Цифровая экономика и управление

УДК 331.108.2
DOI:10.25729/ESI.2026.42.2.012

Оптимизация программы мероприятий по кадровой безопасности предприятия методами дискретного программирования

Туктарова Полина Андреевна[1], Мансурова Юлия Талгатовна[2], Ялтонская Диана Ильвировна[2]

[1]Иркутский государственный аграрный университет имени А.А. Ежевского, Россия, Иркутская область, Иркутский район, поселок Молодежный, *ptuktarova@gmail.com*
[2]Уфимский университет науки и технологий, Россия, Уфа

Аннотация. Статья посвящена оптимизации программы мероприятий по кадровой безопасности предприятия на основе методов дискретного (0–1) линейного программирования в условиях ограниченных ресурсов. Актуальность обусловлена тем, что персонал одновременно выступает и ключевым активом, и потенциальным источником внутренних угроз: от непреднамеренных ошибок до осознанных нарушений, приводящих к финансовым потерям. Цель работы – сформировать формализованную модель выбора набора мер кадровой и информационной безопасности, которая при заданных лимитах бюджета и трудозатрат обеспечивает требуемое снижение интегрального риска и максимизирует ожидаемый экономический эффект. В качестве переменных решения используются бинарные показатели включения мероприятий в программу, а критерий оптимальности задаётся, как максимизация чистой годовой экономии (разницы между предотвращённым ущербом и затратами). В модель заложены ограничения по финансированию, доступному фонду человеко-часов, а также опциональное ограничение минимального совокупного эффекта. Исходные данные сформированы для шести альтернативных мероприятий (система предотвращения утечек данных (далее DLP – Data Leakage Prevention), аналитика поведения пользователей и объектов инфраструктуры (далее UEBA-аналитика), усиление многофакторной аутентификации для привилегированных пользователей (далее MFA – Multi-Factor Authentication) , e-learning по информационной гигиене, ключевые показатели эффективности (далее KPI – Key Performance Indicators) «раннее оповещение» и расширенный соцпакет) с указанием стоимости, трудоёмкости и ожидаемого сокращения потерь на основе экспертной оценки и статистики инцидентов. Практическая апробация выполнена в среде Python с применением MILP-подхода (ветви-и-границы) (MILP – Mixed-Integer Linear Programming – смешанное целочисленное линейное программирование) и демонстрирует получение оптимального набора мероприятий. Полученное решение обеспечивает укладывание в ресурсные лимиты и достижение целевого эффекта, при этом исключая меры с наихудшим соотношением затрат и ожидаемой пользы. Научно-практическая значимость работы состоит в переводе качественных управленческих рассуждений о кадровой безопасности в воспроизводимую оптимизационную постановку, пригодную для пересчёта при изменении цен, трудовых ресурсов и требований регуляторов.

Ключевые слова: кадровая безопасность, инсайдерские угрозы, дискретное программирование, 0–1 оптимизация, UEBA (User and Entity Behavior Analytics – аналитика поведения пользователей и объектов инфраструктуры), DLP (Data Leakage Prevention – система предотвращения утечек данных), MFA (Multi-Factor Authentication – многофакторная аутентификация)

Цитирование: Туктарова П.А. Оптимизация программы мероприятий по кадровой безопасности предприятия методами дискретного программирования / П.А. Туктарова, Ю.Т. Мансурова, Д.И. Ялтонская // Информационные и математические технологии в науке и управлении, 2026. – № 2(42). – С. 153-160. – DOI:10.25729/ESI.2026.42.2.012.

Введение. В современной исследовательской практике оценка кадровой безопасности предприятия опирается на совокупность математических моделей, позволяющих формализовать персонал-ориентированные уязвимости и связать их с наблюдаемыми организационными эффектами. В частности, применяются: 1) модели, описывающие зависимость кадровых уязвимостей от личностных характеристик работников, где отдельные компетенции трактуются, как частные показатели уязвимости, а их относительная значимость задаётся весовыми коэффициентами, определяемыми руководством; 2) модели, учитывающие одновременно личностные и внутриорганизационные детерминанты кадровой безопасности,

в том числе на основе аппарата теории нечётких множеств, что позволяет интегрировать количественные и качественные факторы в единую оценочную процедуру; 3) модели оценки благонадёжности работника, агрегирующие параметры образования, стажа и уровня сформированности компетенций, как основания для управленческих решений в контуре кадровой безопасности. Кадровая безопасность – это процесс предотвращения негативных воздействий на экономическую безопасность организации за счёт снижения рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями. По определению Н.В. Кузнецовой, кадровая безопасность представляет собой «процесс предотвращения, предупреждения и устранения рисков и угроз со стороны персонала с целью обеспечения стабильного функционирования и развития предприятия» [1].

Для построения прикладных моделей диагностики кадровой безопасности используются индикаторные и экономико-статистические подходы. Индикаторный подход основывается на сопоставлении фактических значений показателей с пороговыми (нормативными) уровнями, а величина отклонения от порога интерпретируется, как мера выраженности угроз. Корреляционно-регрессионный анализ применяется для выявления статистически значимых связей между числом кадрово-обусловленных инцидентов и факторами (например, значениями личностных характеристик персонала), а также для последующего прогнозирования. Методы нечётких множеств, в свою очередь, позволяют повысить определённость при оценивании вклада отдельных компонентов в интегральный показатель кадровой безопасности за счёт работы с лингвистическими переменными и экспертными шкалами.

В логике эмпирической параметризации факторов и инцидентов целесообразно выделить корреляционно-регрессионный анализ, как основной инструмент количественной идентификации влияний (при необходимости – с последующим использованием результатов, как входных параметров для оптимизационных постановок).

В обзорных работах по диагностике кадровой безопасности упоминаются подходы, связанные с оценкой надёжности и параметров персонала, в т.ч. у В.Л. Шапошникова, А.С. Артамкина и К.В. Хорошун [2].

Стабильность и надежность кадрового состава – ключевой фактор успеха любого предприятия, ведь именно сотрудники одновременно защищают компанию от угроз и могут стать источником их возникновения. Риски, связанные с персоналом, могут быть как сознательными, так и случайными. Небрежность или профессиональные ошибки сотрудников часто приводят к непреднамеренным угрозам и, как следствие, к существенным финансовым потерям для компании.

Учитывая существующие проблемы с обеспечением кадровой безопасности, например, в компании ООО «ЛУКОЙЛ-МЦПБ», целесообразно создать модель, которая при ограничениях бюджета, трудовых ресурсов и нормативов информационной защиты обеспечивает наибольший ожидаемый эффект – снижение интегрального риска внутренних инцидентов. Такая модель позволит оперативно выявлять уязвимости и принимать эффективные меры по их устранению.

Таким образом, реализованные мероприятия, указанные в таблице 1, создадут надёжный цифровой каркас кадровой безопасности, соответствующий целям программы «Бухгалтерия 2025» и служащий долговременной основой для устойчивого развития и конкурентоспособности всего холдинга.

Порядок действий:

1. Определение переменных решения:

$x_i \in \{0,1\}$ – бинарная переменная, равная 1, если мероприятие i включено в программу. Список мероприятий представлен в таблице 1.

Таблица 1. Список мероприятий, создающий надежный цифровой каркас кадровой безопасности

Номер мероприятия	Название мероприятия
x_1	Расширение лицензии StaffCop Enterprise на 200 узлов. StaffCop Enterprise — российская DLP-система (Data Leakage Prevention) для мониторинга действий сотрудников, расследования инцидентов и предотвращения утечек данных.
x_2	Интенсивный e-learning-курс по информационной гигиене для сотрудников
x_3	Повышение уровня многофакторной аутентификации (MFA) для привилегированных пользователей
x_4	Система KPI и комплекс «раннего оповещения» о неблагоприятных сотрудниках.

$h_i \geq 0$ – количество человеко-часов персонала, необходимое для реализации мероприятия *i*;

$c_i \geq 0$ – прямые денежные затраты на мероприятие *i*;

$r_i \geq 0$ – ожидаемое годовое сокращение потерь (в рублях) при реализации мероприятия *i* – параметр, рассчитанный на основе экспертной оценки UEBA-логов (User and Entity Behavior Analytics – аналитика поведения пользователей и объектов инфраструктуры) и статистики прошлых инцидентов;

UEBA-логи (User and Entity Behavior Analytics – аналитика поведения пользователей и объектов инфраструктуры) представляют собой журналы регистрации действий пользователей и устройств в ИТ-инфраструктуре компании;

R – минимально ожидаемый совокупный эффект, определяемый руководителем безопасности.

2. Определение целевой функции:

формулируем задачу, как максимизацию чистой годовой экономии, то есть разницы между предотвращённым ущербом и совокупными издержками [3, 4] по формуле 1:

$$\sum_{i=1}^{n}(r_i - c_i)x_i \to \max. \quad (1)$$

Бюджетное ограничение по формуле 2:

$$\sum_{i=1}^{n} c_i x_i \leq B, \quad (2)$$

где *B* – утверждённый годовой бюджет (например, 3 200 000 руб.).

Трудовые ресурсы по формуле 3:

$$\sum_{i=1}^{n} h_i x_i \leq H, \quad (3)$$

где H – доступный фонд человеко-часов ИТ-службы и ОКБ за плановый период.

Минимальный целевой эффект (опциональное ограничение качества) по формуле 4:

$$\sum_{i=1}^{n} r_i x_i \geq R. \quad (4)$$

Таким образом, мы имеем задачу оптимизации по формуле 5:

$$f \to \max \begin{cases} \sum_{i=1}^{n} c_i x_i \leq B \\ \sum_{i=1}^{n} h_i x_i \leq H \\ \sum_{i=1}^{n} r_i x_i \geq R \end{cases} \quad (5)$$

При линейной форме цели и ограничений, а также дискретной природе переменных x_i получается задача 0–1 линейного программирования; её можно решать методами ветвей-и-границ, срезовых плоскостей или встроенными MILP-солверами (Mixed-Integer Linear Programming – смешанное целочисленное линейное программирование) [5].

3. Интерпретация результата [6,7]:

оптимальное решение возвращает набор мероприятий, который:

– полностью вписывается в финансовый и трудовой лимиты;
– обеспечивает требуемое снижение риска;
– даёт максимальную чистую экономию.

Получившийся вектор $\overrightarrow{x*}$ позволяет составить дорожную карту внедрения, распределённую по календарным кварталам с учётом технологических зависимостей и кадровой нагрузки [8].

Таким образом, формализованная модель превращает качественные соображения («хорошо бы снизить риск и не выйти за смету») в строгую, проверяемую и оптимизируемую задачу, что обеспечивает прозрачность управленческого выбора и воспроизводимость полученных результатов.

2. Пути решения описываемой проблемы. Задача оптимизации была решена для шести альтернативных мероприятий, каждое из которых характеризуется четырьмя атрибутами: прямыми расходами, трудоёмкостью ИТ- и ОКБ-персонала, ожидаемым годовым снижением ущерба от внутренних инцидентов и принадлежностью к определённому классу действий (технологическая защита, организационная профилактика или мотивационный стимул). Годовой бюджет проекта ограничен тремя миллионами двумястами тысячами рублей, а совокупный фонд человеко-часов на внедрение – двумя сотнями [9]. Минимально приемлемый эффект задаётся на уровне 1,6 млн руб. предотвращённых убытков в год – это значение согласовано с дорожной картой уменьшения интегрального риска на 30 %. В таблице 2 представлены данные для мероприятий.

Таблица 2. Данные для мероприятий

x_i	c_i, руб.	h_i, ч	r_i, руб.
x_1	540 000	80	1 200 000
x_2	180 000	40	800 000
x_3	120 000	60	600 000
x_4	150 000	20	250 000

B = 3 200 000;

H = 200;

R = 1 600 000.

Решение задачи оптимизации:

$$\sum_{i=1}^{n}(r_i - c_i)x_i \to max.$$

$$(1\,200\,000\text{-}540\,000)x_1+(800\,000\text{-}180\,000)x_2+(600\,000\text{-}120\,000)x_3+(250\,000\text{-}150\,000)x_4 \to max.$$

Бюджетное ограничение:

$$540\,000x_1+180\,000x_2+120\,000x_3+150\,000x_4 \leq 3\,200\,000.$$

Ограничение по труду:

$$80x_1+40x_2+60x_3+20x_4 \leq 200.$$

Минимальный целевой эффект:

$$1\,200\,000x_1+800\,00x_2+600\,000x_3+250\,000x_4 \geq 1\,600\,000.$$

Оптимизация выбора мероприятий методом целочисленного линейного программирования (PuLP – Python Linear Programming – библиотека Python для задач линейного программирования). Python-скрипт на библиотеке PuLP решающий задачу 0-1 линейного программирования (листинг 1).

Листинг 1. Функция оптимизации задачи линейного программирования

```
import pulp
# Параметры мероприятий
costs   = [540_000, 180_000, 120_000, 150_000]   # c_i
hours   = [80, 40, 60, 20]                        # h_i
```

```
effects = [1_200_000, 800_000, 600_000, 250_000]  # r_i
# Ресурсы и цели
B = 3_200_000  # бюджет
H = 200        # человеко-часов
R = 1_600_000  # минимальный эффект
# Настройка модели
model = pulp.LpProblem("StaffCop_Optimization", pulp.LpMaximize)
x = [pulp.LpVariable(f"x_{i}", cat=pulp.LpBinary) for i in range(len(costs))]
# Целевая функция
model += pulp.lpSum((effects[i] - costs[i]) * x[i] for i in range(len(costs)))
# Ограничения
model += pulp.lpSum(costs[i]   * x[i] for i in range(len(costs))) <= B
model += pulp.lpSum(hours[i]   * x[i] for i in range(len(costs))) <= H
model += pulp.lpSum(effects[i] * x[i] for i in range(len(costs))) >= R
# UEBA только при DLP
model += x[1] <= x[0]
# Решаем
model.solve(pulp.PULP_CBC_CMD(msg=False))
# Результаты
selected = [i for i in range(len(x)) if pulp.value(x[i]) > 0.5]
print("Выбранные мероприятия (индексы):", selected)
print("Чистая экономия:", pulp.value(model.objective), "руб.")
```

В таблице 3 представлены результаты модели 0-1 линейного программирования, построенной в программе Python [10,11].

Таблица 3. Результаты по модели, построенной в Python

Номер мероприятия	Результат
x_1	1
x_2	1
x_3	1
x_4	1

Заключение. Таким образом, мероприятия 5 и 6 не включены в программу, так как имеют высокий уровень затрат и недостаточно очевидную пользу.

Модель 0-1 линейного программирования, построенная в Python на базе MILP-солвера CBC (CBC – COIN-OR Branch and Cut – Метод ветвей и отсечений (солвер с открытым исходным кодом), максимально увеличивает чистую экономию ($\sum r_i - \sum c_i$) при соблюдении ресурсных и логических ограничений [12, 13]. Оптимальное решение включает четыре мероприятия. Во-первых, расширяется лицензия StaffCop на 200 узлов (540 тыс. руб.; 80 ч ИТ-инженеров) – это закрывает основной периметр финансового контура. Во-вторых, подключается модуль UEBA- аналитики для глубокой корреляции событий (180 тыс. руб.; 40 ч) с обязательной связкой «только при наличии базовой DLP», что соблюдено автоматически. Третьим элементом становится интенсивная программа e-learning для ста сотрудников (120 тыс. руб.; 60 ч кураторских трудозатрат), позволяющая воспитывать культуру безопасного обращения с данными [14,15]. Наконец, вводится KPI-фонд мотивации за соблюдение регламентов (150 тыс. руб.; 20 ч HR-координации).

Совокупные расходы составляют 990 тыс. руб., трудоёмкость точно соответствует лимиту в 200 ч, а ожидаемое сокращение годовых потерь оценивается в 2,85 млн руб. Таким образом, проект обещает чистую экономию 1,86 млн руб. уже в первый год эксплуатации, превышая операционные издержки почти вдвое и формируя положительный денежный поток менее чем за девять месяцев.

На практике реализация распределяется так: ИТ-департамент поднимает сервер и разворачивает агентов, ОКБ настраивает политики контроля и пороги UEBA, HR-куратор организует дистанционный курс и фиксирует результаты тестов, а финансовый отдел ежемесячно сверяет фактический эффект (сокращение DSO (Days Sales Outstanding – период

оборота дебиторской задолженности (финансовый KPI), уменьшение количества алертов критичного уровня, экономию времени аналитиков) с прогнозом модели. Если через квартал отклонение превышает ± 10 %, параметры r_i актуализируются, и оптимизация пересчитывается – модель остаётся «живой» и реагирует на изменения цен, трудовых ресурсов и нормативных требований [16,17].

В работе показано, что задачи планирования мероприятий по кадровой безопасности целесообразно решать, как задачу 0–1 линейного программирования, позволяющую прозрачно сопоставлять эффект от снижения ущерба и стоимость внедрения при жёстких ресурсных ограничениях. По результатам расчёта оптимальный портфель включает четыре мероприятия (контроль/мониторинг, поведенческая аналитика, обучение сотрудников и мотивационно-организационные меры), тогда как инициативы с высокой стоимостью и недостаточно выраженным эффектом исключаются из программы. Предложенный подход формирует «живую» управленческую модель, которую можно регулярно актуализировать по данным инцидентов и пересчитывать при изменении бюджета и трудовых лимитов.

Список источников

1. Кузнецова Н.В. Кадровая безопасность организации. Сущность и механизм обеспечения. – Иркутск: Изд-во БГУЭП, 2019. – 285 с.
2. Шапошников В.Л. Современные модели и методы диагностики кадровой безопасности предприятия / В.Л. Шапошников, А.С. Артамкин, К.В. Хорошун // Вестник Российского университета кооперации, 2017. – № 4 (30). – С. 74-80. – URL: https://cyberleninka.ru/article/n/sovremennye-modeli-i-metody-diagnostiki-kadrovoi-bezopasnosti-predpriyatii
3. Saxena N., Hayes E., Bertino E. et al. Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 2020, vol. 9, no. 9, p. 1460, DOI: 10.3390/electronics9091460.
4. Alsowail R.A., Al-Shehari T. A multi-tiered framework for insider threat prevention. Electronics, 2021, vol. 10, no. 9, p. 1005, DOI: 10.3390/electronics10091005.
5. Software Engineering Institute, Carnegie Mellon University. Common sense guide to mitigating insider threats. 7th ed. Pittsburgh, Carnegie Mellon University, 2022, 65 p.
6. National Insider Threat Task Force. Insider threat guide. Washington, DC, National Counterintelligence and Security Center, Office of the Director of National Intelligence, 2024, 48 p.
7. NIST. Special publication 800-63B: digital identity guidelines – authentication and lifecycle management. Gaithersburg, National Institute of Standards and Technology, 2020, 79 p.
8. NIST. Cybersecurity framework (CSF). Gaithersburg, National Institute of Standards and Technology, 2023, 45 p.
9. Feng Y., Zhang L., Wang H. Recent advances in knapsack problem: a comprehensive review. Neurocomputing, 2025, vol. 650, p. 128073, DOI: 10.1016/j.neucom.2025.132135.
10. Mitchell S., O'Sullivan M., Dunning I. PuLP: a Python linear programming API. GitHub, 2015. Available at: https://github.com/coin-or/pulp (accessed: 01/05/2026).
11. Thapaliya S., Sharma A. Mitigating insider threats and data breaches: integration of behavioral analytics and NLP in DLP systems. International Journal of Multidisciplinary Innovation Research, 2024, vol. 2, no. 1, pp. 15-28.
12. Hoxhunt. Security awareness training: examples, metrics & best practices. Helsinki, Hoxhunt Ltd., 2024. Available at: https://hoxhunt.com/guide/security-awareness-training (accessed: 01/05/2026).
13. Inspired eLearning. Cyber security awareness training: creating an effective program. Tampa, Inspired eLearning, Inc., 2024. Available at: https://inspiredelearning.com/security-awareness/our-approach/ (accessed: 01.05.2026).
14. Aslam T., Khan R., Usman M. Deep learning-based multi-factor authentication: a survey of biometric and smart card integration approaches. arXiv preprint arXiv:2510.05163, 2025, 42 p.
15. Identity Defined Security Alliance. All privileged access requires multi-factor authentication. Seattle, IDSA, 2023. Available at: https://www.idsalliance.org/security-outcome/all-privileged-access-requires-multi-factor-authentication/ (accessed: 01/05/2026).
16. Testlify. The ultimate list of HR KPIs for success in 2025. San Francisco, Testlify, Inc., 2025. Available at: https://testlify.com/hr-kpis/ (accessed: 01/05/2026).
17. The KPI Institute. Top 25 human resources KPIs – 2024 edition. Melbourne, The KPI Institute, 2024, 87 p.

Туктарова Полина Андреевна. *Кандидат экономических наук, доцент кафедры информатики и математического моделирования ФГБОУ ВО «Иркутский государственный аграрный университет имени А.А.*

Ежевского». AuthorID (RSCI): 944221. SPIN: 7889-8580. ORCID: 0000-0003-0773-3138, ptuktarova@gmail.com, Россия, Иркутская область, Иркутский район, поселок Молодежный.

Мансурова Юлия Талгатовна. *Кандидат экономических наук, доцент кафедры экономики предпринимательства ФГБОУ ВО «Уфимский университет науки и технологий». AuthorID (RSCI): 1005445, SPIN: 4596-9811, ORCID: 0000-0001-7373-0344, mansurova.j@mail.ru. Россия, Республика Башкортостан, Уфа, ул. Карла Маркса 12.*

Ялтонская Диана Ильвировна. *Старший преподаватель кафедры экономики предпринимательства ФГБОУ ВО «Уфимский университет науки и технологий». AuthorID (RSCI): 1204681, SPIN: 8811-4946, ORCID: 0009-0007-4430-5657, diana.khamidullina.2016@mail.ru. Россия, Республика Башкортостан, Уфа, ул. Карла Маркса 12.*

UDC 331.108.2
DOI:10.25729/ESI.2026.42.2.012

Optimization of the enterprise personnel security program using discrete programming methods

Polina A. Tuktarova[1], Yulia T. Mansurova[2], Diana I. Yaltonskaya[2]

[1]Irkutsk State Agrarian University named after A.A. Ezhevsky, Russia, Irkutsk region, Irkutsk distrikt, Molodezhny settlement, *ptuktarova@gmail.com*

[2]Ufa University of Science and Technology, Russia, Ufa

Abstract. This article focuses on optimizing an enterprise's personnel security program using discrete (0-1) linear programming methods under resource constraints. This approach is relevant because personnel are both a key asset and a potential source of internal threats, ranging from unintentional errors to deliberate violations leading to financial losses. The objective of this study is to develop a formalized model for selecting a set of personnel and information security measures that, given budget and labor limits, ensures the required reduction in integral risk and maximizes the expected economic impact. Binary indicators for program inclusion are used as decision variables, and the optimality criterion is defined as maximizing net annual savings (the difference between prevented damage and costs). The model incorporates constraints on funding, available man-hours, and an optional minimum cumulative impact constraint. Initial data was generated for six alternative measures (DLP/StaffCop monitoring, UEBA analytics, MFA enhancements for privileged users, information hygiene e-learning, KPIs/early warning, and an expanded benefits package) indicating cost, labor intensity, and expected loss reduction based on expert assessment and incident statistics. Practical testing was performed in the Python environment using the MILP (branch-and-bound) approach and demonstrates the optimal set of measures. The resulting solution ensures compliance with resource limits and the achievement of the target effect, while eliminating measures with the worst cost-to-benefit ratio. The scientific and practical significance of this work lies in the translation of high-quality management reasoning about personnel security into a reproducible optimization formulation suitable for recalculation with changes in prices, labor resources, and regulatory requirements.

Keywords: HR security, insider threats, discrete programming, 0-1 optimization, UEBA, DLP, MFA

References

1. Kuznetsova N.V. Kadrovaya bezopasnost' organizatsii. Sushchnost' i mekhanizm obespecheniya [Personnel security of an organization. Essence and mechanism of provision]. Irkutsk, Baikal State University of Economics and Law Publ., 2019, 285 p.
2. Shaposhnikov V.L., Artamkin A.S., Khoroshun K.V. Sovremennyye modeli i metody diagnostiki kadrovoy bezopasnosti predpriyatiya [Modern models and methods for diagnosing personnel security of an enterprise]. Vestnik Rossiyskogo universiteta kooperatsii [Bulletin of the Russian university of cooperation], 2017, no. 4 (30), pp. 74-80. Available at: https://cyberleninka.ru/article/n/sovremennye-modeli-i-metody-diagnostiki-kadrovoi-bezopasnosti-predpriyatii.
3. Saxena N., Hayes E., Bertino E. et al. Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 2020, vol. 9, no. 9, p. 1460, DOI: 10.3390/electronics9091460.

4. Alsowail R.A., Al-Shehari T. A multi-tiered framework for insider threat prevention. Electronics, 2021, vol. 10, no. 9, p. 1005, DOI: 10.3390/electronics10091005.
5. Software Engineering Institute, Carnegie Mellon University. Common sense guide to mitigating insider threats. 7th ed. Pittsburgh, Carnegie Mellon University, 2022, 65 p.
6. National Insider Threat Task Force. Insider threat guide. Washington, DC, National Counterintelligence and Security Center, Office of the Director of National Intelligence, 2024, 48 p.
7. NIST. Special publication 800-63B: digital identity guidelines – authentication and lifecycle management. Gaithersburg, National Institute of Standards and Technology, 2020, 79 p.
8. NIST. Cybersecurity framework (CSF). Gaithersburg, National Institute of Standards and Technology, 2023, 45 p.
9. Feng Y., Zhang L., Wang H. Recent advances in knapsack problem: a comprehensive review. Neurocomputing, 2025, vol. 650, p. 128073, DOI: 10.1016/j.neucom.2025.132135.
10. Mitchell S., O'Sullivan M., Dunning I. PuLP: a Python linear programming API. GitHub, 2015. Available at: https://github.com/coin-or/pulp (accessed: 01/05/2026).
11. Thapaliya S., Sharma A. Mitigating insider threats and data breaches: integration of behavioral analytics and NLP in DLP systems. International Journal of Multidisciplinary Innovation Research, 2024, vol. 2, no. 1, pp. 15-28.
12. Hoxhunt. Security awareness training: examples, metrics & best practices. Helsinki, Hoxhunt Ltd., 2024. Available at: https://hoxhunt.com/guide/security-awareness-training (accessed: 01/05/2026).
13. Inspired eLearning. Cyber security awareness training: creating an effective program. Tampa, Inspired eLearning, Inc., 2024. Available at: https://inspiredelearning.com/security-awareness/our-approach/ (accessed: 01.05.2026).
14. Aslam T., Khan R., Usman M. Deep learning-based multi-factor authentication: a survey of biometric and smart card integration approaches. arXiv preprint arXiv:2510.05163, 2025, 42 p.
15. Identity Defined Security Alliance. All privileged access requires multi-factor authentication. Seattle, IDSA, 2023. Available at: https://www.idsalliance.org/security-outcome/all-privileged-access-requires-multi-factor-authentication/ (accessed: 01/05/2026).
16. Testlify. The ultimate list of HR KPIs for success in 2025. San Francisco, Testlify, Inc., 2025. Available at: https://testlify.com/hr-kpis/ (accessed: 01/05/2026).
17. The KPI Institute. Top 25 human resources KPIs – 2024 edition. Melbourne, The KPI Institute, 2024, 87 p.

Tuktarova Polina Andreevna. *PhD in Economics of the Department of Computer Science and Mathematical Research, Irkutsk State Agrarian University named after A.A. Ezhevsky. AuthorID (RSCI): 944221. SPIN: 7889-8580. ORCID: 0000-0003-0773-3138, ptuktarova@gmail.com. Russia, Irkutsk region, Irkutsk distrikt, Molodezhny settlement.*

Mansurova Yulia Talgatovna. *PhD in Economics of the Department of Economics of Entrepreneurship, Ufa University of Sciences and Technologies. AuthorID (RSCI): 1005445, SPIN: 4596-9811, ORCID: 0000-0001-7373-0344, mansurova.j@mail.ru. Russia, Republic of Bashkortostan, Ufa, st. Karl Marx 12.*

Yaltonskaya Diana Ilvirovna. *Senior lecturer of the Department of Economics of Entrepreneurship, Ufa University of Sciences and Technologies. AuthorID (RSCI): 1204681, SPIN: 8811-4946, ORCID: 0009-0007-4430-5657, diana.khamidullina.2016@mail.ru, Russia, Republic of Bashkortostan, Ufa, st. Karl Marx 12.*

Статья поступила в редакцию 08.01.2026; одобрена после рецензирования 06.05.2026; принята к публикации 11.05.2026.

The article was submitted 01/08/2026; approved after reviewing 05/06/2026; accepted for publication 05/11/2026.