ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Научная статья

УДК 004.056
DOI 10.37468/2307-1400-2026-2-18-25

Базовый эксперимент по корректировке регламентов работы в автоматизированной системе в интересах противодействия неумышленному IT-инсайдингу

Моисеенко Григорий Юрьевич [1]
Израилов Константин Евгеньевич [2]

[1] *Министерство обороны РФ, Москва, Россия*

[2] *Санкт-Петербургский университет Государственной противопожарной службы МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева, Санкт-Петербург, Россия*

Аннотация
Работа посвящена противодействию неумышленному IT-инсайдингу, под которым понимаются действия операторов автоматизированных систем, нарушающих должностные регламенты деятельности вследствие девиации своего поведения. Данная задача сведена к оптимизационной, для решения которой ранее были предложены авторские аналитическая модель и метод гибридного решения оптимизационной задачи. Для их практического применения разработано соответствующее программное средство, логика работы и функциональные возможности которого приводятся в тексте настоящей статьи. Предлагаются следующие 10 профилей пользователей, отражающих факторы и характеристики девиации их поведения: с нарушением цветовосприятия, с трудностями чтения, сильно уставший, опытный, со слабым зрением, с нарушением рабочей памяти, без девиации, в состоянии стресса, в условиях дефицита времени и обычный пользователь. Проводится базовый эксперимент по повышению устойчивости регламента работы оператора с интерфейсом авторизации, который доказывает работоспособность всех полученных научно-практических результатов.

Ключевые слова: автоматизированная система, информационная безопасность, оператор, профиль пользователя, регламент деятельности, девиация поведения, программный прототип, эксперимент.

Введение

Высокая ценность информационных ресурсов современного IT-мира является стимулирующим фактором для усиления кибератак на организации любого масштаба и рода деятельности [1]. Часть таких атак может проводиться непосредственно самими сотрудниками изнутри организации [2], при этом не обладающими злым умыслом и совершающими небезопасные действия вследствие субъективных факторов, таких как стресс, вызванный временны́м цейтнотом, когнитивным диссонансом и пр. Следствием аномального поведения является то, что оператор отклоняется от строгого следования должностному регламенту деятельности в автоматизированной системе (далее – АС), что приводит к соответствующим нарушениям информационной безопасности (далее – ИБ) [3]. Так, например, невнимательность при вводе логина и пароля может привести к отображению конфиденциальной информации, как на общедоступном экране системы, так и в ее логах. Для обозначения такого непред-

намеренного поведения авторами введено собственное понятие – *неумышленный IT-инсайдинг*, детально рассмотренное в предшествующих публикациях [4]. Необходимо отметить, что в качестве инициатора атаки все также может выступать классический нарушитель, находящийся вне периметра и влияющий непосредственно на легального сотрудника, например, путем усиления информационного стресса последнего для повышения вероятности совершения им фатальных ошибок.

В качестве пути противодействия неумышленному IT-инсайдингу авторы в первую очередь видят корректировку самих регламентов деятельности таким образом, чтобы не допустить или значительно воспрепятствовать выполнению сотрудником ошибочных действий вследствие девиации поведения. Для этого предлагается добавление в текст шагов регламента уточнений касательно элементов интерфейса АС, снижающих ошибки их выбора оператором. Однако у такого механизма есть и обратный эффект, поскольку усложнение регламента затрудняет его восприятие, то это приводит к когнитивной нагрузке на оператора и еще большему усилению девиации его поведения. Таким образом, задача может быть сведена к оптимизационной, в которой параметрами являются уточнения шагов регламента, а критериями – снижение вероятностей угроз ИБ при одновременном ограничении сложности регламента. Для практического решения данной задачи, позволяющей повысить устойчивость регламентов деятельсности к девиации поведения сотрудника, реализован прототип соответствующего программного средства (далее – Прототип), описание и базовый эксперимент с которым приводятся далее.

Реализация прототипа

Прототип был реализован на современном языке программирования Python 3.13, подходящем для моделирования, решения оптимизационных задач, а также теоретических и экспериментальных исследований. Основным назначением Прототипа является осуществление корректировок регламентов работы с интерфейсом АС, заданных в формальном виде, и решение тем самым указанной ранее оптимизационной задачи.

Архитектурная часть Прототипа состоит из набора задачно-ориентированных модулей, опубликованных в авторской публикации [5]. Исходные данные Прототипа, передаваемые в формате JSON, описывают интерфейс АС, регламент деятельности, параметры решения и профили девиации операторов (возможные отклонения при выборе интерфейсного элемента по каждому из его свойств, таких как заголовок, цвет, размер и т. д.) [6].

Прототип осуществляет моделирование выполнения регламентов работы с интерфейсом АС, что является основой для вычисления целевой функции решаемой оптимизационной задачи [7]. Вероятности нарушений КЦД (принятая аббревиатура для К – конфиденциальности, Ц – целостности и Д – доступности) вычисляются по соответствующей модели путем оценки близости признаков графических элементов, заданных на шаге регламента и отображаемых в интерфейсе АС. Учет такой близости позволяет определить вероятность неверного выбора элемента оператором для конкретных значений девиации, также задаваемых по каждому из признаков. Например, в состоянии стресса и при последующей частичной потере цветового различения элементов, указание данного признака в шаге регламента повысит точность совершения корректных действий оператором лишь частично, в особенности если элементы графической формы будут иметь близкие цвета. Т. е. в этом случае по признаку цвета два элемента окажутся близкими, а вероятность неверного выбора – высокой.

Прототип поддерживает поиск расстояния между следующими признаками графических элементов: отображаемое имя (title), функциональное назначение (name), тип (type), позиция (position), цвет (color), размер (size) и порядок (order). Для ограничения времени работы алгоритма полного перебора при решении оптимизационной задачи (которое для большого количества переменных могло стать существенным) в Прототипе есть возможность задания предельно допустимого количества перебираемых параметров.

Логика работы Прототипа состоит из определения возможных для выбора оператором элементов, оценки нарушений КЦД, выявления небезопасных шагов, формирования возможных вариантов корректировки регламента, вычисления целевой функции и осуществления оптимизации (полным перебором и двумя эвристическими алгоритмами – генетическим и «имитацией отжига») [8–10]. Все промежуточные и получаемые результаты также сохраняются в формате JSON.

Прототип представляет собой консольную программу (т. е. без графического окна), что на данном этапе исследования и разработки является оправданным. Основными аргументами Прототипа являются следующие:

1) scenario – указание каталога сценария с входными данными (в JSON-формате);
2) method – выбор метода оптимизации: «bruteforce» – полный перебор (аббр. ПП), «genetic» – генетический алгоритм (аббр. ГА), «simulated_annealing» – имитация отжига (аббр. ИО);
3) output-dir – указание каталога для получаемых результатов;
4) log-dir – указание каталога для логирования работы Прототипа;
5) seed – ввод начального значения генератора случайных чисел (для воспроизводимости результатов).
6) user-file – указание пути к файлу пользовательского профиля.
7) quiet – перевод Прототипа в режим «тихой» работы (без детализации результатов работы в консоли).

В работе Прототипа присутствует ряд ограничений и допущений, таких как независимость расчета расстояния для каждого признака, взвешенное суммирование вероятностей угроз ИБ, оценка усложнения скорректированного регламента лишь по внесенным уточнениям и др., что, впрочем, не ограничивает его применение для корректировки реальных регламентов деятельности.

Профили девиации

Поскольку на угрозы КЦД в рамках решаемой оптимизационной задачи существенное влияние оказывает не только интерфейс АС и регламент деятельности в ней, но и характеристики самого оператора (например, уровень его стресса), то были введены следующие 10 качественно разных профилей, отражающих факторы и особенности его состояния (девиации). Профили встроены в Прототип, хотя имеется возможность их расширения новыми.

Каждый профиль определяет допустимые пороги различий между одним из признаков (title, name, type, position, color, size, order) для эталонного и заданного в шаге регламента элементов. Так, например, значение порога в 1.0 может быть проинтерпретировано как «признак элемента не позволяет пользователю различить элементы», а 0.0 как «пользователь различает элементы по данному признаку без отклонений». Т. е. если для признака «цвет» (color) в профиле пользователя указано значение 1.0, то пользователь с одинаковой вероятностью выберет кнопку любого цвета. Данная ситуация характерна в случае предельного нарушения у оператора цветовосприятия [11].

Описание всех введенных профилей пользователей и значения девиации поведения по каждому из признаков элементов приводится далее.

Профиль 1. Пользователь с нарушением цветовосприятия – практически не использует цвет для различения элементов интерфейса (девиация `"title = 0.25, name = 0.25, type = 0.08, position = 0.35, color = 1.00, size = 0.20, order = 0.25"`); обладает максимальной девиацией поведения по цвету (1.00);

Профиль 2. Пользователь с трудностями чтения – плохо различает элементы по текстовым названиям и их функциональному назначению (девиация `"title = 0.95, name = 0.90, type = 0.10, position = 0.35, color = 0.20, size = 0.20, order = 0.30"`); обладает очень высокой девиацией поведения по отображаемому имени (0.95) и функциональному назначению (0.90);

Профиль 3. Сильно уставший пользователь – характеризуется общим снижением внимания к различиям элементов интерфейса (девиация "title = 1.00, name = 1.00, type = 0.30, position = 0.90, color = 1.00, size = 0.60, order = 0.85"); обладает высокой девиацией поведения практически по всем признакам, а именно максимальными значениями для имени, назначения и цвета (1.00), и высокими для положения (0.90) и порядка (0.85);

Профиль 4. Опытный оператор системы – хорошо знает интерфейс и устойчиво различает его элементы по большинству признаков (девиация "title = 0.05, name = 0.05, type = 0.02, position = 0.10, color = 0.05, size = 0.05, order = 0.08"); обладает очень низкими значениями девиации поведения по всем признакам и является наиболее устойчивым пользователем, отличающимся от «идеального» лишь небольшими отклонениями;

Профиль 5. Пользователь со слабым зрением – испытывает трудности при различении текстовых и визуально-геометрических признаков элементов (девиация "title = 0.85, name = 0.60, type = 0.20, position = 0.80, color = 1.00, size = 0.70, order = 0.75"); обладает максимальной девиацией по цвету (1.00), а также высокой по названию (0.85), положению (0.80), порядку (0.75) и размеру (0.70);

Профиль 6. Пользователь с нарушением рабочей памяти – хорошо различает элементы при восприятии, однако плохо запоминает их положение и порядок (девиация "title = 0.20, name = 0.30, type = 0.10, position = 0.75, color = 0.25, size = 0.25, order = 0.90"); обладает высокой девиацией поведения по порядку (0.90) и чуть меньшей по положению (0.75);

Профиль 7. Пользователь без девиации (эталонный, абсолютно устойчивый оператор) – идеально различает элементы интерфейса (девиация "title = 0.0, name = 0.0, type = 0.0, position = 0.0, color = 0.0, size = 0.0, order = 0.0"); обладает нулевыми значениями девиации поведения по всем признакам, то есть способен всегда корректно выбирать элементы интерфейса;

Профиль 8. Пользователь в состоянии сильного стресса неуточненной природы (по типу «панической атаки») – из-за стресса значительно хуже различает все сходные элементы (девиация "title = 0.95, name = 0.95, type = 0.45, position = 0.95, color = 0.85, size = 0.75, order = 0.95"); обладает высокой девиацией поведения по названию, назначению, положению и порядку (0.95), а также чуть меньшими по цвету (0.85) и размеру (0.75);

Профиль 9. Пользователь в условиях дефицита времени – работает в условиях временно́го цейтнота и чаще игнорирует ряд признаков (девиация "title = 0.85, name = 0.85, type = 0.25, position = 0.85, color = 0.70, size = 0.55, order = 0.90"); обладает высокой девиацией поведения по порядку (0.90) и близкими к этому по названию, назначению и положению (0.85);

Профиль 10. Обычный пользователь – типовой пользователь с умеренной невнимательностью без выраженных нарушений (девиация "title = 0.35, name = 0.35, type = 0.10, position = 0.40, color = 0.20, size = 0.20, order = 0.30"); обладает сбалансированными значениями девиации поведения, среди которых наибольшее относится к положению (0.40), а наименьшее – к типу элемента (0.10).

Эксперимент

Для обоснования работоспособности Прототипа и оценки устойчивости получаемых с его помощью регламентов деятельности была проведена серия экспериментов по следующим 7 сценариям: простой интерфейс авторизации, регистрация обращения, согласование счета, выдача доступа, реагирование на инциденты ИБ, пересмотр прав доступа и переключение сервисов.

В качестве примера приведем лишь 1-й сценарий из перечисленных. Сценарий описывает работу оператора АС с интерфейсом авторизации, состоящим из следующих 3 графических элементов: 2 полей для ввода логина и пароля, а также кнопки входа.

Регламент по работе с АС состоит из трех шагов.

```
Регламент «Авторизация сотрудника»:
Шаг 1. На форме «Корпоративный вход» введите «employee@example.local» в текстовое поле.
Шаг 2. На форме «Корпоративный вход» введите «<секретный пароль>» в текстовое поле.
Шаг 3. На форме «Корпоративный вход» нажмите кнопку.
```

Особенностью сценария с позиции возможных нарушений ИБ из-за девиации поведения оператора является то, что в регламенте используется только тип элементов, что потенциально приводит к путанице полей при их выборе; например, ввод пароля в поле для логина. При этом наиболее критичным с точки зрения ИБ здесь считается нарушение конфиденциальности, за которым следуют нарушения доступности и целостности (это влияет на веса компонентов целевой фуекции.

В качестве профиля девиации был выбран 3-й, характеризующий сильно уставшего оператора.

Результаты эксперимента по решению оптимизационной задачи с помощью Прототипа для всех трех алгоритмов (ПП, ГА и ИО) приведены в таблице 1, имеющей следующую интерпретацию столбцов (по названиям): «Алг.» – алгоритм решения оптимизационной задачи, «КЦД до/после опт.» – значения нарушений конфиденциальности, целостности и доступности до и после решения оптимизационной задачи (в формате «[КЦД до] → [КЦД после]»), «Сложность до/после опт.» – сложность регламента до и после решения оптимизационной задачи (в формате «[Сложность до] → [Сложность после]»), «Время (сек.)» – время работы Прототипа в секундах, «Уточн.» – количество уточнений, внесенных в регламент, «Полн.» – факт исследования алгоритмом всех доступных переменных для уточнения («Да») или их ограниченного множества («Нет»).

Таблица 1 – Результаты эксперимента по корректировке регламентов деятельности (для сценария 1)

Алг.	КЦД до/после опт.	Сложность до/после опт.	Время (сек.)	Уточн.	Полн.
ПП	[К = 0.50; Ц = 0.75; Д = 0.00] → [К = 0.00; Ц = 0.00; Д = 0.00]	1.0500 → 1.2500	0.0539	2	Да
ГА	[К = 0.50; Ц = 0.75; Д = 0.00] → [К = 0.00; Ц = 0.00; Д = 0.00]	1.0500 → 1.2500	0.0587	2	Да
ИО	[К = 0.50; Ц = 0.75; Д = 0.00] → [К = 0.00; Ц = 0.00; Д = 0.00]	1.0500 → 1.2500	0.0567	2	Да

Итоговый регламент, полученный применением Прототипа и устойчивый к девиации сильно уставшего оператора, является следующим (изменения в тексте регламента подчеркнуты):

```
Регламент «Авторизация сотрудника»:
Шаг 1. На форме «Корпоративный вход» введите «employee@example.local» в текстовое поле с номером 1 в порядке элементов формы.
Шаг 2. На форме «Корпоративный вход» введите «<секретный пароль>» в текстовое поле с номером 2 в порядке элементов формы.
Шаг 3. На форме «Корпоративный вход» нажмите кнопку.
```

Таким образом, решение оптимизационной задачи было достигнуто добавлением корректировок регламента в части порядковых номеров элементов для ввода логина и пароля.

Исходя из проведенного эксперимента (см. таблицу), можно сделать следующие выводы.

Во-первых, эксперимент для 1-го сценария подтвердил базовую работоспособность Прототипа интеллектуальной корректировки, поскольку с помощью всех алгоритмов (ПП, ГА и ИО) удалось достичь нулевых показателей нарушения конфиденциальности, целостности и доступности.

Во-вторых, повышение устойчивости регламента удалось достичь умеренным повышением его сложности (после корректировок) – в среднем на 20%.

И в-третьих, несмотря на простоту выбранного сценария, эвристические алгоритмы (т. е. 2-й и 3-й) [12] получили такое же решение, как и полный перебор; при этом за малое время (менее десятой секунды).

Таким образом, проведенный эксперимент доказывает, что разработанные аналитическая модель, метод решения оптимизационной задачи и программный Прототип позволяют повысить устойчивость работы оператора в АС за счет корректировки регламента его деятельности, снизив тем самым расчетные вероятности нарушения КЦД при допустимом повышении сложности регламента. Эксперименты с остальными сценариями и профилями также показали работоспособность Прототипа и планируются к публикации в дальнейшем.

Заключение

Проведенный этап исследования позволяет говорить не только о теоретическом решении оптимизационной задачи по корректировке регламентов деятельности, повышающем их устойчивость к девиации оператора, но и о практической реализации такого решения в виде соответствующего программного прототипа. Практическая значимость полученного результата заключается в возможности непосредственного применения созданного средства для повышения ИБ ресурсов АС, особенно в условиях деструктивных воздействий на пользователей таких систем.

Список литературы

1. *Абдуллин Т.И., Баев В.Д., Буйневич М.В., Бурзунов Д.Д., Васильева И.Н., Галиуллина Э.Ф. и др.* Цифровые технологии и проблемы информационной безопасности: монография. – СПб: СПГЭУ, 2021. – 163 с.

2. *Власов Д.С.* К вопросу о мотивации инсайдера организации и способах его классификации // Электронный сетевой политематический журнал «Научные труды КубГТУ». – 2022. – № 1. – С. 128–147.

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

4. *Буйневич М.В., Иванов И.И.* Повышение «устойчивости» регламентов деятельности как способ противодействия неумышленному инсайдингу // Вопросы кибербезопасности. – 2024. – № 6 (64). – С. 108-116. – DOI: 10.21681/2311-3456-2024-6-108-116.

5. *Моисеенко Г.Ю.* Программно-алгоритмическая архитектура интеллектуальной системы корректировки инструкций по работе в автоматизированной системе в интересах обеспечения информационной безопасности // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2026. – № 3. – С. 186–202. – DOI: 10.61260/2218-130X-2026-3-186-202

6. *Вострых А.В.* Алгоритм оценки эффективности визуальной эстетики интерфейсов специализированных программных продуктов, используемых экстренными службами // Национальная безопасность и стратегическое планирование. – 2024. – № 3 (47). – С. 77–89. – DOI: 10.37468/2307-1400-2024-3-77-89.

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

8. *Тайк Ай.М., Лупин С.А., Кхаинг М.Т.* Методы повышения эффективности алгоритма полного перебора на примере решения задачи о неограниченном ранце // International Journal of Open Information Technologies. – 2023. – Т. 11. – № 5. – С. 41–46.

9. *Сарин К.С.* Гибридный алгоритм смешанной многокритериальной оптимизации «кукушкин поиск» с генетическим оператором скрещивания // Искусственный интеллект и принятие решений. – 2024. – № 2. – С. 87–105. – DOI: 10.14357/20718594240207.

10. *Пиванова Д.Н., Федорова Т.А.* Анализ эффективности модифицированных методов имитации отжига в задачах невыпуклой оптимизации // Неделя науки Санкт-Петербургского государственного морского технического университета. – 2024. – Т. 2. – № 1. – С. 208–218.

11. *Данилова М.В., Моллон Д.Д.* Цветовые категории и цветоразличение // Экспериментальная психология. – 2010. – Т. 3. – № 3. – С. 39–56.

12. *Елисов Л.Н.* К вопросу о точности эвристических алгоритмов при решении оптимизационных задач в эксплуатации // Научный вестник Московского государственного технического университета гражданской авиации. – 2012. – № 179. – С. 123–126.

Статья поступила в редакцию 15 апреля 2026 г.
Принята к публикации 26 июня 2026 г.

Ссылка для цитирования: Моисеенко Г.Ю., Израилов К.Е. Базовый эксперимент по корректировке регламентов работы в автоматизированных системах в интересах противодействия неумышленному IT-инсайдингу // Национальная безопасность и стратегическое планирование. 2026. № 2(54). С. 18-25. DOI: https://doi.org/10.37468/2307-1400-2026-2-18-25

Scientific article

A basic experiment to adjust working regulations in the automated system in the interests of countering IT-insiding

Moiseenko Grigory Y. [1]
Izrailov Konstantin E. [2]

[1] *Ministry of Defense of the Russian Federation, Moscow, Russia*

[2] *Saint Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia named after Hero of the Russian Federation General of the Army E.N. Zinichev, Saint Petersburg, Russia*

Abstract

This study addresses countering unintentional IT insider activity, understood as actions by operators of automated systems that violate official job regulations as a result of behavioural deviation. This problem is reduced to an optimization problem, for which the authors have previously proposed an analytical model and a hybrid method for solving it. To enable their practical application, a corresponding software tool was developed; its operating logic and functionality are presented in this article. The following ten user profiles are proposed, reflecting factors and characteristics of behavioural deviation: impaired colour perception, reading difficulties, severe fatigue, experienced user, low vision, working memory impairment, no deviation, stress, time pressure, and ordinary user. A baseline experiment is conducted to enhance the robustness of the operator's activity regulations in the context of an authorization interface, demonstrating the viability of all the scientific and practical results obtained.

Keywords: automated system; information security; operator; user profile; operational regulations; behavioural deviation; software prototype; experiment

References

1. *Abdullin T.I., Baev V.D., Buinevich M.V., Burzunov D.D., Vasilyeva I.N., Galiullina E.F., et al.* Digital Technologies and Information Security Issues: A Monograph. – St. Petersburg: UNECON, 2021. – 163 p.

2. *Vlasov D.S.* On the Issue of Organizational Insider Motivation and Classification Methods // Electronic Multidisciplinary Journal "Scientific Works of KubSTU". – 2022. – No. 1. – P. 128–147.

3. *Matveev A.V., Matveev V.V*. A Systems-Cybernetic Approach to Defining the Concept of "Security" // National Security and Strategic Planning. – 2015. – No. 1 (9). – P. 18–25.

4. *Buinevich M.V., Ivanov I.I*. Enhancing the "Resilience" of Operational Procedures as a Means to Counter Unintentional Insider Activity // Cybersecurity Issues. – 2024. – No. 6 (64). – P. 108–116. – DOI: 10.21681/2311-3456-2024-6-108-116.

5. *Moiseenko G.Yu.* Software-Algorithmic Architecture of an Intelligent System for Adjusting Automated System Operating Instructions to Ensure Information Security // Scientific-Analytical Journal "Bulletin of the St. Petersburg University of the State Fire Service of EMERCOM of Russia". – 2026. – No. 3. – P. 186–202. – DOI: 10.61260/2218-130X-2026-3-186-202

6. *Vostrykh A.V.* Algorithm for evaluating the visual aesthetics of interfaces in specialized software products used by emergency services // National Security and Strategic Planning. – 2024. – No. 3 (47). – P. 77–89. – DOI: 10.37468/2307-1400-2024-3-77-89.

7. *Moiseenko G.Yu*. Formal problem statement for countering unintentional insider threats in an organization through the adjustment of job descriptions // Information Protection. Inside. – 2025. – No. 6 (126). – P. 61–69.

8. *Taik A.M., Lupin S.A., Khaing M.T.* Methods for improving the efficiency of the brute-force algorithm: a case study of the unbounded knapsack problem // International Journal of Open Information Technologies. – 2023. – Vol. 11. – No. 5. – P. 41–46.

9. *Sarin K.S.* A hybrid "Cuckoo Search" multi-criteria optimization algorithm incorporating a genetic crossover operator // Artificial Intelligence and Decision Making. – 2024. – No. 2. – P. 87–105. – DOI: 10.14357/20718594240207.

10. *Pivanova D.N., Fedorova T.A*. Efficiency analysis of modified simulated annealing methods in non-convex optimization problems // Science Week of St. Petersburg State Marine Technical University. – 2024. – Vol. 2. – No. 1. – P. 208–218. 11.Danilova M.V., Mollon J.D. Color categories and color discrimination // Experimental Psychology. – 2010. – Vol. 3. – No. 3. – P. 39–56.

11. *Elisov L.N.* On the accuracy of heuristic algorithms for solving optimization problems in operations // Scientific Bulletin of the Moscow State Technical University of Civil Aviation. – 2012. – No. 179. – P. 123–126.

For citation: Moiseenko G.Y., Izrailov K.E. A basic experiment to adjust working regulations in the automated system in the interests of countering IT-insiding // National security and strategic planning. 2026. № 2(54). pp. 18-25. DOI: https://doi.org/10.37468/2307-1400-2026-2-18-25

Информация об авторах:

Моисеенко Григорий Юрьевич – руководитель направления Министерства обороны Российской Федерации, г. Москва, *Россия*
e-mail: mogreq@mail.ru

Израилов Константин Евгеньевич – кандидат технических наук, доцент, профессор кафедры прикладной математики и безопасности информационных технологий, Санкт-Петербургский университет Государственной противопожарной службы МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева, *г. Санкт-Петербург, Россия*
ORCID: https://orcid.org/0000-0002-9412-5693
SPIN-код: 5109-3499
e-mail: konstantin.izrailov@mail.ru

Information about authors:

Moiseenko Grigory Y. – Head of direction, Ministry of Defense of the Russian Federation, Moscow, Russia
e-mail: mogreq@mail.ru

Izrailov Konstantin E. – Candidate of Technical Sciences, Associate Professor, Professor of the Applied mathematics and information security technologies Department, St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia named after Hero of the Russian Federation, Army General E.N. Zinichev, St. Petersburg, Russia
ORCID: https://orcid.org/0000-0002-9412-5693
SPIN: 5109-3499
e-mail: konstantin.izrailov@mail.ru