УДК 004.056.5

С. П. Середкин [1], И. В. Кулага [1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТУДЕНТОВ

Аннотация. В статье рассматриваются современные подходы к обеспечению информационной безопасности студентов в Российской Федерации. Анализируется нормативно-правовая база, определяющая общие принципы работы с информацией. Особое внимание уделяется роли образовательных учреждений в формировании культуры кибербезопасности, развитию критического мышления и реализации практических мер противодействия актуальным киберугрозам. Исследуется взаимодействие между государством, вузами и студенческим сообществом в создании безопасной цифровой образовательной среды.

Ключевые слова: информационная безопасность, студенты, кибербезопасность, образовательная среда, цифровая грамотность, цифровая гигиена.

S. P. Seryodkin [1], I.V. Kulaga [1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

MODERN APPROACHES TO ENSURING STUDENTS' INFORMATION SECURITY

Abstract. The article discusses modern approaches to ensuring the information security of students in the Russian Federation. It analyzes the legal framework that defines the general principles of working with information. Special attention is paid to the role of educational institutions in shaping a culture of cybersecurity, developing critical thinking, and implementing practical measures to counter current cyber threats. The article explores the interaction between the government, universities, and the student community in creating a safe digital educational environment.

Keywords: information security, students, cybersecurity, educational environment, digital literacy, digital hygiene.

Введение. Цифровизация образования привела к масштабному внедрению информационных технологий в учебный процесс, что сопровождается ростом числа кибератак на образовательные учреждения [1]. Участились случаи разглашения персональных данных студентов, особенно в условиях дистанционного обучения. Эти факторы обуславливают актуальность проблемы обеспечения информационной безопасности студенческой аудитории как одной из наиболее уязвимых групп в цифровой среде.

Традиционные подходы к защите информации зачастую не учитывают динамичную эволюцию современных угроз и риски, характерные для студентов [2]. Особенности образовательных цифровых экосистем, такие как массовое использование личных устройств и открытость сетевой инфраструктуры, требуют пересмотра политики информационной безопасности. Существующие методы оказываются недостаточно эффективными против целевых атак и социальной инженерии, эксплуатирующей поведенческие особенности молодежи [3].

Постановка цели и задач. Цель данного исследования — проанализировать и систематизировать современные подходы к обеспечению информационной безопасности студентов в образовательной среде. В основе предлагаемого подхода лежит анализ поведенческих факторов студенческой аудитории в сочетании с применением передовых технологических решений. Это позволит сформировать более эффективную систему противодействия актуальным угрозам информационной безопасности.

Для достижения поставленной цели были определены следующие задачи:

1) Выявить специфические угрозы информационной безопасности, характерные для студенческой аудитории.

2) Проанализировать эффективность существующих методов защиты в учебных заведениях.

3) Разработать практические рекомендации по обеспечению информационной безопасности, учитывающие современные технологии и человеческий фактор.

Парадигма исследования. Базовыми правовыми документами, регулирующими вопросы обращения с информацией в России, являются Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4] и Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [5]. Они устанавливают общие принципы и обязанности для всех операторов информационных систем, к числу которых относятся и университетские цифровые платформы.

Общая государственная стратегия в этой сфере определяется такими документами, как Стратегия национальной безопасности РФ и Национальная программа «Цифровая экономика». В рамках последней реализуется федеральный проект «Информационная безопасность», включающий просветительские инициативы, направленные на повышение цифровой грамотности населения, в том числе студенческой молодежи.

Таким образом, правовое поле формирует основу для создания комплексной системы цифровой безопасности, где студенты являются одной из ключевых групп, требующих не столько запретительных мер, сколько образовательных инструментов и развития компетенций.

Статистические данные подтверждают актуальность проблемы: в образовательных учреждениях России за первое полугодие 2025 года было зафиксировано 18 случаев утечек конфиденциальной информации. Это на 20% больше, чем за аналогичный период 2024 года (15 инцидентов). Всего за отчетный период из российских школ, колледжей и вузов утекло около 1,7 млн записей персональных данных против 1,4 млн годом ранее. Примечательно, что глобальная тенденция обратна: в мире количество инцидентов снизилось (168 утечек, что на треть меньше, чем в прошлом году), однако число скомпрометированных записей резко выросло — до 65,3 млн против 40,6 млн. Это свидетельствует о том, что атак стало меньше, но масштаб каждой увеличился. Эксперты отмечают, что данные российских учебных заведений всё чаще появляются на площадках в даркнете.

Даркнет — это скрытая сеть, доступ к которой возможен только с помощью специального программного обеспечения. Именно там можно встретить объявления о продаже информации, похищенной из вузов, школ и центров повышения квалификации. При этом многие подобные инциденты не получают официального подтверждения. Важно понимать, что образовательный сектор является источником ценной информации: персональные данные учащихся и сотрудников, финансовые сведения, научные материалы. Это привлекает как хакеров, так и инсайдеров. Утечки подрывают доверие и могут сформировать негативный имидж вуза у абитуриентов. Следовательно, цифровизация образования должна сопровождаться постоянным повышением уровня информационной безопасности.

Статистика доли успешных кибератак по данным компании «Positive Technologies» за первое полугодие 2025 года представлена на рис. 1.

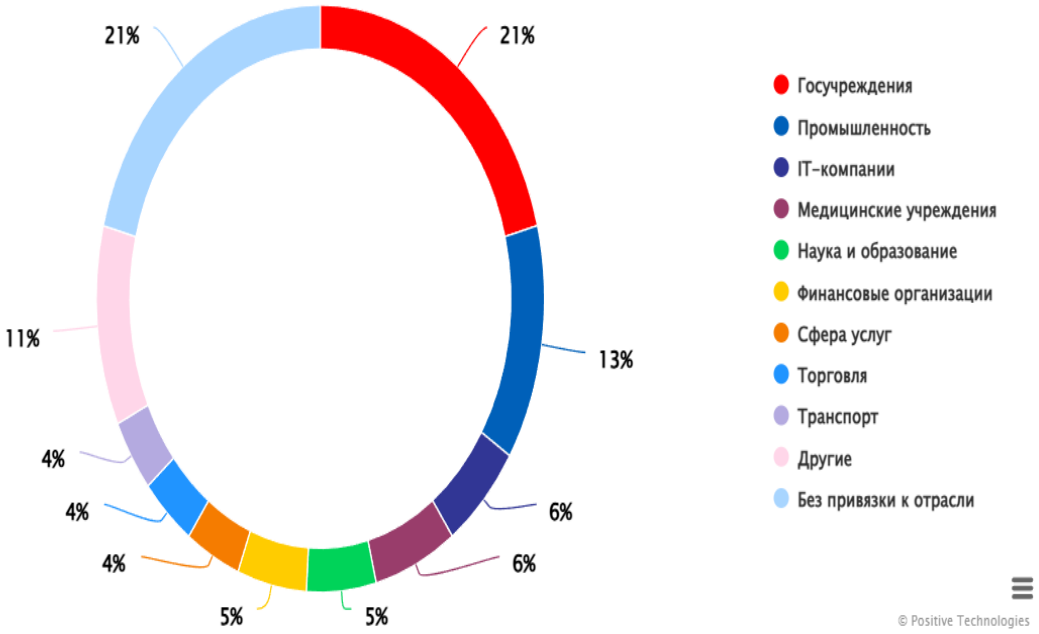

Рис. 1. Доля успешных кибератак на учреждения

Угрозы информационной безопасности в вузах Российской Федерации подразделяются на две основные категории: внутренние и внешние.

1) Внутренние угрозы — это действия, исходящие изнутри информационной системы организации (от сотрудников или студентов), которые нарушают основные свойства безопасности информации конфиденциальность, целостность и доступность информации.

2) Внешние угрозы — это угрозы, исходящие от источников за периметром организации.

Стоит отметить, что, по данным исследований, на внутренние угрозы приходится около 80% всех инцидентов, а на внешние — 20%.

В таблице 1 представлена классификация основных угроз информационной безопасности в вузах РФ.

Практическая реализация. Цифровая инфраструктура современных образовательных учреждений характеризуется высокой степенью распределённости и неоднородности компонентов. Основу учебного процесса составляют облачные сервисы для хранения материалов и организации дистанционной формы образования. Широкое использование студентами личных мобильных устройств для доступа к образовательным ресурсам создаёт множество дополнительных точек входа в сеть. Эти особенности формируют сложную среду, требующую комплексных мер защиты.

Наличие уязвимостей программного и прикладного характера может привести к угрозам информационной безопасности и ущербу для образовательной организации, её сотрудников и студентов.

Таблица 1.

Классификация основных угроз информационной безопасности в вузах РФ

Внутренние угрозы	**Внешние угрозы**
Утечка данных сотрудниками или студентами	Кибератаки (например, DDos-атаки)
Несанкционированный доступ к информации	Вредоносное ПО (вирусы, трояны)
Ошибки в обработке данных	Утрата или утечка данных

Кража оборудования (ноутбуков, серверов)	Уничтожение данных в результате физического повреждения (пожар, затопление)
Неисполнение требований политики безопасности	Атаки с использованием социальной инженерии
Несоответствие законодательству, связанного с защитой данных (например, ФЗ-152 «О персональных данных», ФЗ-149 «Об информации, информационных технологиях и защите информации»)	Несанкционированный доступ

К типичным уязвимостям относятся:

1) Эксплуатация устаревшего программного обеспечения с известными, но не закрытыми уязвимостями.

2) Недостаточно надежные системы аутентификации, упрощающие злоумышленникам доступ к конфиденциальной информации.

3) Недостаточное использование шифрования при передаче и хранении данных студентов, что повышает риск их несанкционированного перехвата и компрометации [7].

Одним из наиболее распространенных и опасных видов атак является фишинг. Фишинг (от англ. phishing — рыбалка) — вид интернет-мошенничества, целью которого является получение конфиденциальных данных (логинов, паролей, данных банковских карт) под видом официального запроса.

Целевые фишинговые атаки часто маскируются под легитимные сообщения от образовательных платформ, преподавателей или администрации вуза. Низкий уровень осведомленности студентов о таких угрозах значительно повышает риски успешных атак [8].

Анализ поведения студентов выявляет распространённые практики, повышающие их уязвимость к киберугрозам. Значительная часть обучающихся использует личные устройства для доступа к корпоративным сетям без должных мер защиты. Типичными проблемами являются пренебрежение своевременным обновлением программного обеспечения и создание слабых паролей [9].

Можно выделить следующие поведенческие факторы риска информационной безопасности:

1) Социально-психологические: Студенты в возрасте 18–22 лет часто некритически воспринимают противоречивую информацию и могут быть подвержены влиянию через молодежные субкультуры;

2) Низкое владение комплексом правил и практик, направленных на защиту персональных данных в интернете и обеспечение безопасности при использовании цифровых технологий (цифровая гигиена): Публикация избыточного количества личной информации в социальных сетях.

3) Правовая и техническая неосведомленность: Стремление получить доступ к запрещенному контенту, отсутствие знаний в области ИБ, что не позволяет предусмотреть последствия посещения сомнительных ресурсов и может привести к утечке данных и финансовым потерям [12, 13].

Критическая оценка современных подходов к обеспечению информационной безопасности в высших учебных заведениях свидетельствует о их недостаточной адаптации к особенностям студенческой аудитории. Многие вузы применяют стандартизированные

решения, разработанные для корпоративной среды, которые не в полной мере учитывают динамичный характер образовательной деятельности. Такие меры часто игнорируют специфику использования персональных устройств студентов (BYOD) и их мобильность [14].

Разработка образовательных программ и тренингов по обеспечению защиты информации для студентов включение в учебный процесс модули по повышению информационной грамотности студентов, направленных на: распознаванию фишинговых атак, управлению паролями и защите персональных данных, развитие критического мышления в поиске и анализе информации, формирование современного информационного мировоззрения [15].

Эффективность тренингов значительно повышается при использовании интерактивных методов обучения, таких как симуляции кибератак и разбор реальных кейсов. Это позволяет студентам получить практический опыт в контролируемых условиях, способствует лучшему усвоению материала и развитию навыков быстрого реагирования на угрозы. Эксперты отмечают, что интерактивные форматы повышают вовлеченность и мотивацию обучающихся [10].

Для разработки эффективных образовательных программ и тренингов по обеспечению информационной безопасности студентов можно рекомендовать следующее:

1) Анализ целевой аудитории: Определение исходного уровня знаний и потребностей студентов;

2) Постановка целей: Формулировка конкретных целей (например, повышение осведомленности о киберугрозах) и задач обучения;

3) Разработка содержания: Создание модульной структуры курса, включающей актуальные темы (основы кибергигиены, защита паролей, безопасность в соцсетях, распознавание фишинга);

4) Выбор методов обучения: Применение разнообразных форматов (лекции, семинары, практикумы, деловые игры) для повышения вовлеченности студентов;

5) Создание учебных материалов: Разработка презентаций, видеороликов, инфографики и онлайн-ресурсов;

6) Проведение тренингов: Организация занятий в офлайн- или онлайн-формате с акцентом на практическое применение знаний;

7) Оценка эффективности: Проведение контроля знаний, сбор обратной связи для улучшения программы;

8) Постоянное обновление: Регулярная актуализация материалов в соответствии с новыми тенденциями в кибербезопасности

Применение современных технологий для защиты данных и систем позволяет существенно снизить риски утечки данных. Внедрение многофакторной аутентификации в образовательных учреждениях значительно снижает вероятность несанкционированного доступа к учетным записям студентов. Этот подход обеспечивает дополнительный уровень защиты, требуя от пользователей предоставления двух или более факторов для подтверждения личности, и эффективно противодействует компрометации аккаунтов даже в случае утечки паролей.

Для обеспечения комплексной защиты данных студентов так же необходимо применять следующие технологии:

1) Шифрование: Преобразование данных в формат, нечитаемый без ключа расшифровки, применяется как при передаче, так и при хранении информации;

2) Регулярное резервное копирование позволяет быстро восстановить данные;

3) SIEM-системы (Security Information and Event Management) обеспечивают сбор и анализ данных о событиях безопасности из различных источников (сетевые устройства, серверы, приложения), что помогает выявлять подозрительную активность и предотвращать атаки в реальном времени [11].

Заключение. Проведенное исследование подтверждает наличие специфических угроз информационной безопасности, характерных для студенческой аудитории. Эти угрозы обусловлены как уязвимостями инфраструктуры образовательных учреждений, так и поведенческими особенностями самих студентов. Выявленные риски, включающие широкий спектр кибератак, подчеркивают необходимость разработки специализированных механизмов защиты.

Критический анализ существующих подходов показал их недостаточную эффективность, поскольку они не в полной мере учитывают динамично меняющийся ландшафт угроз и специфику образовательной цифровой среды. Особую актуальность эта проблема приобретает в контексте роста кибератак на образовательный сектор и широкого применения дистанционного обучения.

В работе предложен комплекс адаптированных мер, направленных на повышение уровня информационной безопасности студентов. Данные меры сочетают технические и образовательные решения и позволяют учитывать факторы образовательной среды тем самым формируя основу для создания надежной системы защиты информации.

Внедрение разработанных рекомендаций позволит существенно повысить защиту персональных данных студентов и снизить риски кибератак, создав безопасную цифровую среду необходимую для современного образовательного процесса. Таким образом, реализация предложенного подхода является критически важным элементом образовательной экосистемы в условиях ее цифровой трансформации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Д.В. Лопатин, Н.Л. Королева, М.С. Анурьева и др. ДИНАМИКА УГРОЗ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОГО ХАРАКТЕРА В МОЛОДЕЖНОЙ ГРУППЕ // Вестник Тамбовского университета. Серия Естественные и технические науки. — 2016. — №1. — С. 154–160.
2. Костюк А.В., Бобонец С.А., Примакин А.И. Подходы к обеспечению информационной безопасности электронного обучения // Вестник Санкт-Петербургского университета МВД России. — 2019. — №3. — С. 181–187.
3. Васько Т.П., Аймаганбетова О.Х., Ихсанова Д.Т. Представление об информационно-психологической безопасности современных студентов // Вестник КазНУ. Серия психологии и социологии. — 2016. — №3. — С. 39–42.
4. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ.
5. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
6. CODE RED 2026: Актуальные киберугрозы для российских организаций [Электронный ресурс]. – URL: https://www.ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id5. (Дата обращения: 15.11.2025).
7. Бабаева А. А. Интегрированные системы безопасности. — Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. — 14 с.
8. Ивлиев Сергей Николаевич, Крылова Светлана Львовна, Кваскова Алексей Александрович УГРОЗЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ // ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ. — 2020. — №6. — С. 82–86.

9. И.А. Исакова КИБЕРУГРОЗЫ ЗДОРОВЬЮ ШКОЛЬНИКОВ В ЭПОХУ ГАДЖЕТИЗАЦИИ // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. — 2022. — №4. — С. 112–117.

10. Соловьева С. А., Кулебяев М. А. Специфика культуры информационной безопасности студентов технического вуза // Развитие образования. — 2024. — №2. — С. 50–56.

11. Перевертун Д.Р. Роль искусственного интеллекта в информационной безопасности // Международный журнал информационных технологий и энергоэффективности. — 2024. — №5. — С. 92–97.

12. Гительман Л. Д., Кожевников М. В. Парадигма управленческого образования для технологического прорыва в экономике // Экономика региона. — 2018. — Т. 14, вып. 2. — С. 433–449

13. Менеджеры прорыва. Востребованы амбициозные идеи и лидеры / Л.Д. Гительман, А.П. Исаев. – М.: Инфра-М, 2015. – 152 с. - ISBN 978-5-16-011724-9. – URL: https://bookmix.ru/book.phtml?id=2238924&ysclid=ltvaldvrf823756146 (дата обращения: 15.11.2025).

14. Фабрики знаний: как новый мир перевернул высшее образование/ - URL: https://info.sibnet.ru/article/579433/?ysclid=ltvar8rczv475168213 (Дата обращения: 15.11.2025).

15. В российской информационной безопасности кадровая катастрофа. – URL: https://www.cnews.ru/news/top/2021-12-07_v_rossii_kadrovaya_katastrofa?ysclid (дата обращения: 15.11.2025).

REFERENCES

1. D.V. Lopatin, N.L. Koroleva, M.S. Anuryeva, et al. DYNAMICS OF INFORMATION AND COMMUNICATION THREATS IN THE YOUTH GROUP // Bulletin of Tambov University. Series of Natural and Technical Sciences. — 2016. — No. 1. — Pp. 154–160.

2. Kostyuk A.V., Bobonets S.A., Primakin A.I. Approaches to Ensuring Information Security of E-Learning // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. — 2019. — No. 3. — Pp. 181–187

3. Vasko T.P., Aimaganbetova O.Kh., Ikhsanova D.T. The Concept of Information and Psychological Security of Modern Students // Bulletin of KazNU. Series of Psychology and Sociology. — 2016. — No. 3. — Pp. 39–42

4. Federal Law "On Information, Information Technologies, and Information Protection" dated 27.07.2006 No. 149-FZ.

5. Federal Law "On Personal Data" dated 27.07.2006 No. 152-FZ.

6. CODE RED 2026: Current Cyber Threats for Russian Organizations [Electronic resource]. – URL:https://www.ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id5. (Accessed: 15.11.2025).

7. Babaeva A. A. Integrated Security Systems. — Kaliningrad: FGBOU VO KSTU, 2022. — 14 p.

8. Ivliev Sergey Nikolaevich, Krylova Svetlana Lvovna, Kvaskov Alexey Aleksandrovich THREATS OF INFORMATION IMPACT ON INFORMATION SYSTEMS OF EDUCATIONAL ORGANIZATIONS // INFORMATICS AND COMPUTER ENGINEERING AND MANAGEMENT. — 2020. — No. 6. — Pp. 82–86.

9. I.A. Isakova CYBER THREATS TO SCHOOLCHILDREN'S HEALTH IN THE GADGETIZATION ERA // Bulletin of Nizhny Novgorod University named after N.I. Lobachevsky. Series: Social Sciences. — 2022. — No. 4. — Pp. 112–117.

10. Solovyova S. A., Kulebyaev M. A. The specifics of the information security culture of students at a technical university // Development of Education. — 2024. — No. 2. — Pp. 50–56.

11. Perevertun D.R. The Role of Artificial Intelligence in Information Security // International Journal of Information Technologies and Energy Efficiency. — 2024. — No. 5. — Pp. 92–97.

12. Gitelman L. D., Kozhevnikov M. V. The Paradigm of Management Education for Technological Breakthrough in the Economy // Economy of the Region. — 2018. — Vol. 14, no. 2. — Pp. 433–449

13. Breakthrough Managers. Ambitious ideas and leaders are in demand / L.D. Gitelman, A.P. Isaev. Moscow: Infra-M, 2015. 152 p. ISBN 978-5-16-011724-9. URL: https://bookmix.ru/book.phtml?id=2238924&ysclid=ltvaldvrf823756146 (date of access: 015.11.2025).

14. Knowledge Factories: how the new world turned higher education upside down/ - URL: https://info.sibnet.ru/article/579433 /?ysclid=ltvar8rczv475168213 (accessed on 15.11.2025).

15. There is a personnel disaster in Russian information security. – URL: https://www.cnews.ru/news/top/2021-12-07_v_rossii_kadrovaya_katastrofa?ysclid (accessed on 15.11.2025).

Информация об авторах

Сергей Петрович Серёдкин– к. э. н., доцент кафедры «Информационные системы и защита информации» Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: Seredkin_SP@irgups.ru.

Иван Васильевич Кулага – студент группы БИ.4-22-1, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: Kulaga21092004@mail.ru.

Information about the authors

Sergey Petrovich Seryodkin– Candidate of Economic Sciences, Associate Professor of the Department of Information Systems and Information Protection, Irkutsk State Transport University, Irkutsk, e-mail: Seredkin_SP@irgups.ru.

Ivan Vasilyevich Kulaga– student of the group BI.4-22-1, Irkutsk State University of Railway Engineering, Irkutsk, e-mail: Kulaga21092004@mail.ru.

Для цитирования

Серёдкин С.П., Кулага И.В. Современные подходы к обеспечению информационной безопасности студентов // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2025. – №4. – С. 16-23. – Режим доступа: http://ismm-irgups.ru/toma/428-2025, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.12.2025)

For citations

Seryodkin S.P., Kulaga I.V. Modern approaches to ensuring students' information securiti // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2025. No. 4. P. 16-23. [Accessed 01/12/25].