Научная статья
УДК 004.056, 004.5; DOI: 10.61260/2218-130X-2025-4-107-116

МЕТОД ПРОТИВОДЕЙСТВИЯ НЕУМЫШЛЕННОМУ ИНСАЙДИНГУ ПУТЕМ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ИНСТРУКЦИЙ ПО РАБОТЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

✉**Моисеенко Григорий Юрьевич.**
Министерство обороны России, Москва, Россия
✉***mogreq@mail.ru***

Аннотация. Рассмотрена проблема неумышленного инсайдинга, являющегося следствием отклонений пользователя от нормального поведения (то есть девиация) при нахождении в состоянии утомленности, стресса, аффекта, длительного выполнения рутинных задач и пр.; обосновываются соответствующие предпосылки к угрозам информационной безопасности. Используя авторскую аналитическую модель такого поведения, предлагается метод противодействия неумышленному инсайдингу путем повышения устойчивости к девиации поведения пользователя самих инструкций; метод состоит из 12 следующих шагов: формализация инструкции, выделение логики и элементов интерфейса, выбор признаков элементов интерфейса, выделение групп пользователей, определение уровня девиации, построение модели поведения, указание предельных значений для нарушений, решение оптимизационной задачи (для корректировки инструкции), уточнение инструкции, адаптация инструкции, апробация инструкции, корректировка модели. Приводится графическая схема метода с ее разделением на область действия эксперта, систему поддержки принятия решений (единого как средства автоматизации), а также взаимодействие со внешними компонентами (данные, алгоритмы и средства). Обосновывается возможность применения больших языковых моделей для помощи эксперту при выполнении ряда шагов.

Ключевые слова: информационная система, информационная безопасность, неумышленный инсайдер, инструкция, метод противодействия, искусственный интеллект

Для цитирования: Моисеенко Г.Ю. Метод противодействия неумышленному инсайдингу путем повышения устойчивости инструкций по работе в информационной системе // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 4. С. 107–116. DOI: 10.61260/2218-130X-2025-4-107-116.

Scientific article

METHOD FOR COUNTERING UNINTENTIONAL INSIDER ATTACKS BY INCREASING THE RESILIENCE OF INFORMATION SYSTEM OPERATING INSTRUCTIONS

✉**Moiseenko Grigory Y.**
Ministry of Defense of Russia, Moscow, Russia
✉***mogreq@mail.ru***

Abstract. The work is devoted to the problem of unintentional insider, which is a consequence of the user's deviations from normal behavior (deviation) when being in a state of fatigue, stress, affect, prolonged performance of routine tasks, etc.; the relevant prerequisites for threats to information security are substantiated. Using the author's analytical model of such behavior, a method is proposed to counteract unintentional insider by increasing the resistance to user behavior deviation of the instructions themselves. The method consists of 12 following steps: formalization of instructions, isolation of logic and interface elements, selection of features of interface elements, identification of user groups, determination of the level of deviation, building a behavior model, specifying limit values for violations, solving an optimization problem (for correcting instructions), clarifying instructions, adapting instructions, testing instructions, correcting the model.

A graphical diagram of the method is presented with its division into the expert's field of action, a decision support system (unified as automation tools), as well as interaction with external components (data, algorithms, and tools). The possibility of using large language models to help an expert perform a number of steps is substantiated.

Keywords: information system, information security, unintentional insider, instruction, countermeasure method, artificial intelligence

For citation: Moiseenko G.Y. Method for countering unintentional insider attacks by increasing the resilience of information system operating instructions // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 4. P. 107–116. DOI: 10.61260/2218-130X- 2025-4-107-116.

Введение

Безопасность данных организации, обрабатываемых в информационной системе (ИС), зависит от множества факторов, таких, как наличие уязвимостей в программном обеспечении [1, 2], слабость политик безопасности [3], наличие злонамеренных сотрудников [4], небезопасность ее состояний и их переходов [5, 6] и др. Однако отдельным проблемным вопросом являются инциденты, когда к информационным угрозам приводят действия легальных пользователей, которые вследствие определенного состояния (из-за утомленности, стресса, аффекта, рутинности задач и пр.) начинают непреднамеренно отклоняться от инструкций по работе в ИС.

Таким образом, причиной нарушения безопасности информации является девиация поведения сотрудника, а сам он (с точки зрения авторской классификации) считается «неумышленным инсайдером» [7]. Ранее было произведено глубокое изучение данного негативного фактора, в результате чего удалось установить, что девиация поведения пользователя приводит к неверному выбору им элементов интерфейсной формы, вводя тем самым некорректные данные (часть из которых являются конфиденциальными) в непредназначенные для этого поля, в том числе приводя к отклонению логики работы с ИС от изначально корректной и потому считающейся безопасной [8]. Была поставлена задача противодействия неумышленному инсайдеру, основанная на соответствующей аналитической модели его поведения в ИС, для решения которой предлагается повышение устойчивости инструкций к пользовательской поведенческой девиации. Поэтому логичным продолжением исследования должно стать создание соответствующего метода противодействия, описание которого приводится в статье далее.

Аналитическая модель и задача

Прежде чем перейти к описанию предлагаемого метода противодействия неумышленному инсайдингу, автор кратко описывает суть лежащей в его основе аналитической модели (основанной, в частности, на предыдущих исследованиях [9]), формализующей поведение такого пользователя в ИС и предназначенной для вычисления целевой функции оптимизационной задачи по повышению устойчивости инструкции.

Обобщенные этапы выполнения инструкций по работе в ИС типовым пользователем были поделены на семь следующих:

1. Изучение описания шага;
2. Выделение элемента интерфейса и действия;
3. Поиск элемента на форме интерфейса;
4. Активация элемента на форме интерфейса;
5. Применение необходимого действия к элементу;
6. Валидация данных;
7. Ожидание результата действия.

При этом девиация поведения пользователя наибольшее влияние оказывает именно на третий этап, поскольку приводит к неверному выбору элемента интерфейса для ввода данных.

Модель поведения неумышленного инсайдера основывалась на следующих положениях:

– во-первых, инструкция по работе в ИС состоит из последовательности шагов, определяющих признаки элементов для ввода данных пользователем, а также необходимые над ними действия. Соответственно, интерфейс ИС представляет собой совокупность форм и элементов, при этом последовательность отображения (для ввода и вывода) последних определяется одной из логик работы в интерфейсе;

– во-вторых, при выборе элемента интерфейса для ввода данных пользователь производит его поиск на форме согласно описанию из шага интерфейса;

– в-третьих, результатом ввода всех пользовательских данных является продуцирование информационного продукта [10] системы;

– в-четвертых, девиация поведения пользователя приводит к ошибочному сопоставлению признаков элементов интерфейса, указанных в инструкции – эталонного, и соседних на интерфейсе – как результат, для ввода данных может быть выбран некорректный элемент;

– в-пятых, неверный выбор элементов потенциально приводит к классической триаде нарушений информационной безопасности (ИБ), что в конечном итоге может быть причиной более серьезных (и не только информационных) последствий [11];

– в-шестых, нарушения ИБ в рамках модели имеют следующую интерпретацию: целостность – данные введены в поле элемента, предназначенного для других данных; конфиденциальность – усиливает нарушение целостности тем, что конфиденциальные данные введены в поле для неконфиденциальных; доступность – неверный ввод данных дополнительно влияет на логику отображения интерфейсных форм и элементов, потенциально не позволяя завершить работу с ИС по заданной инструкции;

– в-седьмых, неверный выбор элементов обосновывается близостью эталонного с также имеющихся на форме. При этом девиация представляет собой вектор, компоненты которого приводят к увеличению диапазона ошибок по каждому признаку элементов;

– в-восьмых, алгоритм поиска элемента на форме согласно шагу инструкции (подсознательно выполняемый пользователем) основан на переборе всех отображаемых элементов, сравнении близости их признаков и выборе тех, которые находятся в рамках девиации; затем из полученного таким образом списка выбирается один, который не всегда будет соответствовать верному;

– в-девятых, для противодействия девиации предлагается добавление в шаги инструкции уточняющей информации, существенно снижающей девиацию по какому-либо признаку; таким образом производится повышение устойчивости инструкции;

– в-десятых, выявлены негативные последствия от указанного противодействия, заключающиеся в том, что уточнение (путем увеличения объема) инструкции само по себе приводит к усложнению ее восприятия человеком и ошибкам при работе в интерфейсе ИС;

– в-одиннадцатых, сама задача противодействия сводима к оптимизационной по следующим причинам. С одной стороны, для снижения вероятности нарушений ИБ из-за влияния девиации поведения пользователя необходимо увеличение объема инструкции (за счет уточнений). С другой стороны, увеличение инструкции ведет к усложнению ее восприятия и увеличению ошибок пользователя, а, следовательно, и к нарушениям ИБ;

– в-двенадцатых, поскольку решение данной оптимизационной задачи полным перебором скорее всего будет недостижимо, то предлагается использование эвристических алгоритмов – то есть получение если не идеального, то рационального содержания (текста) инструкции; также возможно привлечение классического машинного обучения [12] и иных современных технологий искусственного интеллекта (ИИ);

– в-тринадцатых, отдельным направлением противодействия неумышленному инсайдингу может стать поиск «слабых мест» в инструкции в интересах ее будущей модернизации (а не просто уточнения шагов).

Схема метода противодействия

Исходя из аналитической модели и соответствующей формализованной задачи, можно предложить следующие 12 шагов метода противодействия неумышленному инсайдингу путем повышения устойчивости инструкций по работе в ИС.

Шаг 1. Формализация инструкции.

Человеко-ориентированное описание инструкции переводится в более строгий (формализованный) вид, подходящий для аналитического моделирования – как последовательность шагов, каждый из которых содержит описание признаков интерфейсного элемента, а также действия над ним и другую информацию (например, описание ввода фамилии в поле представимо, как совокупность признаков поля ввода и самого действия над ним). Также для перевода человеко-ориентированного текста в формальное представление на сегодняшний день достаточно хорошо себя зарекомендовали большие языковые модели [13, 14].

Шаг 2. Выделение логики и элементов интерфейса.

Происходит изучение интерфейса ИС (по документации, программному коду, опытным путем) для определения логических последовательностей взаимодействия с его элементами, составляется их набор и схема (например, как граф переходов [15]). Также определяется влияние значений элементов на «переключения» логик (например, учет того, что значение флаговой кнопки на текущей форме приводит к различным элементам на последующей).

Шаг 3. Выбор признаков элементов интерфейса.

Выбираются признаки элементов интерфейса и функции сравнения их близости, что необходимо для учета девиации поведения пользователя (как отклонения в значении признаков элементов формы от эталонного), влияющей на третий этап выполнения инструкций по работе в ИС (например, цвет, синтаксис, семантика [16]).

Шаг 4. Выделение групп пользователей.

Выделяются типовые группы пользователей, работающих по инструкции в данной ИС [17], а также их особенности и шаблоны деятельности (например, операторы, аналитики, группы быстрого реагирования, управляющий состав и др.). Для этого может применяться как экспертный анализ деятельности организации, так и более формальные методы, например, кластерный анализ [18] и т.п.

Шаг 5. Определение уровня девиации.

Для группы пользователей определяются возможные уровни девиации поведения по каждому из выбранных признаков элементов, как значение в диапазоне от 0 (пользователь выбирает эталонный элемент формы) до 1 (может быть выбран любой элемент формы); для этого, в частности, может применяться анкетирование [19]. В качестве примера можно привести высокую степень ошибки в понимании семантики заголовка элемента в условиях большого объема и темпа поступающей оперативной информации.

Шаг 6. Построение модели поведения.

Строится модель поведения неумышленного инсайдера, уточненная собранной информацией (логика интерфейса, элементы, их признаки, группы пользователей, уровни девиации и др.), которая позволяет определять вероятности нарушения конфиденциальности, целостности и доступности информации (например, модель указывает на возможность нарушения целостности ввода данных в поле для фамилии, поскольку на форме также расположено поле для имени, заголовки которых синтаксически и семантически слабо различимы – имеют названия «Ф.» и «И.»).

Шаг 7. Указание предельных значений для нарушений.

Задаются предельно максимальные значения для нарушений ИБ по каждому из ее компонентов, определяемые спецификой предметной области, решаемой в ИС задачей и т.п. (например, задается, что основной угрозой является нарушение конфиденциальности, поскольку целостность частично обеспечивается дополнительными проверками введенных данных, а доступность сохраняется из-за линейности логики работы с ИС).

Шаг 8. Решение оптимизационной задачи.

На базе построенной модели поведения производится решение оптимизационной задачи, в результате которой будут получены рекомендации к уточнению отдельных шагов инструкции, что позволит снизить интегральный показатель вероятности нарушений ИБ с учетом заданных критериев и ограничений (например, потребуется детализировать шаг инструкции в части заголовков полей ввода).

Шаг 9. Уточнение инструкции.

Уточнения, полученные в результате оптимизации, применяются к формальному представлению инструкции, что делает ее более устойчивой к девиации поведения пользователя (например, указание точных заголовков «Ф.» и «И.» вместо интуитивно понятного описания назначения полей, что очевидно снизит ошибки пользователя, связанные с его девиативным поведением; при этом сложность восприятия самой инструкции практически не поменяется.

Шаг 10. Адаптация инструкции.

Поскольку формальное представление инструкции плохо подходит для выполнения пользователем, то ее содержание адаптируется (стилистически, по смыслу, иным образом) к человеко-ориентированному виду – выполняется шаг, противоположный первому (например, в шаге инструкции не просто указываются уточняющие заголовки полей, а добавляется текст, связывающий эти названия с основным содержимым) [20]. Также, как и на Шаге 1, могут применяться возможности ИИ в части работы с естественными языками.

Шаг 11. Апробация инструкции.

Поскольку модель поведения и алгоритм оптимизации «работают» с формализованным представлением инструкции, понятным автомату, а человек эволюционно лучше воспринимает текстовое представление, то возможны искажения содержания инструкции на Шагах 1 и 10 и, как следствие, неточность в решении. Таким образом, требуется проверка полученных результатов на практике – апробация инструкции, путем как непосредственного проведения эксперимента, так и анализа данных от систем мониторинга (логов) при ее выполнении (например, если после внедрения в организацию новой инструкции количество нарушений ИБ снизилось недостаточно, то требуется пересмотр данной инструкции [21]).

Шаг 12. Корректировка модели.

По результатам апробации и в случае, если уточненная инструкция неудовлетворительна, будут внесены корректировки в построенную модель, за которой последует повторное решение оптимизационной задачи – то есть переход на Шаг 8 (например, могут быть введены дополнительные признаки или уточнены уровни девиации, а также смягчены оптимизационные ограничения). В ином случае задача считается решенной, а полученная инструкция – конечная, готовая для непосредственного применения в организации.

Этапы метода противодействия

Исходя из сложности и не всегда строгости предложенных шагов метода противодействия, для его выполнения необходима полноценная организационно-техническая система поддержки принятия решений (СППР). Исходя из этого, схема метода, представленная на рисунке, состоит из трех вертикальных слоев – ручные действия эксперта, автоматические действия самой СППР, а также используемые внешние компоненты (данные, предполагаемые алгоритмы и потенциальные средства); применяются следующие обозначения: прямоугольник с белым фоном – шаг метода, с зеленым – входные, промежуточные и выходные данные, с синим – внешние компоненты, сложные стрелки – последовательность шагов, пунктирные линии – связи с внешними компонентами.

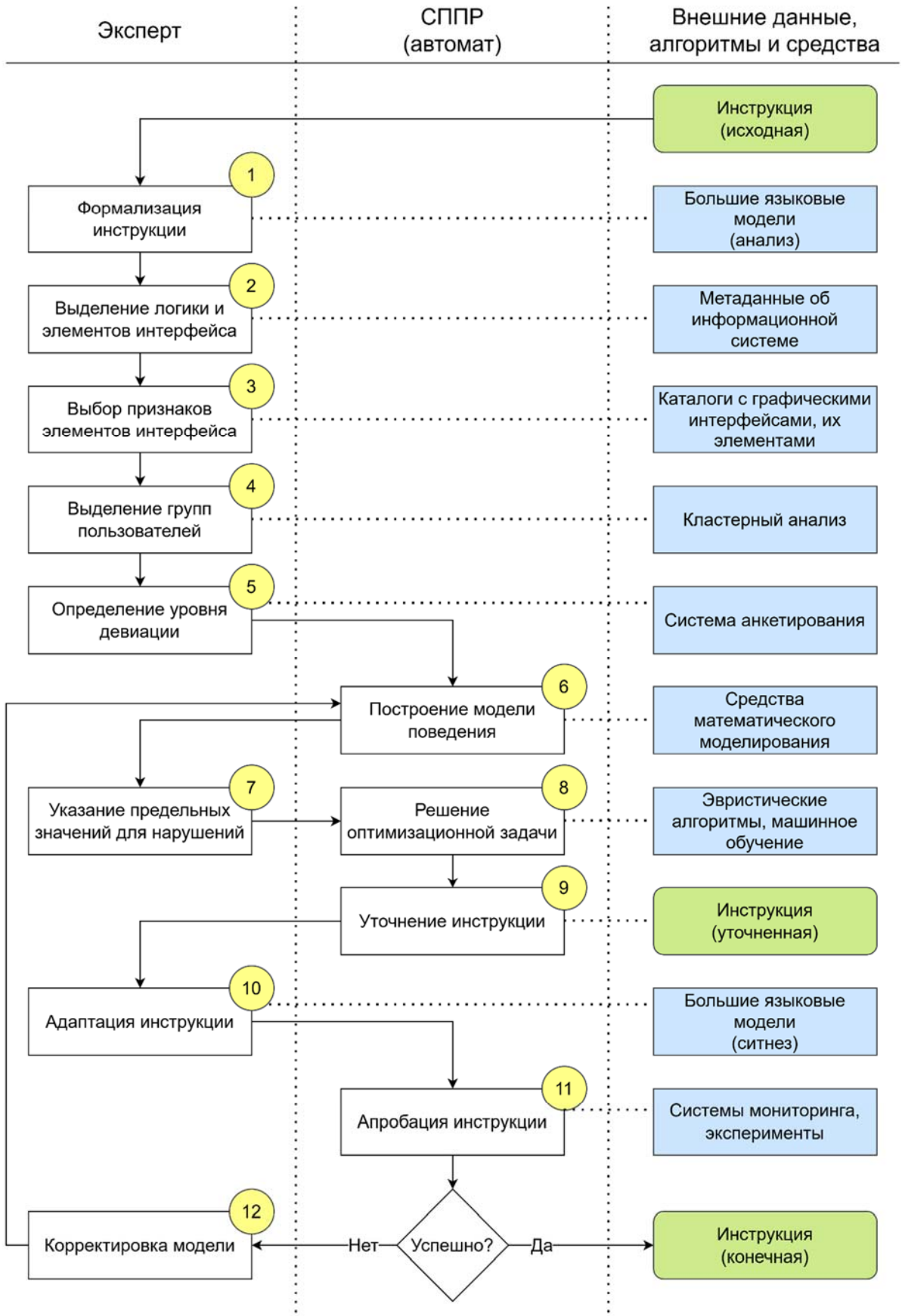

Рис. **Схема метода противодействия неумышленному инсайдингу**

Приведенная на рисунке схема метода полностью соответствует его шагам, описанным выше, и не требует дополнительной интерпретации.

Заключение

Исходя из поставленной задачи противодействия неумышленному инсайдингу, основанному на аналитической модели, предложен соответствующий метод ее решения путем повышения устойчивости самих инструкций к девиации поведения пользователя; обосновано применение ИИ – как для решения оптимизационной задачи, так и для вспомогательных действий. Основным результатом исследования является схема метода, как последовательность шагов, выполняемых экспертом и в СППР, а также использующих внешние данных, предполагаемые алгоритмы и потенциальные средства.

Новизной результата, помимо изучения собственно нового феномена – неумышленного IT-инсайдинга, является доведение противодействия ему до достаточно строгого метода, использующего авторскую формализованную модель поведения пользователя.

Возможность выполнения шагов метода в составе единой СППР как действиями эксперта (левый столбец рисунка), так и с помощью существующих компонентов (правый столбец рисунка), обосновывают его реализуемость, что определяет практическую значимость; алгоритмическая же форма записи метода может быть отнесена к теоретической значимости.

Продолжением исследования должна стать разработка программного прототипа указанной СППР и проведение соответствующих экспериментов. Также, отдельного внимания заслуживает реализация Шагов 1 и 10 с применением ИИ в части больших языковых моделей.

Список источников

1. Леонов Н.В. Методология и элементы технологии моделирования стратегических задач управления уязвимостями в ПО. Часть 1. Концептуальные основы и онтологическая модель // Защита информации. Инсайд. 2025. № 3 (123). С. 17–21.

2. Леонов Н.В. Методология и элементы технологии моделирования стратегических задач управления уязвимостями в ПО. Часть 2. Имитационное моделирование и оценка состояния // Защита информации. Инсайд. 2025. № 4 (124). С. 56–61.

3. Семин Р.В., Новосядлый В.А. Исследование задачи активного аудита парольной политики в компьютерных сетях // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 47–55.

4. Власов Д.С. К вопросу о признаках инсайдерской деятельности // Национальная безопасность и стратегическое планирование. 2024. № 1 (45). С. 35–45. DOI: 10.37468/2307-1400-2024-1-35-45.

5. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3 (55). С. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

6. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4 (56). С. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

7. Буйневич М.В., Моисеенко Г.Ю. Нарушение регламента при работе с информационной системой как угроза безопасности информационным ресурсам // Региональная информатика и информационная безопасность: сб. трудов Санкт-Петербургской междунар. конф. и Санкт-Петербургской межрегион. конф. Санкт-Петербург, 2024. С. 78–79.

8. Моисеенко Г.Ю. Формальная постановка задачи противодействия неумышленному инсайдингу в организации путем корректировки должностных инструкций // Защита информации. Инсайд. 2025. № 6 (126). С. 61–69.

9. Буйневич М.В., Моисеенко Г.Ю. Обзор моделей поведения пользователя информационной системы в интересах противодействия инсайдерской деятельности (по состоянию отечественного научного сегмента) // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2024. № 4. С. 89–102. DOI: 10.61260/2218-130X-2025-2024-4-89-102.

10. Царегородцев А.В., Мухин И.Н., Волков С.Д. Методика оценки уровня цифровой автономии информационного продукта // Современная наука: актуальные проблемы теории и практики. Сер.: Естественные и технические науки. 2024. № 7-2. С. 196–203. DOI: 10.37882/2223-2966.2024.7-2.38.

11. Матвеев А.В., Матвеев В.В. Системно-кибернетический подход к определению понятия «безопасность» // Национальная безопасность и стратегическое планирование. 2015. № 1 (9). С. 18–25.

12. Антропова Е.Г. Решение оптимизационных задач при помощи нейронных сетей // Процессы управления и устойчивость. 2024. Т. 11. № 1. С. 173–178.

13. Резцов С.М. Сравнительный анализ языковых моделей в обработке неструктурированных данных на примере DeepSeek и GigaChat // Парадигма. 2025. № 5-2. С. 200–204.

14. Матвеев А.В., Иванов А.Ю. Использование больших языковых моделей в области безопасности в чрезвычайных ситуациях: обзор исследований и анализ возможностей // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 3. С. 136–146. DOI: 10.61260/2218-130X-2025-3-136-146.

15. Курта П.А., Буйневич М.В. Онтологическая модель взаимодействия пользователя с информационной системой в рамках получения услуги информационного сервиса // Вестник кибернетики. 2021. № 2 (42). С. 17–23. DOI: 10.34822/1999-7604-2021-2-17-23.

16. Буйневич М.В., Вострых А.В. Методы оценки графических пользовательских интерфейсов. Визуальная составляющая. СПб.: Санкт-Петербургский университет ГПС МЧС России, 2024. 340 с.

17. Гапонец Е.Г., Марьин А.И. Проблемы эффективности группового поведения по опыту внутренних войск МВД России // Актуальные проблемы гуманитарных и социально-экономических наук. 2010. Т. 4. № 3. С. 40–44.

18. Будникова И.К., Плетенева Е.В. Кластерный анализ как функция интеллектуального анализа данных // Информационные технологии в строительных, социальных и экономических системах. 2022. № 1 (27). С. 25–28.

19. Максимус Д.А. Анализ данных анкетирования государственных служащих как пользователей свободного программного обеспечения // Новое в экономической кибернетике. 2020. № 3-4. С. 133–147.

20. Гусев А.А. Адаптация инструкций по решению проблем доступа к сети интернет на основе портрета компетенций пользователя // Математическое моделирование и информационные технологии: материалы XV Всерос. (VII междунар.) науч.-техн. конф. студентов, аспирантов и молодых ученых. Иваново, 2020. Т. 5. С. 19.

21. Буйневич М.В., Моисеенко Г.Ю. Нарушение регламента при работе с информационной системой как угроза безопасности информационным ресурсам // Региональная информатика и информационная безопасность: сб. трудов Санкт-Петербургской междунар. конф. и Санкт-Петербургской межрегион. конф. Санкт-Петербург, 2024. С. 78–79.

References

1. Leonov N.V. Metodologiya i elementy tekhnologii modelirovaniya strategicheskikh zadach upravleniya uyazvimostyami v PO. Chastʹ 1. Kontseptualʹnye osnovy i ontologicheskaya modelʹ // Zashchita informatsii. Insajd. 2025. № 3 (123). S. 17–21.

2. Leonov N.V. Metodologiya i elementy tekhnologii modelirovaniya strategicheskikh zadach upravleniya uyazvimostyami v PO. Chastʹ 2. Imitatsionnoe modelirovanie i otsenka sostoyaniya // Zashchita informatsii. Insajd. 2025. № 4 (124). S. 56–61.

3. Semin R.V., Novosyadlyj V.A. Issledovanie zadachi aktivnogo audita parolʹnoj politiki v kompʹyuternykh setyakh // Izvestiya YuFU. Tekhnicheskie nauki. 2015. № 5 (166). S. 47–55.

4. Vlasov D.S. K voprosu o priznakakh insajderskoj deyatelʹnosti // Natsionalʹnaya bezopasnostʹ i strategicheskoe planirovanie. 2024. № 1 (45). S. 35–45. DOI: 10.37468/2307-1400-2024-1-35-45.

5. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob″ekty na osnove informatsii sostoyaniya. Chast′ 1. Predposylki i skhema // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 90–100. DOI: 10.21681/2311-3456-2023-3-90-100.

6. Izrailov K.E., Bujnevich M.V. Metod obnaruzheniya atak razlichnogo geneza na slozhnye ob″ekty na osnove informatsii sostoyaniya. Chast′ 2. Algoritm, model′ i eksperiment // Voprosy kiberbezopasnosti. 2023. № 4 (56). S. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93.

7. Bujnevich M.V., Moiseenko G.Yu. Narushenie reglamenta pri rabote s informatsionnoj sistemoj kak ugroza bezopasnosti informatsionnym resursam // Regional′naya informatika i informatsionnaya bezopasnost′: sb. trudov Sankt-Peterburgskoj mezhdunar. konf. i Sankt-Peterburgskoj mezhregion. konf. Sankt-Peterburg, 2024. S. 78–79.

8. Moiseenko G.Yu. Formal′naya postanovka zadachi protivodejstviya neumyshlennomu insajdingu v organizatsii putem korrektirovki dolzhnostnykh instruktsij // Zashchita informatsii. Insajd. 2025. № 6 (126). S. 61–69.

9. Bujnevich M.V., Moiseenko G.Yu. Obzor modelej povedeniya pol′zovatelya informatsionnoj sistemy v interesakh protivodejstviya insajderskoj deyatel′nosti (po sostoyaniyu otechestvennogo nauchnogo segmenta) // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii». 2024. № 4. S. 89–102. DOI: 10.61260/2218-130X-2025-2024-4-89-102.

10. Tsaregorodtsev A.V., Mukhin I.N., Volkov S.D. Metodika otsenki urovnya tsifrovoj avtonomii informatsionnogo produkta // Sovremennaya nauka: aktual′nye problemy teorii i praktiki. Ser.: Estestvennye i tekhnicheskie nauki. 2024. № 7-2. S. 196–203. DOI: 10.37882/2223-2966.2024.7-2.38.

11. Matveev A.V., Matveev V.V. Sistemno-kiberneticheskij podkhod k opredeleniyu ponyatiya «bezopasnost′» // Natsional′naya bezopasnost′ i strategicheskoe planirovanie. 2015. № 1 (9). S. 18–25.

12. Antropova E.G. Reshenie optimizatsionnykh zadach pri pomoshchi nejronnykh setej // Protsessy upravleniya i ustojchivost′. 2024. T. 11. № 1. S. 173–178.

13. Reztsov S.M. Sravnitel′nyj analiz yazykovykh modelej v obrabotke nestrukturirovannykh dannykh na primere DeepSeek i GigaChat // Paradigma. 2025. № 5-2. S. 200–204.

14. Matveev A.V., Ivanov A.Yu. Ispol′zovanie bol′shikh yazykovykh modelej v oblasti bezopasnosti v chrezvychajnykh situatsiyakh: obzor issledovanij i analiz vozmozhnostej // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MChS Rossii». 2025. № 3. S. 136–146. DOI: 10.61260/2218-130X-2025-3-136-146.

15. Kurta P.A., Bujnevich M.V. Ontologicheskaya model′ vzaimodejstviya pol′zovatelya s informatsionnoj sistemoj v ramkakh polucheniya uslugi informatsionnogo servisa // Vestnik kibernetiki. 2021. № 2 (42). S. 17–23. DOI: 10.34822/1999-7604-2021-2-17-23.

16. Bujnevich M.V., Vostrykh A.V. Metody otsenki graficheskikh pol′zovatel′skikh interfejsov. Vizual′naya sostavlyayushchaya. SPb.: Sankt-Peterburgskij universitet GPS MCHS Rossii, 2024. 340 s.

17. Gaponets E.G., Mar′in A.I. Problemy effektivnosti gruppovogo povedeniya po opytu vnutrennikh vojsk MVD Rossii // Aktual′nye problemy gumanitarnykh i sotsial′no-ekonomicheskikh nauk. 2010. T. 4. № 3. S. 40–44.

18. Budnikova I.K., Pleteneva E.V. Klasternyj analiz kak funktsiya intellektual′nogo analiza dannykh // Informatsionnye tekhnologii v stroitel′nykh, sotsial′nykh i ekonomicheskikh sistemakh. 2022. № 1 (27). S. 25–28.

19. Maksimus D.A. Analiz dannykh anketirovaniya gosudarstvennykh sluzhashchikh kak pol′zovatelej svobodnogo programmnogo obespecheniya // Novoe v ekonomicheskoj kibernetike. 2020. № 3-4. S. 133–147.

20. Gusev A.A. Adaptatsiya instruktsij po resheniyu problem dostupa k seti internet na osnove portreta kompetentsij pol′zovatelya // Matematicheskoe modelirovanie i informatsionnye tekhnologii: materialy XV Vseros. (VII mezhdunar.) nauch.-tekhn. konf. studentov, aspirantov i molodykh uchenykh. Ivanovo, 2020. T. 5. S. 19.

21. Bujnevich M.V., Moiseenko G.Yu. Narushenie reglamenta pri rabote s informatsionnoj sistemoj kak ugroza bezopasnosti informatsionnym resursam // Regional′naya informatika i informatsionnaya bezopasnost′: sb. trudov Sankt-Peterburgskoj mezhdunar. konf. i Sankt-Peterburgskoj mezhregion. konf. Sankt-Peterburg, 2024. S. 78–79.

Информация о статье:
Статья поступила в редакцию: 12.11.2025; одобрена после рецензирования: 10.12.2025;
принята к публикации: 15.12.2025

Information about the article:
The article was submitted to the editorial office: 12.11.2025; approved after review: 10.12.2025;
accepted for publication: 15.12.2025

Информация об авторах:
Моисеенко Григорий Юрьевич, руководитель направления Министерства обороны России (119160, Москва, ул Знаменка, д. 19), e-mail: mogreq@mail.ru

Information about authors:
Moiseenko Grigory Y., head of direction of Ministry of Defense of Russia (119160, Moscow, Znamenka st., 19), e-mail: e-mail: mogreq@mail.ru