ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2026 • Volume 41 No 1

DOI: 10.32517/0234-0453-2026-41-1-109-118

ФОРМИРОВАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: УПРАВЛЕНЧЕСКИЕ МЕХАНИЗМЫ И РАЗВИТИЕ КОМПЕТЕНЦИЙ ПЕРСОНАЛА

П. С. Балицкий[1], **И. Н. Белогруд**[1], **М. В. Масалева**[1], **С. А. Резниченко**[1] ✉

[1] ***Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия***

✉ *sareznichenko@fa.ru*

Аннотация

Представленное в статье исследование посвящено анализу управленческих механизмов формирования культуры информационной безопасности в цифровой образовательной среде высших учебных заведений. Цифровая трансформация актуализирует защиту персональных данных, обеспечение непрерывности образовательного процесса в условиях киберугроз, развитие компетенций персонала. Сектор образования демонстрирует высокую уязвимость вследствие недостаточной подготовки кадров. Целью исследования стала разработка интегрированной модели управления культурой информационной безопасности, основанной на системном развитии компетенций персонала. Методологическую основу исследования составили институциональный подход к организационной культуре, концепция управления человеческими ресурсами в цифровой экономике, компетентностный подход. Эмпирическая база включала опрос 130 сотрудников образовательных организаций г. Москвы, анализ регламентов 12 университетов, экспертные интервью с руководителями служб безопасности. Временные рамки исследования: январь—ноябрь 2025 года. Результаты опроса показали, что 74,6 % респондентов недостаточно осведомлены о защите информации, 62,3 % не владеют навыками распознавания фишинга. Внедрение модели повысило информационную грамотность персонала на 41,8 %, снизило инциденты на 37,5 %. Установлена корреляция между культурой информационной безопасности и лояльностью к цифровым трансформациям ($r = 0{,}71$). Теоретическая значимость исследования состоит в развитии концепций формирования культуры информационной безопасности в цифровизации образования, его практическая ценность заключается в совершенствовании управления персоналом, повышении устойчивости образовательных организаций к киберугрозам.

Ключевые слова: информационная безопасность, культура информационной безопасности, управление персоналом, цифровая трансформация, образовательная организация, компетенции персонала, корпоративная культура.

Для цитирования:

Балицкий П. С., Белогруд И. Н., Масалева М. В., Резниченко С. А. Формирование культуры информационной безопасности в цифровой образовательной среде: управленческие механизмы и развитие компетенций персонала. *Информатика и образование*. 2026;41(1):109–118. DOI: 10.32517/0234-0453-2026-41-1-109-118.

FORMATION OF INFORMATION SECURITY CULTURE IN DIGITAL EDUCATIONAL ENVIRONMENT: MANAGEMENT MECHANISMS AND STAFF COMPETENCY DEVELOPMENT

P. S. Balitsky[1], **I. N. Belogrud**[1], **M. V. Masaleva**[1], **S. A. Reznichenko**[1] ✉

[1] ***Financial University under the Government of the Russian Federation, Moscow, Russia***

✉ *sareznichenko@fa.ru*

Abstract

The study presented in the article is devoted to the analysis of management mechanisms for formation of information security culture in the digital educational environment of higher educational institutions. Digital transformation actualizes the problem of protecting personal data, ensuring continuity of the educational process under cyber threats, developing staff competencies. The education sector demonstrates high vulnerability due to insufficient staff training. The purpose of the study is to develop an integrated model for managing information security culture based on systematic development of personnel competencies. The methodological basis consisted of an institutional approach to organizational culture, the concept of human resource management in the digital economy, competency-based approach. The empirical base included a survey of 130 employees of educational organizations in Moscow, analysis of

regulations of 12 universities, expert interviews with security service heads. Timeframe of the study: January—November 2025. The survey results showed that 74.6 % of respondents are insufficiently aware of information protection, 62.3 % do not possess phishing recognition skills. Model implementation increased information literacy by 41.8 %, reduced incidents by 37.5 %. A correlation was established between information security culture and loyalty to digital transformations (r = 0.71). The theoretical significance of the research lies in the development of concepts for the formation of an information security in the digitalization of education, its practical value lies in improving personnel management and increasing the resilience of educational organizations to cyber threats.

Keywords: information security, information security culture, personnel management, digital transformation, educational organization, staff competencies, corporate culture.

For citation:

Balitsky P. S., Belogrud I. N., Masaleva M. V., Reznichenko S. A. Formation of information security culture in digital educational environment: Management mechanisms and staff competency development. *Informatics and Education.* 2026;41(1):109–118. (In Russian.) DOI: 10.32517/0234-0453-2026-41-1-109-118.

1. Введение

Цифровая трансформация высшего образования создает вызовы в области информационной безопасности (ИБ). Согласно Белой книге цифровой экономики, численность специалистов в ИТ-отрасли России в 2023 году достигла 857 тысяч человек[1]. Прогнозирование изменений на российском рынке труда фиксирует нарастающий дефицит специалистов в сфере информационных технологий, при этом спрос на таких специалистов максимален в сегменте информационной безопасности [1]. Образовательные организации, накапливающие персональные данные обучающихся и сотрудников, становятся целями киберпреступников, при этом исследования информационно-образовательных сред вузов выявляют существенные дефициты их защищенности [2]. В 2023 году количество утекших данных превысило 1 миллиард записей[2]. Доктрина информационной безопасности РФ определяет приоритеты государственной политики в этой области[3], Федеральный закон № 152-ФЗ устанавливает требования к защите персональных данных[4]. Более 70 % инцидентов в области ИБ обусловлены человеческим фактором, при этом мотивационные сбои в системе управления персоналом существенно усугубляют проблему недостаточной осведомленности сотрудников о возможных угрозах информационной безопасности и их неспособности распознавать такие угрозы [3]. Управление персоналом предполагает формирование корпоративной культуры, ориентированной на соблюдение требований безопасности [4]. Формирование эффективной культуры информационной безопасности как элемента социальной ответственности организации снижает инциденты на 40–45 % и повышает доверие стейкхолдеров [5].

Следует отметить, что существующие подходы к формированию культуры информационной безопасности в цифровой образовательной среде высших учебн2ых заведений характеризуются фрагментарностью, слабой интеграцией с управлением персоналом, недостаточной связью с цифровой трансформацией [6]. Отсутствуют модели, учитывающие специфику образовательной деятельности, многообразие категорий персонала [7].

Отличия представленного в данной статье исследования от существующих работ заключаются в следующем:

- анализ интеграции управления информационной безопасностью в систему корпоративной культуры образовательной организации, а не изолированное рассмотрение технических аспектов защиты;
- дифференцированный подход к развитию компетенций для трех категорий персонала с учетом специфики их должностных функций и взаимодействия с информационными системами;
- эмпирическая верификация модели через апробацию в реальных условиях образовательной организации с измерением количественных показателей эффективности;
- установление корреляционных связей между культурой информационной безопасности и лояльностью персонала к процессам цифровой трансформации.

Цели исследования — разработка и апробация интегрированной модели управления культурой информационной безопасности, основанной на системном развитии компетенций персонала.

2. Методы

Методологическую основу исследования составил институциональный подход к организационной культуре, рассматривающий культуру безопасности как совокупность формальных и неформальных институтов [8]. Анализ влияния цифровой трансформации общества на различные сферы деятельности обеспечил рамку для понимания развития компетенций персонала в условиях цифровизации [9]. Применялся компетентностный подход для структурирования требований к знаниям и навыкам [10].

Исследование проводилось в январе—ноябре 2025 года.

Эмпирическая база исследования включала опрос 130 сотрудников 12 университетов г. Москвы. **Выборка** была представлена:

---

1 Белая книга цифровой экономики 2023. М.: АНО «Цифровая экономика»; 2024. 87 с. https://d-economy.ru/project/wp/

2 Цифровая экономика России: основные показатели и тенденции развития. *TADviser*. 2024. https://www.tadviser.ru/index.php/Статья:Цифровая_экономика_России

3 Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». http://static.kremlin.ru/media/acts/files/0001201612060002.pdf

4 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». https://www.consultant.ru/document/cons_doc_LAW_61801/

- административно-управленческим персоналом (31 человек, 23,8 %);
- научно-педагогическими работниками (74 человека, 56,9 %);
- техническим персоналом (25 человек, 19,3 %).

Отбор производился в ходе стратифицированной случайной выборки по должности, стажу, уровню взаимодействия с информационными системами.

Инструмент сбора данных — структурированный опросник на основе методики оценки культуры безопасности, включающий блоки вопросов по:

- осведомленности о политиках безопасности:
- владению навыками защиты;
- отношению к процедурам;
- готовности к обучению.

Проведен **контент-анализ** регламентов 12 университетов — проанализированы:

- политики безопасности;
- инструкции для пользователей;
- программы обучения;
- регламенты мониторинга.

Реализованы **экспертные интервью** с восемью руководителями служб безопасности университетов.

На основе диагностики **разработана модель управления культурой безопасности:** стратегическое планирование, развитие компетенций, коммуникация, мониторинг, совершенствование.

Апробация модели проводилась в трех подразделениях Финансового университета при Правительстве Российской Федерации (56 человек, май—ноябрь 2025 года).

Для статистической обработки использовались описательная статистика и корреляционный анализ. Качественные данные, полученные в ходе экспертных интервью, обрабатывались методом тематического кодирования, что позволило систематизировать экспертные оценки барьеров формирования культуры информационной безопасности.

3. Результаты

Проведенный опрос 130 сотрудников образовательных организаций выявил существенные дефициты культуры информационной безопасности персонала. Ниже представлены результаты по каждому из направлений диагностики: оценке уровня осведомленности, анализу навыков, контент-анализу регламентов и экспертным интервью.

Для оценки уровня осведомленности сотрудников о принципах информационной безопасности применялась адаптированная методика S. Getenet с соавторами [8], включающая 25 вопросов закрытого типа, структурированных по пяти тематическим блокам:

- правовые основы защиты информации;
- актуальные угрозы безопасности;
- технические средства защиты информации;
- организационные меры защиты информации;
- обработка персональных данных.

Каждый правильный ответ оценивался в 4 балла, что позволило получить для каждого респондента интегральную оценку по шкале от 0 до 100 баллов. Полученные индивидуальные баллы категоризировались следующим образом:

- 0–40 баллов соответствуют низкому уровню осведомленности;
- 41–70 баллов — среднему уровню;
- 71–100 баллов — высокому уровню.

Средний балл для каждой категории персонала рассчитывался как среднее арифметическое индивидуальных оценок респондентов.

Результаты диагностики представлены в таблице 1, из которой видно, что только 25,4 % сотрудников обладают достаточным уровнем знаний о защите информации, тогда как 74,6 % сотрудников демонстрируют недостаточную осведомленность.

Представители административно-управленческого персонала набрали в среднем 57 баллов, научно-педагогические работники — 43 (при этом 40,5 % продемонстрировали низкий уровень осведомленности), технический персонал — 49 баллов.

Для оценки владения навыками информационной безопасности применялась двухкомпонентная методика: самооценка по шкале с тремя градациями для шести навыков (табл. 2) и объективное тестирование на распознавание фишинга (10 образцов писем, 6 из них — с признаками социальной инженерии). Корреляция результатов r = 0,81 подтверждает валидность инструментария.

Анализ выявил критические пробелы: распознавание фишинга доступно 37,7 % сотрудников,

Таблица 1 / Table 1

Уровень осведомленности персонала о принципах информационной безопасности
Level of staff awareness of information security principles

Категория персонала	Высокий уровень, %	Средний уровень, %	Низкий уровень, %	Средний балл
Административно-управленческий персонал	35,5	41,9	22,6	57
Научно-педагогические работники	20,3	39,2	40,5	43
Технический персонал	32,0	32,0	36,0	49
ОБЩАЯ ВЫБОРКА	25,4	38,5	36,1	48

Таблица 2 / Table 2

Владение навыками информационной безопасности

Proficiency in information security skills

Навык	Владеют в полной мере, %	Владеют частично, %	Не владеют, %
Распознавание фишинговых атак	37,7	36,9	25,4
Создание надежных паролей	53,1	30,0	16,9
Регулярное обновление ПО	46,9	29,2	23,9
Безопасная работа с персональными данными	33,8	43,1	23,1
Многофакторная аутентификация	28,5	40,0	31,5
Резервное копирование	40,8	35,4	23,8

создание надежных паролей — 53,1 %, регулярное обновление ПО — 46,9 %, безопасная работа с персональными данными — 33,8 %. Такое положение создает риски нарушения законодательства и требует формирования новых компетенций сотрудников в условиях цифровизации образования [11].

Контент-анализ документов 12 университетов проведен по матрице оценки:

- наличие документа;
- дата актуализации;
- степень детализации;
- доступность;
- механизмы контроля исполнения требований информационной безопасности.

Запрашивались следующие документы:

- политики безопасности;
- инструкции для пользователей;
- программы обучения;
- регламенты мониторинга инцидентов.

Актуальность документа определялась по критерию его пересмотра за последние 12 месяцев, регулярность обучения по программам — по периодичности: не реже раза в год с подтверждением проведения.

Анализ показал вариативность подходов к регламентации информационной безопасности (табл. 3): все имеют политики безопасности, но актуализация за 12 месяцев наличествует только у 33,3 % университетов, регулярное обучение — у 25,0 %, что отражает общие риски цифровой трансформации системы высшего образования [12].

Экспертные интервью с руководителями служб безопасности выявили следующие барьеры формирования культуры информационной безопасности в образовательных организациях:

- недостаточное финансирование обучения (87,5 %);
- низкая приоритетность безопасности в стратегии (75,0 %);
- отсутствие мониторинга культуры информационной безопасности (62,5 %).

Разработана интегрированная модель управления культурой информационной безопасности в образовательных организациях (рис. 1), включающая:

- стратегическое планирование культуры информационной безопасности, интегрированное в общую стратегию цифровой трансформации образовательной организации;
- дифференцированное развитие компетенций персонала в области информационной безопасности с учетом категории должности и характера взаимодействия с информационными системами;

Таблица 3 / Table 3

Характеристики регламентации информационной безопасности

Characteristics of information security regulation

Характеристика	Количество организаций	Доля, %
Наличие утвержденной политики ИБ	12	100,0
Актуализация политики безопасности (за 12 месяцев)	4	33,3
Детальные инструкции для пользователей	9	75,0
Программы обучения персонала	7	58,3
Регулярное обучение (не менее одного раза в год)	3	25,0
Система мониторинга инцидентов	8	66,7

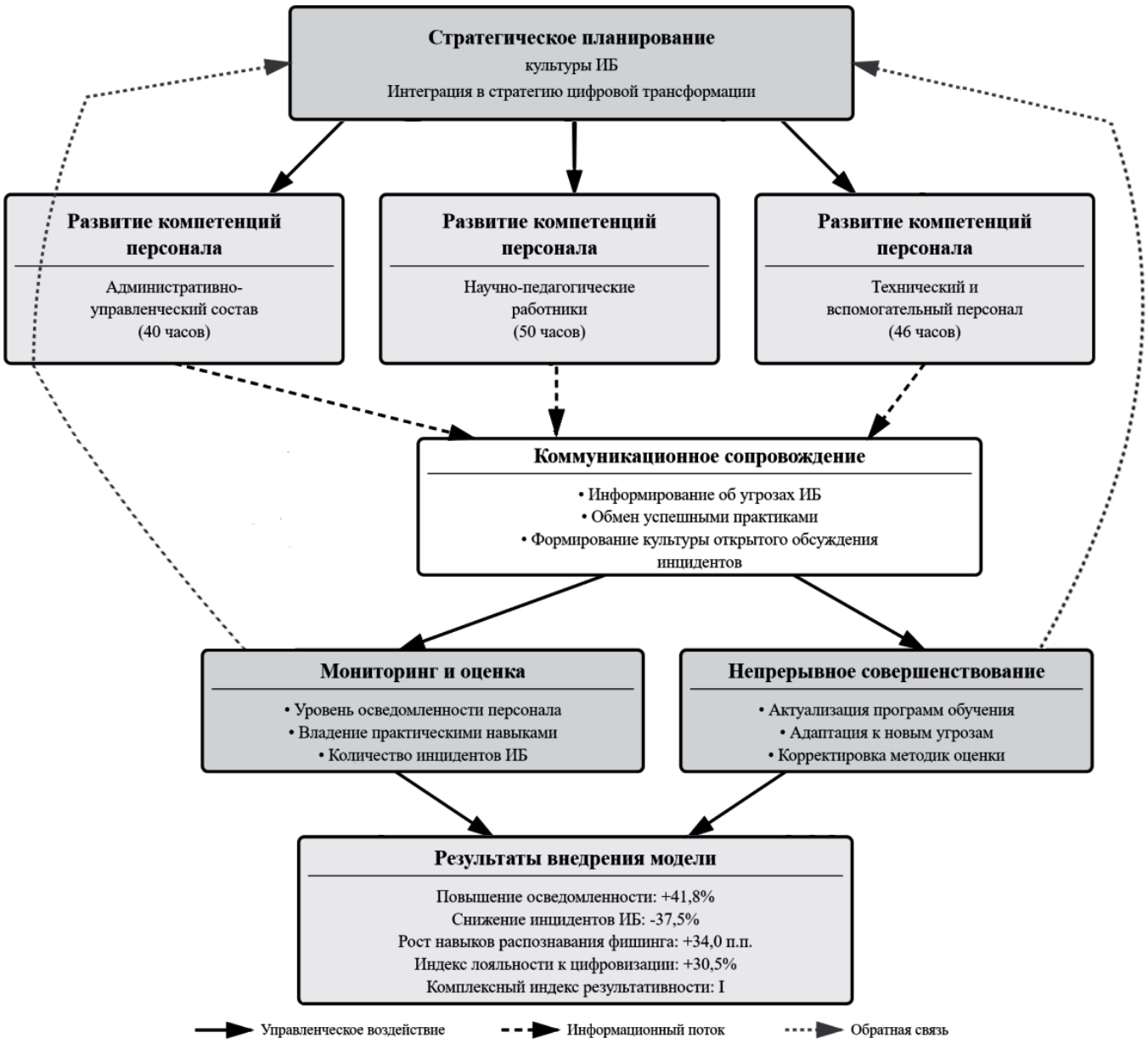


Рис. 1. Интегрированная модель управления культурой информационной безопасности в образовательных организациях
Fig. 1. Integrated model for managing information security culture in educational organizations

- коммуникационное сопровождение процессов обеспечения информационной безопасности, включающее информирование об актуальных угрозах и обмен успешными практиками;
- мониторинг и оценку уровня осведомленности персонала, владения практическими навыками защиты информации и динамики инцидентов;
- непрерывное совершенствование системы управления информационной безопасностью на основе результатов мониторинга и адаптации к изменяющимся угрозам.

Модель представляет собой многоуровневую систему взаимосвязанных компонентов, объединяющих стратегический, тактический и операционный уровни управления.

Внедрение разработанной интегрированной модели управления культурой информационной безопасности в практику работы университетов позволило достичь системного повышения компетенций персонала образовательных организаций в области защиты информации.

На основе выявленных дефицитов осведомленности и навыков персонала (см. табл. 1, 2) в рамках разработанной интегрированной модели была создана **дифференцированная программа развития компетенций в области информационной безопасности.** Структура программы сформирована с опорой на действующие профессиональные стандарты и с учетом функциональных обязанностей различных категорий сотрудников, что согласуется с компетент-

ностным подходом к построению образовательных программ в условиях цифровизации [10].

Распределение часов по модулям определено методом Дельфи в два раунда с участием руководителей служб безопасности восьми университетов.

Приоритетность модулей установлена матричным методом на основе анализа должностных инструкций и характера взаимодействия с информационными системами.

Структура программы (табл. 4):

- *административно-управленческий персонал* обучается 40 часов с акцентом на правовые основы ИБ и управление рисками;
- *научно-педагогические работники* — 50 часов, причем наибольшее внимание уделяется изучению вопросов защиты персональных данных обучающихся;
- *технический персонал* — 46 часов с углубленным изучением практических навыков администрирования.

Такой подход согласуется с пониманием образования и профессиональной подготовки как ключевых инструментов формирования человеческого капитала организации [13].

Апробация модели в трех подразделениях Финансового университета при Правительстве Российской Федерации (56 человек, май—ноябрь 2025 года) проведена методом двукратных измерений: входящая диагностика в мае до начала образовательных программ, итоговая — в ноябре после завершения обучения. Использовался идентичный инструментарий для сопоставимости данных.

Осведомленность оценивалась опросником из 25 вопросов, структурированных по пяти блокам:

- знание нормативных требований к защите персональных данных;
- идентификация типов киберугроз;
- понимание принципов криптографической защиты;
- знание организационных процедур реагирования на инциденты;
- владение терминологией информационной безопасности.

Инциденты фиксировались по единой классификации:

- несанкционированный доступ;
- утечка данных;
- вредоносное ПО;
- нарушение регламентов.

Лояльность к цифровизации измерялась по десятибалльной шкале Л. М. Андрюхиной [10] через 15 утверждений.

Относительное изменение вычислялось по формуле: (Ноябрь – Май) / Май × 100 %.

Результаты представлены в таблице 5:

- осведомленность выросла с 47 до 67 баллов (+41,8 %);
- владение распознаванием фишинга — с 36,0 % до 70,0 % (+34,0 п.п.);
- инциденты снизились с 24 до 15 (–37,5 %);
- лояльность увеличилась с 5,9 до 7,7 балла (+30,5 %).

Эти показатели согласуются с выводами о влиянии цифровой трансформации на развитие компетенций и карьерное продвижение работников образовательных организаций [14].

Комплексный индекс результативности I_{ef} рассчитан с весовыми коэффициентами, отражающими важность показателей для формирования культуры безопасности:

$$I_{ef} = \frac{\sum(w_i \cdot \Delta P_i)}{\sum w_i},$$

где:

- w_i — весовой коэффициент i-го показателя;
- ΔP_i — относительное изменение в процентах.

Коэффициенты установлены экспертно:

- $w_1 = 0{,}3$ (осведомленность);
- $w_2 = 0{,}25$ (навыки);
- $w_3 = 0{,}25$ (инциденты);
- $w_4 = 0{,}2$ (лояльность).

$$I_{ef} = \frac{0{,}3 \cdot 41{,}8 + 0{,}25 \cdot 94{,}4 + 0{,}25 \cdot 37{,}5 + 0{,}2 \cdot 30{,}5}{1{,}0} = 48{,}5.$$

Таблица 4 / Table 4

Структура программы развития компетенций

Structure of the competency development program

Модуль программы	Административный персонал, часы	НПР, часы	Технический персонал, часы
Правовые основы ИБ	8	6	4
Управление рисками	6	4	8
Защита персональных данных	10	12	6
Безопасность цифровых платформ	4	10	4
Социальная инженерия и фишинг	6	8	6
Практические навыки защиты	6	10	18
ВСЕГО	40	50	46

Таблица 5 / Table 5

Динамика показателей культуры информационной безопасности

Dynamics of information security culture indicators

Показатель	Май 2025	Ноябрь 2025	Изменение, %	Изменение, п.п.
Средний балл осведомленности	47	67	+41,8	+20
Владение распознаванием фишинга (%)	36,0	70,0	+94,4	+34,0
Количество инцидентов (за полугодие)	24	15	–37,5	–9
Доля прошедших обучение (%)	16,1	100,0	—	+83,9
Индекс лояльности к цифровизации	5,9	7,7	+30,5	+1,8

Значение 48,5 превышает пороговое 30,0, что свидетельствует о высокой эффективности модели.

Корреляционный анализ методом Пирсона на выборке 56 респондентов выявил взаимосвязи между аспектами культуры безопасности.

Результаты корреляционного анализа представлены в таблице 6, из которой видна сильная связь осведомленности и навыков ($r = 0,79$), что подтверждает эффективность комплексного подхода к компетенциям. Отрицательная корреляция навыков и инцидентов ($r = –0,68$) показывает, что компетентность снижает нарушения. Положительная связь осведомленности и лояльности ($r = 0,71$) подтверждает, что цифровые компетенции являются неотъемлемой частью подготовки специалистов и непосредственно влияют на готовность персонала к цифровизации [15].

Комплексная визуализация результатов исследования представлена на рисунке 2.

Установлено, что дифференцированный подход к обучению различных категорий сотрудников с учетом специфики их функциональных обязанностей обеспечивает более высокую эффективность по сравнению с унифицированными программами. Выявленная положительная корреляция между уровнем культуры информационной безопасности и лояльностью персонала к процессам цифровой трансформации ($r = 0,71$) доказывает, что инвестиции в формирование культуры безопасности одновременно способствуют успешной реализации стратегий цифровизации образовательных организаций. Комплексный индекс результативности модели составил 48,5 при пороговом значении эффективности 30,0, что подтверждает целесообразность внедрения предложенной модели в практику управления персоналом образовательных организаций высшего образования.

Повышение эффективности управления деятельностью вузов и подготовки кадров непосредственно связано с системными механизмами оценки и развития персонала, при этом результативность данных механизмов определяется их встроенностью в общую стратегию университета [16].

В перспективе исследований лежит автоматизированный мониторинг на основе искусственного интеллекта с учетом современных подходов к многостороннему регулированию на законодательном уровне данных технологий [17].

Таблица 6 / Table 6

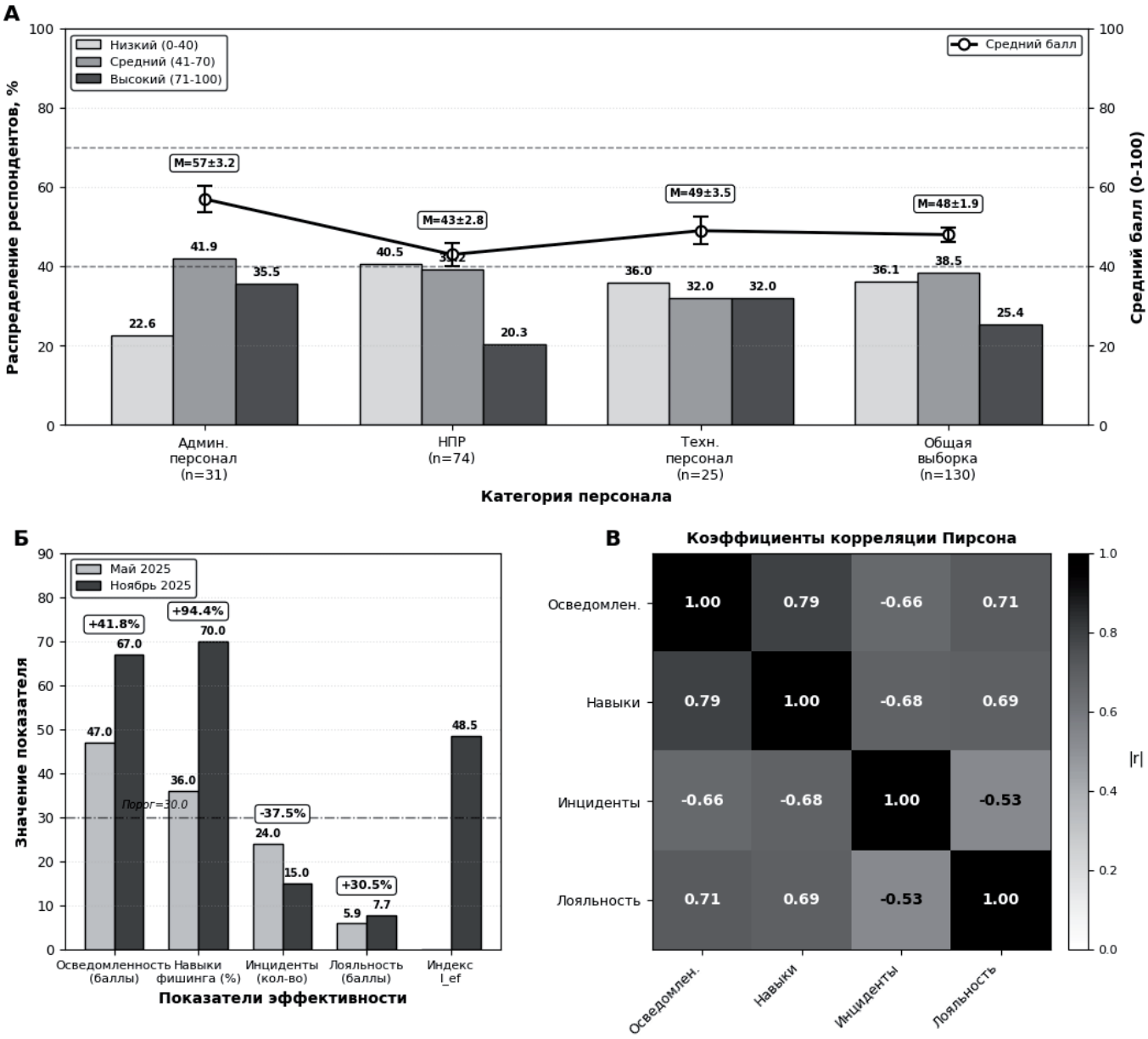
Корреляционная матрица

Correlation matrix

Показатель	Осведомленность	Навыки	Инциденты	Лояльность
Осведомленность	1,00	0,79	–0,66	0,71
Навыки	0,79	1,00	–0,68	0,69
Инциденты	–0,66	–0,68	1,00	–0,53
Лояльность	0,71	0,69	–0,53	1,00

Примечание.
В таблице представлены данные ноябрьской диагностики:
- осведомленность и навыки измеряются в индивидуальных баллах;
- инциденты — количество с участием сотрудника (0–3 на человека);
- лояльность — значения по шкале 0–10.

Статистическая значимость коэффициентов $p < 0,01$.



Общая выборка: n=130; Пилотные подразделения: n=56; Статистическая значимость: p<0.01

Рис. 2. Результаты диагностики культуры информационной безопасности и эффективности модели:
А — распределение уровня осведомленности по категориям персонала с доверительными интервалами средних баллов (n = 130);
Б — динамика ключевых показателей и индекса результативности I_ef в пилотных подразделениях (n = 56);
В — корреляционная матрица показателей культуры безопасности (коэффициенты Пирсона, p < 0.01)

Fig. 2. Results of the information security culture and model effectiveness assessment:
A — Distribution of awareness levels by personnel categories with confidence intervals for mean scores (n = 130);
Б — Dynamics of key performance indicators and the I_ef performance index in pilot units (n = 56);
B — Correlation matrix of security culture indicators (Pearson coefficients, p < 0.01)

4. Заключение

Исследование подтвердило критичность формирования культуры информационной безопасности в условиях цифровой трансформации образования. Дефициты осведомленности (74,6 % персонала) создают риски для защиты персональных данных, непрерывности образовательного процесса.

Разработанная модель управления культурой безопасности обеспечила повышение осведомленности на 41,8 %, снижение инцидентов на 37,5 %, рост лояльности к цифровизации на 30,5 %.

Корреляция между культурой безопасности и готовностью к цифровизации (r = 0,71) свидетельствует о стратегической значимости данного направления.

Результаты расширяют представления о механизмах формирования организационной культуры в цифровизации, интеграции управления безопасностью в систему управления персоналом. Модель адаптируема для различных типов образователь-

ных организаций. Перспективным направлением дальнейших исследований является анализ долгосрочных эффектов внедрения модели управления культурой информационной безопасности, в частности, оценка устойчивости достигнутых результатов через 12–24 месяца после завершения обучения. Отдельного изучения требует разработка механизмов поддержания достигнутого уровня культуры информационной безопасности персонала в условиях постоянного изменения ландшафта киберугроз. Актуальной практической задачей также представляется создание системы автоматизированного мониторинга состояния культуры информационной безопасности образовательных организаций на основе технологий искусственного интеллекта. Практическая реализация предложенной интегрированной модели управления культурой информационной безопасности способствует повышению устойчивости образовательных организаций к киберугрозам, укреплению доверия общества к цифровым образовательным сервисам, а также формированию безопасной среды для инновационного развития системы высшего образования.

Список источников / References

1. *Гусев А. А., Медведева Е. В., Григорьева А. С.* Прогнозирование изменений на российском рынке труда в сфере информационных технологий до 2029 года. *Экономика. Налоги. Право.* 2024;17(4):111–122. DOI: 10.26794/1999-849X-2024-17-4-111-122. EDN: XETQTH.

[*Gusev A. A., Medvedeva E. V., Grigoryeva A. S.* Forecasting changes in the Russian labor market in the field of information technology until 2029. *Economics, Taxes & Law*. 2024;17(4):111–122. (In Russian.) DOI: 10.26794/1999-849X-2024-17-4-111-122. EDN: XETQTH.]

2. *Фролова Е. В., Рогач О. В., Кузнецов Ю. В.* Информационно-образовательная среда вуза: приоритеты и дефициты развития. *Образование и наука.* 2025;27(6):9–28. DOI:10.17853/1994-5639-2025-6-9-28. EDN: MOPYYX.

[*Frolova E. V., Rogach O. V., Kuznetsov Yu. V.* Information and educational environment of the university: Development priorities and deficits. *The Education and Science Journal.* 2025;27(6):9–28. (In Russian.) DOI:10.17853/1994-5639-2025-6-9-28. EDN: MOPYYX.]

3. *Жигун Л. А., Литвинюк А. А.* Мотивационные сбои в системе управления персоналом. *Экономика. Налоги. Право.* 2023;16(2):48–58. DOI: 10.26794/1999-849X-2023-16-2-48-58. EDN: HAGYDK.

[*Zhigun L. A., Litvinyuk A. A.* Motivational failures in the personnel management system. *Economics, Taxes & Law*. 2023;16(2):48–58. (In Russian.) DOI: 10.26794/1999-849X-2023-16-2-48-58. EDN: HAGYDK.]

4. *Багдыков К. Т., Шевченко Д. А.* Развитие корпоративной культуры и гибких компетенций в контексте цифровой трансформации компании. *Креативная экономика.* 2022;16(6):2277–2288. DOI: 10.18334/ce.16.6.114799. EDN: ZPUXNW.

[*Bagdykov K. T., Shevchenko D. A.* Development of corporate culture and flexible competencies in the context of the company's digital transformation. *Creative Economy.* 2022;16(6):2277–2288. (In Russian.) DOI: 10.18334/ce.16.6.114799. EDN: ZPUXNW.]

5. *Колодняя Г. В.* Социальная ответственность бизнеса как ключевой фактор устойчивого развития. *Экономика. Налоги. Право.* 2023;16(5):78–85. DOI: 10.26794/1999-849X-2023-16-5-78-85. EDN: COHQUX.

[*Kolodnyaya G. V.* Social responsibility of business as a key factor of sustainable development. *Economics, Taxes & Law*. 2023;16(5):78–85. (In Russian.) DOI: 10.26794/1999-849X-2023-16-5-78-85. EDN: COHQUX.]

6. *Степанова Т. Ю.* Обеспечение информационной безопасности в образовательной организации. *Электронный научно-методический журнал Омского ГАУ.* 2020;(4(23)):25. EDN: NVBAWF.

[*Stepanova T. Yu.* Ensuring of information security in educational organizations. *Ehlektronnyj nauchno-metodicheskij zhurnal Omskogo GAU*. 2020;(4(23)):25. (In Russian.) EDN: NVBAWF.]

7. *Крошилин С. В.* Цифровая трансформация российских вузов в период пандемии. *Наука. Культура. Общество.* 2022;28(3):93–110. DOI: 10.19181/nko.2022.28.3.7. EDN: PSDTKS.

[*Kroshilin S. V.* Digital transformation of Russian universities during the pandemic. *Science. Culture. Society.* 2022;28(3):93–110. (In Russian.) DOI: 10.19181/nko.2022.28.3.7. EDN: PSDTKS.]

8. *Getenet S., Cantle R., Redmond P., Albion P.* Students' digital technology attitude, literacy and self-efficacy and their effect on online learning engagement. *International Journal of Educational Technology in Higher Education*. 2024;21:3. DOI: 10.1186/s41239-023-00437-y.

9. *Капранова Л. Д.* Цифровая трансформация общества и уровень жизни населения. *Экономика. Налоги. Право.* 2025;18(3):81–91. DOI: 10.26794/1999-849X-2025-18-3-81-91. EDN: GDXTGU.

[*Kapranova L. D.* Digital transformation of society and the standard of living of the population. *Economics, Taxes & Law*. 2025;18(3):81–91. (In Russian.) DOI: 10.26794/1999-849X-2025-18-3-81-91. EDN: GDXTGU.]

10. *Андрюхина Л. М., Садовникова Н. О., Уткина С. Н., Мирзаахмедов А. М.* Цифровизация профессионального образования: перспективы и незримые барьеры. *Образование и наука.* 2020;22(3):116–147. DOI: 10.17853/1994-5639-2020-3-116-147. EDN: WAVBRF.

[*Andryukhina L. M., Sadovnikova N. O., Utkina S. N., Mirzaakhmedov A. M.* Digitalization of professional education: Prospects and invisible barriers. *The Education and Science Journal.* 2020;22(3):116–147. (In Russian.) DOI: 10.17853/1994-5639-2020-3-116-147. EDN: WAVBRF.]

11. *Ильина И. Ю.* Формирование конкурентных стратегий преподавателей российских вузов в условиях цифровизации образования. *Экономика. Налоги. Право.* 2024;17(4):92–101. DOI: 10.26794/1999-849X-2024-17-4-92-101. EDN: BQXUXU.

[*Ilyina I. Yu.* Formation of competitive strategies for teachers of Russian universities in the context of digitalization of education. *Economics, Taxes & Law*. 2024;17(4):92–101. (In Russian.) DOI: 10.26794/1999-849X-2024-17-4-92-101. EDN: BQXUXU.]

12. *Шелепаева А. Х.* Цифровая трансформация системы высшего образования: направления и риски. *Открытое образование.* 2023;27(4):42–51. DOI: 10.21686/1818-4243-2023-4-42-51. EDN: UPTUSJ.

[*Shelepaeva A. Kh.* Digital transformation of the higher education system: Directions and risks. *Open Education*. 2023;27(4):42–51. (In Russian.) DOI: 10.21686/1818-4243-2023-4-42-51. EDN: UPTUSJ.]

13. *Молчанов И. Н.* Образование и профессиональная подготовка как инструменты формирования человеческого капитала. *Экономика. Налоги. Право.* 2023;16(2):108–118. DOI: 10.26794/1999-849X-2023-16-2-108-118. EDN: NITYNT.

[*Molchanov I. N.* Education and professional training as tools for human capital. *Economics, Taxes & Law*. 2023;16(2):108–118. (In Russian.) DOI: 10.26794/1999-849X-2023-16-2-108-118. EDN: NITYNT.]

14. *Бондаренко В. В., Полутин С. В., Юдина В. А., Танина М. А., Пензина Д. П.* Влияние цифровой трансформа-

ции системы российского высшего образования на необходимость развития компетенций и карьерного продвижения научно-педагогических работников. *Интеграция образования.* 2023;27(3(112)):490–505. DOI: 10.15507/1991-9468.112.027.202303.490-505. EDN: VZFJAG.

[*Bondarenko V. V., Polutin S. V., Yudina V. A., Tanina M. A., Penzina D. P.* Impact of digital transformation of the Russian higher education system on the need to develop competencies development and career advancement of scientific and pedagogical employees. *Integration of Education.* 2023;27(3(112)):490–505. (In Russian.) DOI: 10.15507/1991-9468.112.027.202303.490-505. EDN: VZFJAG.]

15. *Жуковская И. Е.* Цифровые компетенции как неотъемлемая часть подготовки специалистов в условиях современных вызовов. *Открытое образование.* 2025;29(5):12–21. DOI: 10.21686/1818-4243-2025-5-12-21. EDN: UJVIUH.

[*Zhukovskaya I. E.* Digital competencies as an integral part of training specialists in the context of modern challenges. *Open Education.* 2025;29(5):12–21. (In Russian.) DOI: 10.21686/1818-4243-2025-5-12-21. EDN: UJVIUH.]

16. *Полевая М. В., Жигун Л. А., Чуб А. А., Белогруд И. Н., Руденко Г. Г., Федченко А. А., Колесникова Ю. С.* Влияние рейтингов на эффективность управления деятельностью вузов и подготовки высококвалифицированных кадров. *Экономика. Налоги. Право.* 2024;17(4):42–52. DOI: 10.26794/1999-849X-2024-17-4-42-52. EDN: JCMCOK.

[*Polevaya M. V., Zhigun L. A., Chub A. A., Belogrud I. N., Rudenko G. G., Fedchenko A. A., Kolesnikova Ju. S.* The impact of ratings on the effectiveness of university management and training of highly qualified personnel. *Economics, Taxes & Law.* 2024;17(4):42–52. (In Russian.) DOI: 10.26794/1999-849X-2024-17-4-42-52. EDN: JCMCOK.]

17. *Ревенко Л. С., Ревенко Н. С.* Искусственный интеллект: современные подходы к многостороннему регулированию. *Экономика. Налоги. Право.* 2025;18(5):165–177. DOI: 10.26794/1999-849X-2025-18-5-165-177. EDN: DOPNSY.

[*Revenko L. S., Revenko N. S.* Artificial intelligence: Modern approaches to multilateral regulation. *Economics, Taxes & Law.* 2025;18(5):165–177. (In Russian.) DOI: 10.26794/1999-849X-2025-18-5-165-177. EDN: DOPNSY.]

Информация об авторах

Балицкий Петр Станиславович, канд. воен. наук, доцент, доцент кафедры «Безопасность жизнедеятельности», Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия; *ORCID:* http://orcid.org/0009-0004-6739-4291; *e-mail:* psbalitskij@fa.ru

Белогруд Игорь Николаевич, доктор филос. наук, доцент, профессор кафедры психологии и развития человеческого капитала, факультет социальных наук и массовых коммуникаций, Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия; *ORCID:* https://orcid.org/0000-0001-9338-8478; *e-mail:* inbelogrud@fa.ru

Масалева Мария Владимировна, канд. тех. наук, доцент кафедры «Безопасность жизнедеятельности», Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия; *ORCID:* http://orcid.org/0000-0002-4524-504X; *e-mail:* m.masaleva@fa.ru

Резниченко Сергей Анатольевич, канд. тех. наук, доцент, доцент кафедры информационной безопасности, факультет информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия; *ORCID:* http://orcid.org/0000-0002-1539-0457; *e-mail:* sareznichenko@fa.ru

Information about the authors

Petr S. Balitsky, Candidate of Sciences (Military Sciences), Docent, Associate Professor at the Department of Life Safety, Financial University under the Government of the Russian Federation, Moscow, Russia; *ORCID:* http://orcid.org/0009-0004-6739-4291; *e-mail:* psbalitskij@fa.ru

Igor N. Belogrud, Doctor of Sciences (Philosophy), Docent, Professor at the Department of Psychology and Human Capital Development, Faculty of Social Sciences and Mass Communications, Financial University under the Government of the Russian Federation, Moscow, Russia; *ORCID:* https://orcid.org/0000-0001-9338-8478; *e-mail:* inbelogrud@fa.ru

Maria V. Masaleva, Candidate of Sciences (Engineering), Associate Professor at the Department of Life Safety, Financial University under the Government of the Russian Federation, Moscow, Russia; *ORCID:* http://orcid.org/0000-0002-4524-504X; *e-mail:* m.masaleva@fa.ru

Sergey A. Reznichenko, Candidate of Sciences (Engineering), Docent, Associate Professor at the Department of Information Security, Faculty of Information Technologies and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russia; *ORCID:* http://orcid.org/0000-0002-1539-0457; *e-mail:* sareznichenko@fa.ru

Поступила в редакцию / Received: 15.12.25.
Поступила после рецензирования / Revised: 30.01.26.
Принята к печати / Accepted: 03.02.26.