УДК 004.056:378.4

Заруцкая Арина Евгеньевна - студент; институт цифровых технологий и экономики; Казанский государственный энергетический университет; Российская Федерация, город Казань, улица Красносельская, дом 51

Куценко Светлана Мунавировна – доцент; кафедра информатики и информационно-управляющих систем; Казанский государственный энергетический университет; Российская Федерация, город Казань, улица Красносельская, дом 51; тел.

КИБЕРБЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ РОССИЙСКИХ УНИВЕРСИТЕТОВ

Аннотация

В статье рассматривается обеспечение кибербезопасности информационных систем российских университетов в условиях цифровизации высшего образования, роста объема персональных данных и расширения использования внешних сервисов. Цель работы состоит в разработке риск-ориентированной модели управления защитой университетской цифровой среды. Использованы методы сравнительно-правового анализа, классификации активов, моделирования угроз и экспертного ранжирования рисков. Выделены ключевые активы: электронная образовательная среда, личные кабинеты, сервисы приемной кампании, кадровые и финансовые подсистемы, научная инфраструктура, сетевые и облачные сервисы. Установлено, что наиболее значимыми являются риски фишинга и компрометации учетных записей, вредоносного программного обеспечения и программ-шифровальщиков, уязвимостей веб-приложений, утечек персональных данных, внутренних нарушений и зависимости от поставщиков. Предложена циклическая модель управления, включающая инвентаризацию активов, построение модели угроз, оценку рисков, выбор мер защиты, мониторинг, реагирование, аудит и обучение пользователей. Сформулированы рекомендации по внедрению единого управления идентификацией, многофакторной аутентификации, резервного

копирования с тестированием восстановления, сегментации сети, контроля уязвимостей, управления привилегированным доступом и оценки внешних поставщиков. Предложен набор показателей зрелости, позволяющий контролировать результативность программы кибербезопасности университета и переходить от реактивного устранения инцидентов к управляемой киберустойчивости.

Ключевые слова: кибербезопасность; информационные системы; университет; персональные данные; киберинцидент; управление рисками; цифровая образовательная среда.

Abstract

The article examines cybersecurity of information systems in Russian universities under the conditions of digital transformation, increasing volumes of personal data and wider use of external educational services. The purpose of the study is to develop a risk-based model for managing protection of the university digital environment. The research applies comparative legal analysis, asset classification, threat modeling and expert risk ranking. The paper identifies key assets: electronic educational environment, personal accounts, admission services, human resources and finance subsystems, research infrastructure, network and cloud services. The highest-priority risks are phishing and account compromise, malware and ransomware, web application vulnerabilities, personal data leaks, insider misuse and dependence on external suppliers. A cyclic management model is proposed. It includes asset inventory, threat modeling, risk assessment, selection of security controls, monitoring, incident response, audit and user training. Practical recommendations include unified identity management, multi-factor authentication, backup with recovery testing, network segmentation, vulnerability management, privileged access management and supplier security assessment. A set of maturity indicators is proposed to monitor the effectiveness of a university cybersecurity program and to move from reactive incident elimination to managed cyber resilience.

Keywords: cybersecurity; information systems; university; personal data; cyber incident; risk management; digital educational environment.

Введение

Цифровизация высшего образования привела к изменению рисков, с которыми сталкиваются российские университеты. В современных учебных заведениях активно используются электронные информационно-образовательные платформы, личные кабинеты студентов, системы дистанционного обучения, электронные библиотеки, кадровые и финансовые подсистемы, сервисы для приема студентов, научные репозитории, беспроводные сети, облачные хранилища и интеграции с государственными ресурсами. Через эти системы ежедневно проходят персональные данные абитуриентов, студентов и сотрудников, результаты учебной деятельности, финансовая информация, данные о научных проектах и служебные документы [1]. Следовательно, утечка конфиденциальности, целостности или доступности информационных систем вуза может привести к правовым, репутационным, организационным и социальным последствиям. Актуальность данного исследования обусловлена открытостью цифровой среды университетов. В отличие от многих закрытых корпоративных систем, вузы обязаны предоставлять доступ различным категориям пользователей: студентам, преподавателям, сотрудникам, абитуриентам, родителям, внешним экспертам, подрядчикам и выпускникам. Дополнительные сложности возникают в периоды пиковых нагрузок, таких как приемная кампания, экзамены, защита выпускных работ и массовое дистанционное обучение. На практике центральные сервисы вузов часто сосуществуют с локальными системами кафедр, лабораторий и проектных групп, что увеличивает риск неучтенных активов и уязвимостей. Нормативная база защиты информации в университетах включает Федеральный закон № 149-ФЗ, Федеральный закон № 152-ФЗ, Федеральный закон № 187-ФЗ, постановление Правительства Российской Федерации № 1119, приказы ФСТЭК России № 17 и № 21, а также приказ Министерства науки и высшего образования Российской Федерации № 840, который определяет актуальные угрозы

безопасности персональных данных в информационных системах научной и образовательной сферы [3]. Международные подходы, такие как NIST Cybersecurity Framework 2.0 и OWASP Top 10, могут быть использованы как методические инструменты для упорядочивания процессов управления рисками и защиты веб-приложений. Цель данной статьи заключается в предложении риск-ориентированной модели управления кибербезопасностью информационных систем российских университетов и определении приоритетных мер для ее реализации [2].

Материалы и методы исследования

Исследование было проведено как аналитико-прикладная работа, в ходе которой использовались методы сравнительно-правового анализа, классификации информационных активов, моделирования угроз, экспертного ранжирования рисков и сопоставления угроз с организационными и техническими мерами защиты. В качестве источников информации были задействованы нормативные документы Российской Федерации, материалы ФСТЭК России, данные из Национального координационного центра по компьютерным инцидентам, а также международные документы NIST и OWASP, а также открытые отчеты и публикации о кибератаках на организации и образовательный сектор. Информационная система университета представляет собой комплекс программных, технических, организационных и пользовательских компонентов, которые обеспечивают обработку данных в области учебной, научной, административной и хозяйственной деятельности. Кибербезопасность рассматривается как способность этой системы сохранять конфиденциальность, целостность, доступность, подотчетность и управляемость в условиях внешних и внутренних угроз [4]. Цифровая среда университета имеет свои особенности, включая разнообразие ролей пользователей. Один человек может одновременно выступать как студент, сотрудник лаборатории, участник гранта, администратор учебного курса и жилец общежития. Преподаватель

может иметь права на создание электронного курса, быть научным руководителем, членом экзаменационной комиссии и пользователем финансовых сервисов. Эта множественность ролей затрудняет разграничение доступа и увеличивает риск накопления ненужных полномочий. Поэтому управление учетными записями должно быть интегрировано с учебными и кадровыми процессами, а не осуществляться вручную по отдельным запросам. Еще одной важной особенностью является необходимость сочетания открытости и защиты [5]. Университет обязан публиковать информацию о своих программах, приемной кампании, научных мероприятиях и образовательных результатах, но одновременно должен ограничивать доступ к персональным данным и внутренним документам. Наибольшую нагрузку несут публичные веб-сервисы, электронная образовательная среда и почтовая инфраструктура. Их компрометация может привести к утечке данных, изменению информации, остановке образовательного процесса и распространению атак на партнеров университета.

Таблица 1 – Основные активы, угрозы и приоритетные меры защиты

Актив	Ключевые угрозы	Приоритетные меры
Учебные и приемные сервисы	подмена оценок, отказ сайта, фишинг, кража учетных записей	многофакторная аутентификация, защита веб-приложений, мониторинг
Кадровые и финансовые подсистемы	несанкционированный доступ, мошенничество, вредоносное ПО	сегментация, контроль привилегий, резервное копирование
Научные и внешние сервисы	утрата исследований, компрометация поставщика	инвентаризация, изоляция, оценка поставщиков

Анализ актуальных угроз

Наиболее вероятный сценарий атаки на университет включает в себя использование фишинга и компрометацию учетных записей. Злоумышленники могут создавать поддельные страницы для входа в электронные образовательные платформы, отправлять вредоносные вложения или сообщения, маскируясь под

деканат или преподавателей. Это позволяет им получить доступ к системам без необходимости в сложных технических манипуляциях. Компрометированная учетная запись сотрудника может быть использована для рассылки новых сообщений, получения договоров и ведомостей, восстановления паролей или атак на внешних партнеров. Поэтому основными мерами защиты должны стать многофакторная аутентификация, защита почтового домена, мониторинг аномальных входов и регулярное обучение пользователей [6].

Второй блок угроз связан с вредоносным программным обеспечением, включая программы-шифровальщики. Согласно открытым данным отраслевых отчетов, заражение вредоносным ПО, сетевые атаки, веб-атаки, эксплуатация уязвимостей и компрометация учетных записей остаются значительными типами инцидентов для российских организаций. Для университета последствия шифрования серверов могут быть особенно тяжелыми: недоступными могут оказаться расписания, ведомости, учебные курсы, библиотечные ресурсы, данные приемной комиссии и научные материалы. Поэтому резервное копирование должно быть независимым от основной инфраструктуры и регулярно проверяться с помощью тестов восстановления.

Третий блок угроз включает в себя уязвимости веб-приложений и систем дистанционного обучения. Университетские сервисы часто создаются в сжатые сроки и интегрируются с внешними модулями, платежными сервисами, формами регистрации и устаревшими базами данных. OWASP Top 10 выделяет критические классы дефектов веб-безопасности, такие как нарушения контроля доступа, криптографические ошибки, инъекции и ошибки конфигурации. Эти риски особенно актуальны для вузов, так как публичные сервисы доступны широкому кругу пользователей и могут подвергаться пиковым нагрузкам [7].

Четвертая группа угроз связана с утечками персональных данных. В университетах обрабатываются паспортные данные, сведения о документах об образовании, контактная информация, данные о работниках, информация о проживании в общежитиях и результаты обучения. В открытых сообщениях отмечается рост утечек персональных данных в российских вузах; среди причин

называются устаревшая и разнородная инфраструктура, активное использование внешних сервисов и недостаточная осведомленность пользователей. Это подтверждает необходимость внедрения процессного управления персональными данными, минимизации выгрузок и контроля прав доступа [8].

Модель управления рисками

Для университетов предлагается циклическая модель управления кибербезопасностью, включающая шесть этапов: инвентаризация активов и данных; построение модели угроз; оценка рисков; выбор и внедрение мер защиты; мониторинг и реагирование; аудит, обучение и улучшение. Модель ориентирована на постоянное обновление, поскольку состав пользователей, информационных систем и внешних сервисов в вузе меняется каждый семестр.

Рисунок 1 – Цикл управления кибербезопасностью информационных систем университета

Для первичного ранжирования рисков может использоваться экспертная оценка по формуле:

$$R_i = (P_i \times D_i \times V_i) / K_i \quad (1)$$

где R_i – интегральный балл i-го риска; P_i – вероятность реализации угрозы; D_i – ожидаемый ущерб; V_i – степень уязвимости актива; K_i – коэффициент готовности мер защиты. Показатели оцениваются по шкале от 1 до 5. Формула не заменяет детальный аудит, но позволяет определить первоочередные направления работ [10].

Рекомендации по повышению киберустойчивости

Первым приоритетом должно стать централизованное управление идентификацией пользователей. Каждая учетная запись – будь то студента, сотрудника, внешнего преподавателя или подрядчика – должна иметь четко определенного владельца, установленный срок действия, назначенную роль и обоснование доступа. В случае отчисления, увольнения, завершения договора или окончания проекта права доступа должны автоматически отзывать или аннулироваться по контролируемой заявке. Для критически важных систем необходимо внедрить многофакторную аутентификацию, а для администраторов – использовать отдельные привилегированные учетные записи с обязательным журналированием их действий.

Вторым приоритетом является защита от вредоносного программного обеспечения и обеспечение возможности восстановления. Следует организовать централизованное управление обновлениями, защиту конечных точек, запрет на предоставление локальных администраторских прав без необходимости, сегментацию сети и резервное копирование с учетом независимости от основной инфраструктуры. Для критически важных сервисов необходимо установить целевые показатели времени восстановления и допустимой потери данных. Регулярная проверка резервных копий на практике является обязательной, иначе они не могут считаться надежным средством обеспечения непрерывности [9].

Третьим приоритетом следует сделать безопасность веб-сервисов и электронной образовательной среды. Перед запуском нового сервиса необходимо удостовериться в соответствии требованиям к ролям, журналированию, защите от распространенных веб-уязвимостей и планам восстановления. В процессе эксплуатации следует проводить сканирование на уязвимости, контроль конфигурации, ограничение доступа к административным интерфейсам, защиту от автоматизированных атак и мониторинг доступности. В период приемной кампании целесообразно заранее проводить нагрузочное тестирование и готовить резервные сценарии для публикации информации.

Четвертым приоритетом является защита персональных данных и работа с поставщиками. Университету следует вести карту обработки персональных

данных, минимизировать ненужные выгрузки, ограничивать использование внешних облачных хранилищ, включать требования безопасности в контракты, проверять порядок уведомления об инцидентах и учитывать риски интеграций. При переходе на отечественное программное обеспечение важно оценивать не только происхождение продукта, но и зрелость его сопровождения, совместимость, безопасность миграции данных и квалификацию администраторов.

Организационное обеспечение

Эффективная кибербезопасность невозможна без четкого распределения ответственности среди всех участников процесса. Руководство университета устанавливает общую политику и выделяет необходимые ресурсы; служба информационной безопасности формулирует требования, проводит оценку рисков и организует реагирование на инциденты; ИТ-подразделение отвечает за внедрение и поддержку технических средств защиты; владельцы информационных систем определяют состав данных и роли пользователей; юридическая служба следит за соблюдением законодательства в области обработки персональных данных; руководители подразделений обеспечивают соблюдение дисциплины среди пользователей. Такой подход позволяет избежать ситуации, когда безопасность воспринимается исключительно как задача системных администраторов [11].

Для оценки эффективности кибербезопасности следует использовать измеримые показатели, такие как: доля систем, зарегистрированных в реестре активов; процент критически важных сервисов, использующих многофакторную аутентификацию; количество привилегированных учетных записей без назначенного владельца; среднее время устранения критических уязвимостей; доля систем с проверенной возможностью восстановления; процент пользователей, прошедших обучение по вопросам безопасности; количество незакрытых исключений из политики безопасности; среднее время обнаружения и реагирования на инциденты. Эти показатели должны регулярно обсуждаться

на уровне комиссии по информационной безопасности или комитета по цифровой трансформации.

Обсуждение

Предложенная модель учитывает специфику российских университетов, включая нормативные требования, открытость образовательной среды, разнообразие пользователей, ограниченные ресурсы, разнородность систем и зависимость от внешних сервисов. Ее основное преимущество заключается в интеграции обязательных законодательных требований с практиками управления рисками. Вместо изолированной закупки отдельных средств защиты модель связывает активы, угрозы, владельцев процессов, меры контроля и показатели зрелости.

Тем не менее, исследование имеет свои ограничения, поскольку выводы носят обобщенный характер. Риски, связанные с техническим университетом, имеющим множество лабораторных серверов, существенно отличаются от рисков гуманитарного вуза, где большее внимание уделяется электронным курсам и документам. Федеральный университет с филиалами сталкивается с более сложными задачами сегментации и мониторинга по сравнению с небольшим институтом. Поэтому предложенная модель требует адаптации на основе анализа конкретной организации, ее информационных систем, состава данных и ключевых образовательных процессов.

Заключение

Кибербезопасность информационных систем российских университетов должна рассматриваться как непрерывный управленческий процесс, интегрированный в образовательные, научные и административные практики. К основным рискам относятся фишинг и компрометация учетных записей, вредоносное программное обеспечение, уязвимости веб-сервисов, утечки персональных данных, внутренние нарушения и риски, связанные с внешними поставщиками. Для их минимизации необходимо не только внедрение технических решений, но и четкое распределение ответственности, регулярное

обучение пользователей, контроль за жизненным циклом учетных записей и готовность к восстановлению после инцидентов.

Практическая ценность данной работы заключается в предложении модели, которая может служить основой для первичного аудита и разработки программы кибербезопасности в университете. В качестве первоочередных мер рекомендуется провести инвентаризацию активов, обеспечить централизованное управление идентификацией, внедрить многофакторную аутентификацию для ключевых ролей, организовать резервное копирование с тестированием восстановления, сегментировать сеть, контролировать уязвимости веб-приложений, управлять привилегированным доступом, оценивать поставщиков и разработать набор измеримых показателей зрелости. Реализация этих мер позволит университетам перейти от реактивного реагирования на инциденты к проактивной стратегии управления киберустойчивостью.

Библиографический список

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31. – Ст. 3448.

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31. – Ст. 3451.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. – № 31. – Ст. 4736.

4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.

5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. – URL: https://fstec.ru (дата обращения: 14.06.2026).

6. Национальный координационный центр по компьютерным инцидентам. Официальный сайт [Электронный ресурс]. – URL: https://cert.gov.ru (дата обращения: 14.06.2026).
7. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg: NIST, 2024. – DOI: 10.6028/NIST.CSWP.29.
8. OWASP Foundation. OWASP Top Ten Web Application Security Risks [Электронный ресурс]. – URL: https://owasp.org/www-project-top-ten/ (дата обращения: 14.06.2026).
9. «Информзащита»: у вузов стали чаще утекать персональные данные // ТАСС. – 2025. – 22 августа [Электронный ресурс]. – URL: https://tass.ru/ekonomika/24844239 (дата обращения: 14.06.2026).
10. Куценко, С. М. Кибербезопасность в цифровой экономике // Экономика и предпринимательство. - 2025. - № 1(174). - С. 130-132. - DOI 10.34925/EIP.2024.174.1.021
11. Куценко С. М., Салтанаева Е. А. Современные вызовы кибербезопасности и системы обнаружения вторжени // Экономика и предпринимательство. - 2025. - №6(179). - С. 950-954—DOI 10.34925/EIP.2025.179.6.170.

References

1. Federal Law No. 149-FZ of July 27, 2006 “On Information, Information Technologies and Information Protection”.
2. Federal Law No. 152-FZ of July 27, 2006 “On Personal Data”.
3. Federal Law No. 187-FZ of July 26, 2017 “On the Security of Critical Information Infrastructure of the Russian Federation”.
4. Government of the Russian Federation. Resolution No. 1119 of November 1, 2012 “On Approval of Requirements for Personal Data Protection in Personal Data Information Systems”.
5. FSTEC of Russia. Order No. 17 of February 11, 2013. Available at: https://fstec.ru (accessed June 14, 2026).
6. FSTEC of Russia. Order No. 21 of February 18, 2013. Available at: https://fstec.ru (accessed June 14, 2026).

7. Ministry of Science and Higher Education of the Russian Federation. Order No. 840 of September 7, 2021.
8. National Coordination Center for Computer Incidents. Official website. Available at: https://cert.gov.ru (accessed June 14, 2026).
9. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, NIST, 2024. DOI: 10.6028/NIST.CSWP.29.
10. OWASP Foundation. OWASP Top Ten Web Application Security Risks. Available at: https://owasp.org/www-project-top-ten/ (accessed June 14, 2026).
11. Lallie H.S., Thompson A., Titis E., Stephens P. Understanding cyber threats against the universities, colleges, and schools. Computers, 2025, vol. 14, no. 2, article 49. DOI: 10.3390/computers14020049.
12. Solar JSOC. Cyberattacks on Russian companies in 2024: analytical report. Available at: https://rt-solar.ru/analytics/reports/5320/ (accessed June 14, 2026).
13. Informzashchita: personal data leaks in universities have become more frequent. TASS, August 22, 2025. Available at: https://tass.ru/ekonomika/24844239 (accessed June 14, 2026).
14. Kutsenko, S. M. Cybersecurity in the Digital Economy // Economics and Entrepreneurship. - 2025. - Nº 1(174). - C. 130-
132. - DOI 10.34925/EIP.2024.174.1.021
15. Kutsenko S. M., Saltanaeva E. A. Modern Challenges of Cybersecurity and Intrusion Detection Systems / S. M. Kutsenko, // Economics and Entrepreneurship. - 2025. - Nº6(179). - C. 950-954. DOI 10.34925/EIP.2025.179.6.170.