Borzov V.I. Information Security Risk Management. Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020. Pp. 96–98. DOI: 10.1109/ITQMIS51053.2020.9322901 .
15. Tumbinskaia M.V., Volkov V.V., Zagidullin B.G. Primenenie statisticheskikh metodov dlia prognozirovaniia UDP-FLOOD atak. Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki. 2020. T. 47. No. 2. Pp. 108–122. DOI: 10.21822/2073-6185-2020-47-2-108-122 .
16. Buchta R., Gkoktsis G., Heine F., Kleiner C. Advanced Persistent Threat Attack Detection Systems: A Review of Approaches, Challenges, and Trends. Digital Threats. 2024. Vol. 5. No. 4. Article 39. Pp. 1–37. URL: <https://doi.org/10.1145/3696014>
17. Saurenko T.N., Anisimov V.G., Anisimov E.G., Kasatkin V.V., Los' V.P. Information Security Incident Forecasting. Automatic Control and Computer Sciences. 2021. Vol. 55. No. 8. Pp. 903–907. DOI: 10.3103/S0146411621080277 .
18. Li W. Prediction and Analysis of Network Information Security Risk Based on Convolutional Neural Network. 2021 4th International Conference on Information Systems and Computer Aided Education (ICISCAE 2021). 2021. Pp. 2819–2823. DOI: 10.1145/3482632.3487522 .
19. Kostogryzov A.I. O modeliakh i metodakh veroiatnostnogo analiza zashchity informatsii v standartizovannykh protsessakh sistemnoi inzhenerii. Voprosy kiberbezopasnosti. 2022. No. 6(52). Pp. 71–82. DOI: 10.21681/2311-3456-2022-6-71-82 .
20. Staňa R., Pekarčík P., Gajdoš A., Sokol P. Network Security Situation Awareness Forecasting Based on Neural Networks. Theory and Applications of Time Series Analysis and Forecasting. ITISE 2021. Contributions to Statistics. 2023. Pp. 255–270. DOI: 10.1007/978-3-031-14197-3_17 .
21. Beliaeva T.A., Mikriukov A.A. Neurosetevoe prognozirovanie intsidentov informatsionnoi bezopasnosti. Mezhdunarodnyi studencheskii nauchnyi vestnik. 2023. No. 6. Pp. 30–36.