

ПРИМЕНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ВЫЯВЛЕНИЯ СКРЫТЫХ АНОМАЛИЙ В ЖУРНАЛАХ СОБЫТИЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

Саенко И. Б.¹, Цыпнятов В. Б.², Сажина А. В.³

DOI:10.21681/3034-4050-2026-5-59-66

Ключевые слова: журналы событий, логи, машинное обучение, скрытые аномальные последовательности, автоматизированная система военного назначения.

Аннотация

Цель: разработка и экспериментальное обоснование метода обнаружения скрытых аномальных последовательностей действий пользователей в журналах событий автоматизированной системы военного назначения (АСВН), основанного на использовании рекуррентных нейронных сетей с механизмом долговременной краткосрочной памяти (LSTM).

Методы: для классификации последовательностей событий применена архитектура LSTM-сети. Поскольку размеченные наборы данных для обучения в большинстве случаев отсутствуют, был разработан алгоритм генерации синтетического датасета, имитирующий поведение пользователей с разными функциональными профилями. Для достижения максимальной эффективности обнаружения скрытых аномалий проведен поиск оптимальной конфигурации гиперпараметров нейронной сети.

Результат: экспериментально подтверждено, что предложенная LSTM-модель позволяет эффективно детектировать скрытые аномальные последовательности пользовательских действий, каждое отдельное действие в которых выглядит легитимным. Определена архитектура, при которой достигается максимальное значение обобщенного показателя эффективности обнаружения аномалий. Показана практическая применимость подхода.

Научная новизна: дана математическая формализация понятия «скрытой аномальной последовательности», позволяющая определить условия, когда упорядоченный набор легитимных действий классифицируется как вредоносный. Предложен метод генерации синтетического датасета логов, воспроизводящего сложные паттерны. Экспериментально обосновано, что настройка гиперпараметров LSTM-модели влияет на способность выявлять распределенные во времени многошаговые аномалии.

Введение

Современные условия функционирования автоматизированных систем военного назначения (АСВН) характеризуются постоянным усложнением решаемых задач и ростом требований к оперативности и достоверности управления [1]. АСВН представляют собой совокупность технических и программных средств, интегрированных в единое информационное пространство, предназначенную для автоматизации процессов сбора, обработки и доведения информации до органов управления. Основное предназначение таких систем заключается в обеспечении командования достоверными и своевременными данными о состоянии своих войск и сил противника, что напрямую влияет на сокращение цикла управления и повышение точности принимаемых решений в условиях динамично меняющейся обстановки. В условиях проведения специальной военной операции, защита

АСВН от деструктивных воздействий выходит на первый план.

Проблема защиты информации в АСВН обусловлена, с одной стороны тем, что активно внедряются новые сетевые технологии, а с другой – реализуется концепция «информационной войны», где АСВН рассматриваются как одна из главных целей для воздействия. Обеспечение требуемого уровня защищенности становится возможным только благодаря постоянному анализу угроз безопасности и комплексному применению различных средств защиты. Однако большую сложность представляет поведенческий аспект. Злоумышленники, все чаще используют различные методы маскировки вредоносной активности, выдавая их под легитимные действия пользователя. Это делает традиционные средства контроля и сигнатурные методы анализа неэффективными.

В АСВН, как и в любых других корпоративных информационных системах, пользовательская

¹ Саенко Игорь Борисович, доктор технических наук, профессор, профессор кафедры Военной академии связи, Санкт-Петербург, Россия. E-mail: ibsaen@mail.ru

² Цыпнятов Валерий Борисович, кандидат технических наук, доцент, начальник кафедры Военной академии связи, Санкт-Петербург, Россия. E-mail: zvb097@mail.ru

³ Сажина Александра Владимировна, адъюнкт Военной академии связи, Санкт-Петербург, Россия. E-mail: sashasazhina@yandex.ru

активность фиксируется в журналах событий (логах), объемы которых постоянно растут. Ручной анализ таких данных практически невозможен, а классические системы обнаружения вторжений, построенные на жестко заданных правилах и сигнатурах, которые не способны распознать новые, ранее неизвестные сценарии атак. Особенно если каждое отдельное действие пользователя не нарушает политику безопасности. Такие целенаправленные атаки формируют, так называемые, скрытые аномальные последовательности, в которых вредоносный паттерн выявляется только при совокупности действия [2].

За последние годы в области обнаружения аномалий в пользовательской активности достигнут значительный прогресс. Классические подходы, основанные на статистических моделях, деревьях решений или методах кластеризации, демонстрируют хорошие результаты при выявлении изолированных отклонений. Анализ современных исследований показывает, что рекуррентные нейронные сети, в частности архитектуры с механизмом долговременной краткосрочной памяти (англ. *LongShort-TermMemory*, *LSTM*), которые рассматривают последовательный характер событий, демонстрируют существенное превосходство над традиционными методами. Тем не менее, существует недостаток, заключающийся в отсутствии обоснованных методов использования LSTM именно для задачи выявления скрытых аномальных последовательностей, при условии отсутствия размеченных реальных данных об инсайдерских угрозах [3].

В данной работе предлагается подход к обнаружению скрытых аномальных последовательностей действий пользователей на основе архитектуры LSTM. В рамках этого подхода предложен и реализован метод генерации специализированного синтетического обучающего набора данных. Этот метод показывает скрытые аномальные последовательности действий пользователя с различными профилями, обеспечивая высокую реалистичность и репрезентативность. В сформированный набор данных были целенаправленно внедрены сценарии, имитирующие действия злоумышленника, пытающегося скрыть свою активность за легитимными операциями. Это позволило создать основу для обучения и валидации модели [4].

В работе описывается процесс обучения архитектуры LSTM-модели на сгенерированном датасете [5]. Особое внимание уделено процедуре подбора и варьирования гиперпараметров. Экспериментальная оценка показала, что конфигурация сети существенно влияет на ее способность находить скрытые аномальные последовательности. Экспериментальным путем были

определены оптимальные настройки гиперпараметров, при которых достигается максимальное значение показателя эффективности (*F-меры*). Данный показатель показывает баланс между полнотой и точностью обнаружения. Значимость представленного исследования заключается в разработке метода генерации синтетического датасета и экспериментальном доказательстве высокой эффективности применения LSTM-сетей для выявления сложных аномальных последовательностей [6, 7].

Анализ релевантных работ

Обеспечение информационной безопасности АСВН связано с постоянным анализом журналов событий (логов). В условиях стремительного развития информационных технологий традиционные сигнатурные методы и системы обнаружения вторжений показывают низкую эффективность против сложных инсайдерских угроз с использованием скомпрометированных легитимных учетных записей. Как показывают современные исследования, такие атаки по своей природе являются многошаговыми [8]. В подобных сценариях каждое отдельное действие (например, чтение конфигурационного файла, вход в систему в рабочее время или выполнение штатной сетевой команды) в изоляции не нарушает правил безопасности и выглядит легитимным. Однако их совокупность, с учетом порядка выполнения, частоты и временных интервалов между событиями, образует паттерн, говорящий о злонамеренной активности [9, 10].

Первое значимое направление исследований заключалось в применении классических методов машинного обучения для анализа логов.

К ним относятся скрытые марковские модели, метод главных компонент, одноклассовый метод опорных векторов и алгоритмы на основе изолирующего леса [11, 12]. Несмотря на их эффективность при выявлении ярко выраженных, изолированных отклонений, недостатком этих подходов остается неспособность учитывать долгосрочные временные зависимости. Как показано в работах [13, 14], классические методы анализируют события либо разрозненно, либо в рамках короткого скользящего окна, что уменьшает их эффективность против сложных многошаговых сценариев, разбросанных во времени. У них нет механизма, связанного с запоминанием контекста предшествующих событий. Это чаще всего приводит к высокому уровню ложных срабатываний при попытке оценить последовательность действий пользователя в целом [15].

Это ограничение обусловило переход ко второму направлению: применению методов глубокого

обучения для анализа последовательных данных. Архитектуры глубокого обучения демонстрируют существенное превосходство в задачах выявления сложных нелинейных и долгосрочных зависимостей в потоках логов. В отличие от традиционных методов, нейронные сети способны автоматически извлекать последовательные признаки из сырых данных журналов, выявляя скрытые закономерности.

Перспективным инструментом в рамках этого направления является использование рекуррентных нейронных сетей, в частности, архитектур LSTM. Архитектура LSTM, обладает ячейками состояния и способна избирательно запоминать и передавать временной контекст действий пользователя. Исследования в работах [16, 17] подтверждают, что модели на основе LSTM способны выявлять скрытые паттерны инсайдерских угроз, которые остаются полностью незаметными для методов, оценивающих данные отдельно.

Однако при практическом применении LSTM-моделей к реальным пользовательским логам возникает проблема, связанная с настройкой параметров самой модели. Качество применения LSTM-сети зависит от точного выбора ее гиперпараметров. К ключевым параметрам относятся: количество слоев LSTM, размерность скрытого состояния, длина входной последовательности и коэффициент регуляризации. Как отмечается в современных работах, неоптимальная конфигурация этих гиперпараметров может привести к существенному снижению качества обнаружения. Слишком маленькая длина последовательности не позволит выявить многошаговую атаку, а слишком большая (также как и избыточное количество слоев) приведет к необходимости переобучения сети.

Данная работа включает реализацию архитектуры LSTM для выявления скрытых аномальных последовательностей действий и проведение экспериментального исследования по варьированию ключевых гиперпараметров для достижения максимального показателя обнаружения.

Формализация задачи

Для строгого описания процесса выявления угроз в журналах событий информационной системы необходимо формализовать понятия действия, последовательности действий и скрытой аномальной последовательности, а также определить математический аппарат для оценки качества их обнаружения.

Пусть $A = \{a_1, a_2, \dots, a_m\}$ – конечное множество всех возможных дискретных действий, регистрируемых в информационной системе.

Множество всех возможных действий A естественным образом разбивается на два непересекающихся подмножества: множество заведомо нормальных действий A_{norm} и множество заведомо аномальных (вредоносных) действий A_{anom} . Формально это записывается как:

$$A_{norm} \cap A_{anom} = \emptyset, A_{norm} \cup A_{anom} = A. \quad (1)$$

Активность пользователя за некоторый фиксированный интервал времени представляет собой упорядоченную во времени последовательность действий S длины T . Математически последовательность S определяется как упорядоченный набор элементов из множества A :

$$S = \langle s_1, s_2, \dots, s_T \rangle, \text{ где } s_t \in A, t = \{1, 2, 3, \dots, T\}. \quad (2)$$

В рамках общей последовательности S нас интересует выявление специфических паттернов. Пусть C – это непрерывная подпоследовательность действий длины L ($L \leq T$), извлеченная из S . Формально цепочка C определяется как:

$$C = \langle s_j, s_{j+1}, \dots, s_{j+L-1} \rangle, 1 \leq j \leq (T - L + 1). \quad (3)$$

Обозначим через Ω_L множество всех возможных цепочек длины L , которые можно составить из множества A (то есть $\Omega_L \subset A_L$). Внутри этого множества выделим подмножество $\Omega_{anom}^L \subset \Omega_L$, содержащее цепочки, представляющие собой известные шаблоны вредоносного поведения. Цепочка C классифицируется как скрытая аномальная последовательность (рис. 1). Формально это записывается как:

$$(\forall s \in C: s \in A_{norm}) \wedge (C \in \Omega_{anom}^L). \quad (4)$$

В результате модель идентифицирует данную совокупность как скрытую аномальную последовательность, свидетельствующую о потенциально вредоносной активности. Это служит основанием для формирования предупреждения службы безопасности.

Для количественной оценки эффективности алгоритма используется стандартный набор метрик, основанный на матрице ошибок. Матрица ошибок формируется путем сопоставления предсказанных алгоритмом меток с истинными метками цепочек и включает четыре базовые величины: истинно положительные срабатывания (TP), когда скрытая аномальная цепочка обнаружена верно. Истинно отрицательные срабатывания (TN), когда нормальная цепочка классифицирована правильно. Ложные срабатывания (FP), когда нормальная цепочка ошибочно признана аномальной. Пропущенные аномалии (FN), когда реальная скрытая аномальная цепочка не была выявлена.

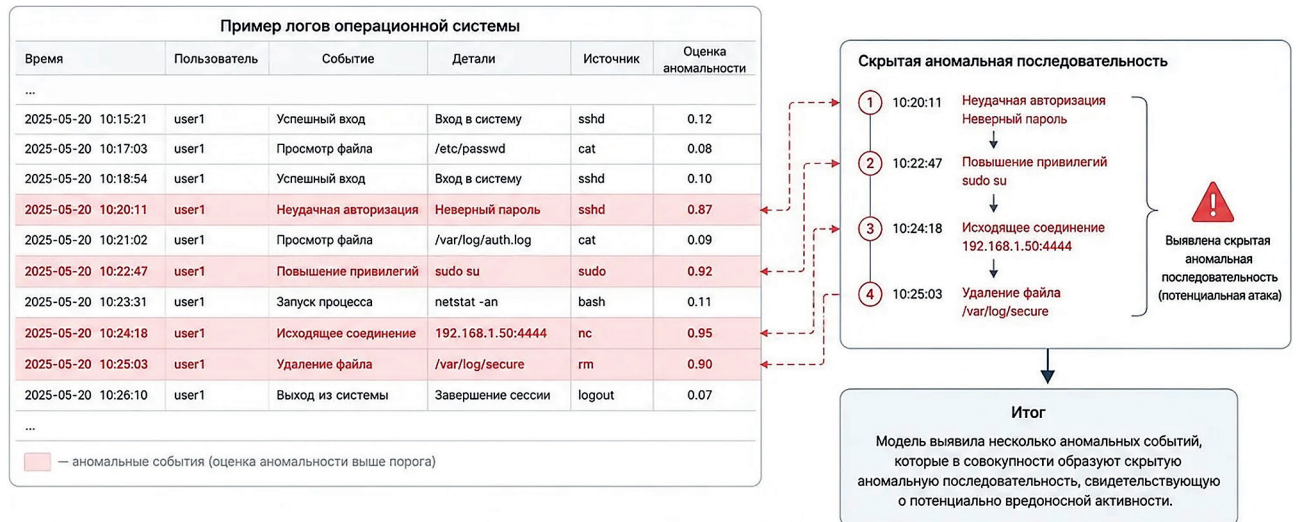


Рис. 1. Скрытая аномальная последовательность

На основе этих величин рассчитываются основные показатели качества классификации. Точность определяет долю цепочек, классифицированных как аномальные, которые действительно являются таковыми, и вычисляется по формуле:

$$Precision = TP / (TP + FP). \quad (5)$$

Полнота (отражает долю реально аномальных цепочек, успешно выявленных алгоритмом:

$$Recall = TP / (TP + FN). \quad (6)$$

Для получения общей оценки используется F -мера, представляющая собой гармоническое среднее точности и полноты:

$$F_1 = 2 \cdot RP / (P + R). \quad (7)$$

В качестве основной целевой метрики для оценки качества обнаружения выбирается F -мера (F_1). Она отражает способность алгоритма выявлять скрытые цепочки действий, максимизируя полноту их обнаружения при допустимом уровне ложных срабатываний.

Генерация набора данных и реализация рекуррентной нейронной сети

Поскольку открытые наборы данных с размеченными скрытыми инсайдерскими атаками отсутствуют, в рамках исследования был разработан и реализован алгоритм генерации специализированного синтетического датасета. Математическая формализация пользовательского поведения задается кортежем $\Pi_u = \langle E_u, P_u, T_u, V_u, R_u \rangle$, где E_u представляет собой множество типов событий, характерных для пользователя; P_u – матрицу вероятностей переходов между событиями; T_u – множество распределений временных

интервалов; V_u – множество параметров вариативности; а R_u – множество ресурсных ограничений. Для обеспечения репрезентативности модель поведения была разделена на несколько функциональных профилей, охватывающих весь спектр субъектов сети. Для каждого профиля на основе экспертного анализа сформированы базовые параметры кортежа Π_u .

Базовой единицей анализа выступает событие – одно действие пользователя, зафиксированное в логе. Признаковое пространство каждого события включает временную метку, должность пользователя, тип действия, объект взаимодействия, длительность действия, результат выполнения, код ошибки, идентификатор сессии и количество ошибок в сессии. Процесс генерации и векторизации данных включает несколько последовательных этапов. Сначала рассматривается множество пользователей, и на основе их профилей генерируется поток событий аудита путем случайного блуждания по графу переходов, заданному матрицей P_u , с учетом распределений временных интервалов T_u и ограничений R_u . Затем выбирается шаг дискретизации $\Delta t > 0$, и временная ось разбивается на равные интервалы $t_k = k\Delta t$, где $k = 0, 1, 2, \dots$. На каждом интервале $[t_k, t_k + \Delta t]$ подсчитываются характеристики активности пользователя, и формально вводится отображение F , ставящее в соответствие набору событий за k -й интервал вектор признаков $x_k(t_k) = [x_{k,1}(t_k), x_{k,2}(t_k), \dots, x_{k,D}(t_k)]^T$, где D – размерность признакового пространства. После векторизации получается обучающая выборка в виде размеченного временного ряда для каждого пользователя, а итоговый датасет формируется как объединение выборок всех пользователей.

Итоговый синтетический датасет был сформирован и разделен на три непересекающихся подмножества: обучающую выборку (70 %), валидационную выборку (15 %) и тестовую выборку (15 %), объективную оценку качества модели.

Для решения задачи классификации последовательностей была реализована архитектура рекуррентной нейронной сети с механизмом долговременной краткосрочной памяти. Входной слой сети принимает матрицу признаков размерности $T \times D$, где T – длина последовательности, а D – размерность признакового пространства. За входным слоем следуют скрытые LSTM-слои, извлекающие долгосрочные временные зависимости и характеризующиеся размерностью скрытого состояния U . Для предотвращения переобучения применяется механизм регуляризации Dropout. Итоговое скрытое состояние подается на выходной слой, вычисляющий вероятность принадлежности последовательности к классу скрытых аномалий.

Ключевым этапом исследования являлось подбор гиперпараметров сети для достижения максимальной F -меры. Пространство поиска включало количество LSTM-слоев L , размерность скрытого состояния U , коэффициент Dropout и длину входной последовательности T . Нахождение оптимальной конфигурации осуществлялось методом случайного поиска на валидационной выборке. Для каждой комбинации гиперпараметров модель обучалась до отсутствия улучшения функции потерь на валидационной выборке. Конфигурация гиперпараметров, обеспечившая наивысшее значение F_1 -меры на этапе валидации, фиксировалась как оптимальная. Финальная оценка достоверности модели проводилась исключительно на тестовой выборке. Это гарантирует объективно судить о способности LSTM-сети выявлять скрытые аномальные последовательности на ранее неизвестных данных.

Экспериментальные исследования и анализ результатов

Целью экспериментальных исследований являлась оценка эффективности предложенной LSTM-сети для выявления скрытых аномальных последовательностей действий пользователей, а также определение оптимальной конфигурации гиперпараметров модели.

Первая часть экспериментов была направлена на анализ влияния ключевых гиперпараметров (количества скрытых слоев, размерности скрытого состояния и коэффициента регуляризации) архитектуры LSTM на значение F_1 -меры. Каждая комбинация гиперпараметров модели обучалась на обучающей выборке, а тестировалась на независимой тестовой выборке последовательностей. Результаты экспериментов представлены на рисунке 2.

Наилучший результат F -меры (0,95) был достигнут при конфигурации: Dropout = 0,5, один скрытый слой, 128 нейронов. Данная конфигурация обеспечивает оптимальный баланс между способностью модели выявлять скрытые аномальные последовательности и предотвращением переобучения. Высокое значение коэффициента Dropout, эффективно регулирует конечный показатель. Он отключает половину нейронов в процессе обучения, что особенно важно при работе с нелинейными данными, характерными для задач обнаружения аномалий.

При сравнении архитектур с одним и двумя скрытыми слоями установлено, что увеличение глубины сети не приводит к существенному улучшению качества обнаружения. Анализ влияния количества нейронов показывает, что при увеличении размерности скрытого состояния с 32 до 128 нейронов приводит к росту F -меры в среднем на 15 %. Это свидетельствует о том, что для эффективного выявления сложных временных паттернов требуется достаточная емкость скрытого состояния LSTM-ячейки.

Эффективность конфигураций LSTM по метрике F_1 -мера

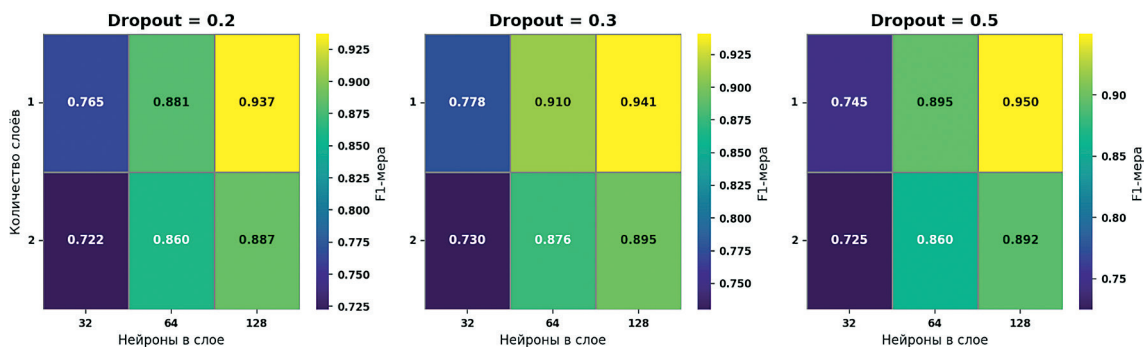


Рис. 2. Эффективность конфигураций LSTM по метрике F -меры

Вторая часть экспериментов была посвящена оценке вычислительной эффективности различных конфигураций LSTM-сети и анализу зависимости времени обучения от параметров архитектуры. На рисунке 3 представлена зависимость времени обучения модели от настройки конфигурации LSTM-модели.

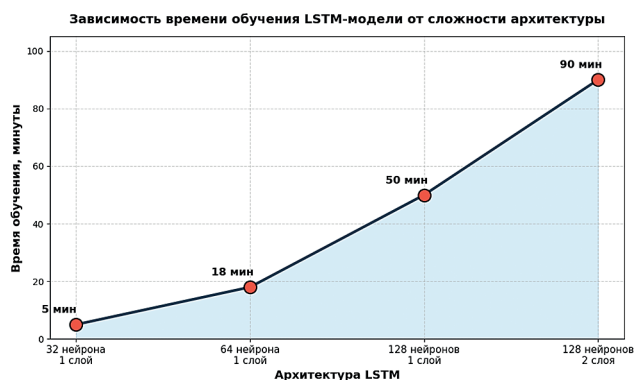


Рис. 3. График зависимости времени обучения от настройки конфигурации LSTM-модели

Анализ полученных результатов показывает, что время обучения зависит от архитектур различной сложности. Легкая конфигурация (32 нейрона, один слой) демонстрирует наилучшую вычислительную эффективность. Время обучения для такой конфигурации составило 5 минут. Для средней конфигурации (64 нейрона, один слой) время обучения составило 18 минут обучения. Тяжелая конфигурация (128 нейронов, один слой), обеспечивающая наилучшее качество обнаружения, требует уже около 50 минут обучения, что является приемлемым только для систем с ежедневным или еженедельным циклом обновления модели. При конфигурации в 128 нейронов и в два слоя время обучения достигает 90 минут. Таким образом, анализ вычислительной эффективности подтверждает обоснованность выбора оптимальной конфигурации, включающей 128 нейронов, один слой и Dropout = 0,5. Она обеспечивает наивысшее качество обнаружения при умеренных временных затратах на обучение.

Заключение

В статье предложен и экспериментально обоснован метод выявления скрытых аномальных последовательностей действий пользователей в журналах событий информационной системы на основе применения рекуррентных нейронных сетей с механизмом долговременной краткосрочной памяти. Проведено сравнение различных конфигураций архитектуры LSTM, включающих варьирование количества скрытых слоев, размерности скрытого состояния и коэффициента регуляризации Dropout. Сделан вывод о том, что математическая формализация скрытых аномальных последовательностей с методами глубокого обучения обеспечивает значительное повышение качества обнаружения угроз при сохранении допустимого уровня вычислительных затрат.

Основные результаты исследования заключаются в следующем:

- 1) разработана математическая формализация понятия скрытой аномальной последовательности на основе теории множеств, которая позволяет определить условия, при которых каждое отдельное действие является легитимным, однако их упорядоченная совокупность классифицируется как вредоносная;
- 2) предложен метод генерации синтетического датасета логов с функциональными профилями пользователей с внедрением скрытых аномальных последовательностей;
- 3) показана практическая применимость предложенного подхода и сделан вывод о том, что модель может быть обучена на стандартном ноутбуке в течение одного рабочего дня. Это позволяет проводить регулярное переобучение модели без необходимости использования специализированных вычислительных машин.

Направления дальнейших исследований включают расширение признаков пространства за счет контекстной информации о сессиях пользователей и ресурсах системы, а также валидацию метода на реальных логах корпоративных информационных систем.

Литература

1. Бушуев С. Н., Авраменко В. С., Козленко А. В. Оценка защищенности информации от несанкционированного доступа в условиях стохастической неопределенности угроз // Вопросы радиоэлектроники. 2013. – Т. 3. – № 1. – С. 82–95. EDN: OJYHPJ.
2. Козленко А. В., Авраменко В. С., Саенко И. Б., Кий А. В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. – 2012. – № 2 (21). – С. 41–55. – EDN: PCCYEH.
3. Nguyen H. D., Tran K. P., Thomassey S., Hamad M. Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management // International Journal of Information Management. – 2021. – Vol. 57. – Pp. 102282. DOI: 10.1016/j.ijinfomgt.2020.102282.

4. Котенко И. В., Ичетовкин Е. А. Методика защиты систем обнаружения вторжений от состязательных атак на основе шумоподавляющих автокодировщиков // Правовая информатика. – 2025. – Т. 12. – № 1. – С. 17–25. – DOI: 10.24412/1994-1404-2025-1-110-120.
5. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. – 2023. – № 3 (326). – С. 65–72. – DOI: 10.53598/2410-3225-2023-3-326-65-72.
6. Букин А. В., Самонов А. В., Тихонов Э. И. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей // Вопросы кибербезопасности. – 2022. – № 5. – С. 61–73. – DOI: 10.21681/2311-3456-2022-5-61-73.
7. Зуев В. Н. Обнаружение аномалий сетевого трафика методом глубокого обучения // Программные продукты и системы. – 2021. – № 1. – С. 91–97. – DOI: 10.15827/0236-235X.133.091-097.
8. Aziz A., Munir K. Anomaly Detection in Logs Using Deep Learning // IEEE Access. – 2024. – Vol. 12. – Pp. 176129–176145. – DOI: 10.1109/ACCESS.2024.3506332.
9. Gonzales O., Yang K., Huang S. Contextual Sequence-Based User Behavior Anomaly Detection // IEEE Access. – 2025. – Vol. 13. – Pp. 35539–35554. – DOI: 10.1109/ACCESS.2025.3543500.
10. Саенко И. Б., Котенко И. В., Аль-Барри М. Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. – 2022. – № 2 (48). – С. 87–97. – DOI: 10.21681/2311-3456-2022-2-87-97.
11. Карцхия А. А., Макаренко Г. И. Актуальные тренды в развитии искусственного интеллекта // Правовая информатика. – 2025. – № 3. – С. 219–231. – DOI: 10.24412/1994-1404-2025-3-00-24.
12. Ветров И. А., Подтопелный В. В. Особенности использования марковских процессов принятия решений при моделировании атак на системы искусственного интеллекта // Вестник Самарского университета. Естественно-научная серия. – 2024. – Т. 30. – № 4. – С. 147–160. – DOI: 10.18287/2541-7525-2024-30-5-147-160.
13. Kiriachek V. A., Salpagarov S. I. Predictive diagnostics of computer systems logs using natural language processing techniques // Discrete and Continuous Models and Applied Computational Science. – 2025. – Vol. 33. – No. 2. – Pp. 172–183. – DOI: 10.22363/2658-4670-2025-33-2-172-183.
14. Lapina M. A., Podruchny N. V., Rusanov M. A., Babenko M. G. Research of machine learning methods for detecting network attacks // Proceedings of the Institute for System Programming of the RAS. – 2025. – Vol. 37. – No. 4-2. – Pp. 147–174. – DOI: 10.15514/ISPRAS-2025-37(4)-24.
15. Macas M., Wu C., Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities // Computer Networks. – 2022. – Vol. 212. – P. 109032. – DOI: 10.1016/j.comnet.2022.109032.
16. Пашшоев Б., Петрусевиц Д. А. Анализ нейросетевых моделей для прогнозирования временных рядов // Russian Technological Journal. – 2024. – Т. 12. – № 4. – С. 106–116. – DOI: 10.32362/2500-316X-2024-12-4-106-116.
17. Чуб В. С. Использование рекуррентных нейронных сетей для анализа временных рядов и выявления тенденций в данных // Образовательные ресурсы и технологии. – 2024. – №2 (47). – С. 91–102. – DOI: 10.21777/2500-2112-2024-2-91-102.

APPLICATION OF RECURRENT NEURAL NETWORKS TO DETECT HIDDEN ANOMALIES IN EVENT LOGS OF AUTOMATED MILITARY SYSTEMS

Sayenko I. B.⁴, Tsypanyatov V. B.⁵, Sazhina A. V.⁶

Keywords: event logs, logs, machine learning, hidden anomalous sequences, automated military system.

Abstract

Objective: development and experimental substantiation of a method for detecting hidden anomalous sequences of user actions in the event logs of an automated military system (ASV), based on the use of recurrent neural networks with a long-term memory (LSTM) mechanism.

Methods: The LSTM network architecture was used to classify event sequences. Since there are no labeled training datasets in most cases, an algorithm for generating a synthetic dataset was developed to simulate the behavior of users with different functional profiles.

Result: it has been experimentally confirmed that the proposed LSTM model allows us to effectively detect hidden anomalous sequences of user actions, each individual action in which looks legitimate.

Scientific novelty: the author provides mathematical formalization of the concept of «hidden anomalous sequence», which makes it possible to determine the conditions when an ordered set of legitimate actions is classified as malicious.

4 Igor B. Sayenko, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: ibsaen@mail.ru

5 Valery B. Tsypanyatov, Ph.D. of Technical Sciences, Associate Professor, Head of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: zvb097@mail.ru

6 Alexandra V. Sazhina, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E-mail: sashasazhina@yandex.ru

A method for generating a synthetic log dataset that reproduces complex patterns is proposed. It is experimentally substantiated that the adjustment of the hyperparameters of the LSTM model affects the ability to detect multistep anomalies distributed in time.

References

1. Bushuev S. N., Avramenko V. S., Kozlenko A. V. Ocenka zashchishchennosti informacii ot nesankcionirovannogo dostupa v usloviyah stohasticheskoy neopredelennosti ugroz // Voprosy radioelektroniki. – 2013. – V. 3. – No. 1. – Pp. 82–95. – EDN: OJYHPJ.
2. Kozlenko A. V., Avramenko V. S., Saenko I. B., Kij A. V. Metod ocenki urovnya zashchity informacii ot NSD v komp'yuternyh setyah na osnove grafa zashchishchennosti // Trudy SPIIRAN. – 2012. – No. 2 (21). – Pp. 41–55. – EDN: PCCYEH.
3. Nguyen H. D., Tran K. P., Thomassey S., Hamad M. Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management // International Journal of Information Management. – 2021. – Vol. 57. – Pp. 102282. – DOI: 10.1016/j.ijinfomgt.2020.102282.
4. Kotenko I. V., Ichetovkin E. A. Metodika zashchity sistem obnaruzheniya vtorzhenij ot sostyazatel'nyh atak na osnove shumopodavlyayushchih avtokodirovshchikov // Pravovaya informatika. – 2025. – V. 12. – No. 1. – Pp. 17–25. – DOI: 10.24412/1994-1404-2025-1-110-120. EDN: JAJRNO.
5. Kozlova N. Sh., Dovgal' V. A. Analiz primeneniya iskusstvennogo intellekta i mashinnogo obucheniya v kiberbezopasnosti // Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya: Estestvenno-matematicheskie i tehniccheskie nauki. – 2023. – No. 3 (326). – Pp. 65–72. – DOI: 10.53598/2410-3225-2023-3-326-65-72.
6. Bukin A. V., Samonov A. V., Tihonov Eh. I. Obnaruzhenie incidentov informacionnoj bezopasnosti na osnove tehnologii nejronnyh setej // Voprosy kiberbezopasnosti. – 2022. – No. 5. – Pp. 61–73. – DOI: 10.21681/2311-3456-2022-5-61-73.
7. Zuev V. N. Obnaruzhenie anomalij setevogo trafika metodom glubokogo obucheniya // Programmnye produkty i sistemy. – 2021. – No. 1. – Pp. 91–97. – DOI: 10.15827/0236-235X.133.091-097.
8. Aziz A., Munir K. Anomaly Detection in Logs Using Deep Learning // IEEE Access. – 2024. – Vol. 12. – Pp. 176129–176145. – DOI: 10.1109/ACCESS.2024.3506332
9. Gonzales O., Yang K., Huang S. Contextual Sequence-Based User Behavior Anomaly Detection // IEEE Access. – 2025. – Vol. 13. – Pp. 35539–35554. – DOI: 10.1109/ACCESS.2025.3543500.
10. Saenko I. B., Kotenko I. V., Al-Barri M. H. Primenenie iskusstvennyh nejronnyh setej dlya vyyavleniya anomal'nogo povedeniya pol'zovatelej centrov obrabotki dannyh // Voprosy kiberbezopasnosti. – 2022. – No. 2 (48). – Pp. 87–97. – DOI: 10.21681/2311-3456-2022-2-87-97
11. Karchiya A. A., Makarenko G. I. Aktual'nye trendy v razvitii iskusstvennogo intellekta // Pravovaya informatika. – 2025. – No. 3. – Pp. 219–231. – DOI: 10.24412/1994-1404-2025-3-00-24.
12. Vetrov I. A., Podtopel'nyj V. V. Osobennosti ispol'zovaniya markovskih processov prinyatiya reshenij pri modelirovanii atak na sistemy iskusstvennogo intellekta // Vestnik Samarskogo universiteta. Estestvennonauchnayaseriya. – 2024. – V. 30. – No. 4. – Pp. 147–160. – DOI:10.18287/2541-7525-2024-30-5-147-160. – EDN: SLIVCV.
13. Kiriachek V. A., Salpagarov S. I. Predictive diagnostics of computer systems logs using natural language processing techniques // Discrete and Continuous Models and Applied Computational Science. – 2025. – Vol. 33. – No. 2. – Pp. 172–183. – DOI: 10.22363/2658-4670-2025-33-2-172-183.
14. Lapina M. A., Podruchny N. V., Rusanov M. A., Babenko M. G. Research of machine learning methods for detecting network attacks // Proceedings of the Institute for System Programming of the RAS. – 2025. – Vol. 37. – No. 4-2. – Pp. 147–174. – DOI: 10.15514/ISPRAS-2025-37(4)-24.
15. Macas M., Wu C., Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities // Computer Networks. – 2022. – Vol. 212. – P. 109032. – DOI: 10.1016/j.comnet.2022.109032.
16. Pashshoev B., Petrushevich D. A. Analiz nejrosetevykh modelej dlyaprognozirovaniya vremennyh ryadov // Russian Technological Journal. – 2024. – V. 12. – No. 4. – Pp. 106–116. – DOI: 10.32362/2500-316X-2024-12-4-106-116.
17. Chub V. S. Ispol'zovanie rekurrentnyh nejronnyh setej dlya analiza vremennyh ryadov i vyyavleniya tendencij v dannyh // Obrazovatel'nye resursy i tehnologii. – 2024. – No. 2 (47). – Pp. 91–102. – DOI: 10.21777/2500-2112-2024-2-91-102.

