УДК 34

Правовые и организационные проблемы обеспечения сетевой безопасности в образовательных организациях: пути совершенствования управления и нормативного регулирования

Хаджиева Лаура Куйраевна

Старший преподаватель,
кафедра Информатика и вычислительная техника,
Грозненский государственный нефтяной технический университет
им. академика М.Д. Миллионщикова,
364051, Российская Федерация, Грозный, пр. Исаева, 100;
e-mail: laura.hadjieva3009@mail.ru

Чадаев Ахмед Куйраевич

Студент,
Грозненский государственный нефтяной технический университет
им. академика М.Д. Миллионщикова,
364051, Российская Федерация, Грозный, пр. Исаева, 100;
e-mail: khadjiev.a@mail.ru

Аннотация

В последние годы управление сетевой безопасностью в колледжах и университетах сталкивается с растущими вызовами, включая появление «зон неконтролируемых рисков», что снижает эффективность защиты информационной инфраструктуры образовательных организаций. Целью данного исследования является анализ текущего состояния правового и технического регулирования сетевой безопасности в вузах, а также выявление ключевых проблем, связанных с нормативным обеспечением, межведомственным взаимодействием и управлением киберрисками. В статье применяется системный подход, основанный на анализе законодательства в сфере информационной безопасности, а также практики его применения в образовательных учреждениях. Научная новизна исследования заключается в разработке механизмов преодоления правовых и организационных пробелов, включая предложения по совершенствованию нормативной базы, созданию скоординированной системы управления с четким распределением ответственности и оптимизацией взаимодействия между структурными подразделениями. Практическая значимость работы заключается в том, что предлагаемые решения направлены на укрепление соответствия деятельности вузов требованиям законодательства о защите информации, а также на повышение эффективности реагирования на киберинциденты. Результаты исследования могут быть использованы для разработки комплексных правовых и организационных мер по обеспечению сетевой безопасности в образовательной сфере.

Для цитирования в научных исследованиях

Хаджиева Л.К., Чадаев А.К. Правовые и организационные проблемы обеспечения сетевой безопасности в образовательных организациях: пути совершенствования управления и нормативного регулирования // Вопросы российского и международного права. 2025. Том 15. № 3А. С. 344-350.

Ключевые слова

Правовое регулирование, сетевая безопасность, колледжи и университеты, управление, интеллектуализация университетов.

Введение

Современные образовательные организации, являясь важнейшими элементами цифрового пространства, сталкиваются с растущими угрозами в сфере сетевой безопасности. Активное внедрение информационных технологий в учебный процесс, развитие дистанционного образования и увеличение объемов обрабатываемых персональных данных делают университеты и колледжи потенциальными мишенями для кибератак. При этом существующие системы управления информационной безопасностью зачастую не успевают адаптироваться к быстро меняющемуся ландшафту угроз, что создает серьезные правовые и организационные риски.

Правовое регулирование вопросов кибербезопасности в образовательной сфере остается фрагментарным и не всегда соответствует современным вызовам. Несмотря на наличие базовых нормативных актов, таких как Федеральный закон «О безопасности критической информационной инфраструктуры» и Федеральный закон «О персональных данных», их практическая реализация в вузах сталкивается с рядом системных проблем. К ним относятся: отсутствие четкого разграничения ответственности между структурными подразделениями, недостаточная координация между образовательными учреждениями и регуляторами, а также нехватка специализированных правовых механизмов, учитывающих специфику учебных заведений.

Организационные трудности усугубляются такими факторами, как ограниченное финансирование мер защиты информации, дефицит квалифицированных кадров в области информационной безопасности и слабая интеграция технологических решений с правовыми требованиями. Особую озабоченность вызывает рост числа инцидентов, связанных с утечками персональных данных студентов и преподавателей, а также с атаками на научно-исследовательские базы данных, что ставит под угрозу не только конфиденциальность информации, но и академическую репутацию учреждений.

В данном контексте возникает острая необходимость в разработке комплексного подхода к совершенствованию управления сетевой безопасностью в образовательных организациях. Такой подход должен включать как модернизацию нормативной базы с учетом отраслевой специфики, так и оптимизацию организационных структур, ответственных за защиту информации. Особое значение приобретает создание эффективных механизмов межведомственного взаимодействия, развитие системы мониторинга киберугроз и внедрение стандартизированных протоколов реагирования на инциденты.

Целью настоящего исследования является анализ ключевых правовых и организационных проблем обеспечения сетевой безопасности в образовательных учреждениях и разработка

практических рекомендаций по совершенствованию системы управления киберрисками. В работе использованы методы сравнительно-правового анализа, системного подхода и изучения лучших практик организации защиты информации в образовательной сфере. Научная новизна исследования заключается в предложении конкретных механизмов модернизации нормативного регулирования и организационных структур с учетом современных вызовов цифровой эпохи.

Практическая значимость работы определяется возможностью применения ее результатов для разработки ведомственных актов и методических рекомендаций по защите информационной инфраструктуры образовательных организаций. Предлагаемые решения направлены на создание сбалансированной системы управления рисками, сочетающей правовые, организационные и технические аспекты, что в конечном итоге будет способствовать повышению уровня кибербезопасности в сфере образования.

Основное содержание

В целом, текущее состояние безопасности сетей в колледжах и университетах в основном характеризуется следующими проблемами.

Во-первых, в колледжах и университетах наблюдается общая нехватка профессиональных и технических управленческих кадров. С одной стороны, существует острое противоречие между все более сложной работой по управлению сетевой безопасностью и нехваткой профессионального и технического персонала [Гордейчик, www...]; с другой стороны, частая смена должностных обязанностей персонала в различных подразделениях колледжей и университетов затрудняет эффективное наследование и продолжение предыдущего ценного опыта работы и технических накоплений.

В то же время другие сотрудники отдела управления информацией имеют свои собственные сильные стороны в области технологий сетевой безопасности, но из-за отсутствия эффективного механизма интеграции они не могут в полной мере использовать эти возможности и ресурсы [Щеглов, 2015].

Во-вторых, в колледжах и университетах до сих пор не сформирована система управления сетевой безопасностью. Отделу управления информацией необходимо направить большую часть своей энергии на создание общедоступных базовых платформ и общее управление информационными проектами. Значительная часть создания и управления веб-сайтом и системой может быть выполнена только самими вторичными подразделениями, и им часто не хватает достаточного понимания сетевых атрибутов ИТ-активов и угроз сетевой безопасности.

Исходя из этой ситуации, отдел управления информацией сталкивается с огромными проблемами в координации этих подразделений. Трудно сформировать единую систему управления сетевой безопасностью, и невозможно составить всеобъемлющий и систематизированный список задач по управлению сетевой безопасностью для всего учреждения. Невозможно эффективно реализовать работу по защите сетевой безопасности всего учебного заведения. Это в определенной степени увеличило риски сетевой безопасности на территории университета.

Например, строительство проекта сосредоточено только на функциях и игнорирует безопасность, развертывает «двойные не-» системы для обхода управления учреждением, управляющие активами часто меняются и передают не в полном объеме, уязвимости не устраняются вовремя, исправления не обновляются вовремя, системы не очищаются, а бездействующие активы не восстанавливаются [Одам, 2014]. Эти проблемы не только

негативно сказываются на работе систем информационной и сетевой безопасности, но и открывают возможности для преднамеренных атак [Шаньгин, 2008].

В-третьих, сложно получить своевременную и точную общую информацию об активах. Колледжи и университеты не могут полностью понять информацию об активах из-за неясной финансовой информации, а некоторые даже имеют неверную и устаревшую информацию об активах [Лаборатория защиты, www...]. Это сильно влияет на точность оценки истинного состояния сетевой безопасности, затрудняя формулирование своевременных, эффективных и надежных стратегий защиты, тем самым усугубляя риски безопасности, такие как подделка контента, утечка данных и компрометация интрасети.

В-четвертых, работа по обеспечению сетевой безопасности в колледжах и университетах сложна, и повысить эффективность работы трудно. Прежде всего, в повседневной работе по обеспечению сетевой безопасности возникают такие проблемы, как разрозненные, неполные и непоследовательные записи, что приводит к низкой эффективности работы, большим затратам времени и труда, а также невозможности эффективного обобщения опыта работы.

Во-вторых, большая часть оборудования сетевой безопасности, добавленного в процессе построения сетевой безопасности в колледжах и университетах, находится в изолированном рабочем состоянии, что требует его проверки по отдельности при возникновении инцидентов безопасности, что серьезно влияет на эффективность обработки инцидентов [Шаньгин, 2017]. Кроме того, некоторые университеты постепенно усилили управление ИТ-активами с точки зрения административного управления и включили работу по сетевой безопасности в показатели оценки вторичных подразделений. Хотя это увеличило внимание, уделяемое работе по сетевой безопасности различными подразделениями, это также увеличило рабочую нагрузку и расходы на связь вторичных подразделений [Гладкий, 2012].

В целом, колледжи и университеты еще не сформировали стандартизированную и систематическую систему процессов для управления сетевой безопасностью. Механизм координации между управлением сетевой безопасностью и технической профилактикой немного слаб, что затрудняет формирование сильного синергетического эффекта [Мельников, Клейменов, Петраков, 2019]. Отсутствует эффективная комплексная система управления сетевой безопасностью, что делает колледжи и университеты несколько бессильными при решении проблем сетевой безопасности.

Идеи создания платформы.

В ответ на такие проблемы, как недостаточный уровень управления ИТ-активами, несвоевременное и неточное обслуживание информации об активах, отсутствие записей о работе по сетевой безопасности, изолированное оборудование безопасности, которое невозможно связать, и разрозненные возможности технологий безопасности, которые невозможно интегрировать, создается комплексная платформа управления сетевой безопасностью для колледжей и университетов, основанная на управлении полным жизненным циклом ИТ-активов [Олифер, Олифер, 2016]. Общая идея построения платформы заключается в следующем.

1. Заложить прочную основу для цифровой трансформации управления сетевой безопасностью и реализовать управление полным жизненным циклом ИТ-активов. С помощью технических средств мы подключаемся к платформам виртуальных машин, хостам-бастионам, платформам реагирования на безопасность терминалов и другим каналам, интеллектуально собираем информацию об активах, проводим углубленный статистический анализ активов, всесторонне и точно представляем панорамный вид ИТ-активов, углубляем усовершенствованное управление ИТ-активами, способствуем эффективному сотрудничеству

между несколькими людьми, бесперебойному обмену информацией и эффективной передаче работы, а также способствуем значительному повышению эффективности управления сетевой безопасностью.

2. Усилить управление процессами сетевой безопасности и создать полный журнал работ по сетевой безопасности. Платформа связана с существующим процессом онлайн-обслуживания, интегрируя и структурируя записи различных ежедневных журналов работы по сетевой безопасности.

3. Создать единый модуль совместной работы по обеспечению безопасности сети, чтобы обеспечить удобный доступ к работе по обеспечению безопасности сети для вторичных подразделений [Беленькая, Малиновский, Яковенко, 2011]. Каждое вторичное подразделение может интуитивно понимать профиль ИТ-активов, конфигурацию персонала службы безопасности, а также статус отчетности об инцидентах безопасности и статус их устранения своего подразделения, тем самым способствуя бесперебойной связи и эффективной координации информации о безопасности сети, снижая административную нагрузку, формируя объединенные силы для совместного создания барьера безопасности сети и обеспечивая безопасность и стабильность сетевой среды университета.

4. Интеграция сил технологий безопасности для повышения эффективности и уровня автоматизации работы по обеспечению безопасности сети. Создать шлюз веб-безопасности, который позволит осуществлять мониторинг образовательных веб-сервисов, собирать данные и функции общего оборудования безопасности и платформ управления, а также создать центр управления и контроля сетевой безопасности.

Заключение

С правовой точки зрения, приоритетным направлением является внедрение интеллектуальных и автоматизированных систем управления, что позволит:

– Минимизировать субъективный человеческий фактор в соответствии с требованиями п. 3 ст. 16 Федерального закона "Об информации, информационных технологиях и о защите информации";
– Обеспечить соответствие принципам эффективности и точности управления, установленным отраслевыми стандартами информационной безопасности;
– Сократить операционные риски, связанные с ручным вмешательством.

Заключение

Таким образом, по мере того как конструкция платформы становится все более совершенной, а ее приложения постепенно развертываются, посредством непрерывной итерации может быть постепенно сформирована устойчивая модель НИОКР, в которой уровни технологий и управления способствуют друг другу, а функциональные модули могут быть дополнительно обогащены и улучшены на основе ежедневных сценариев работы по обеспечению безопасности сети.

Необходимо постараться внедрить интеллектуальное и автоматизированное управление, чтобы сократить ручное вмешательство и повысить эффективность и точность управления безопасностью сети. Продолжать совершенствовать систему защиты сетевой безопасности, рассмотреть возможность дальнейшей интеграции функций управления безопасностью данных в платформу и улучшить общие возможности защиты безопасности платформы. Кроме того, укреплять кросс-отраслевое сотрудничество с другими университетами, делиться опытом создания платформ и совместно решать проблемы сетевой безопасности.

Библиография

1. Беленькая М.Н., Малиновский С.Т., Яковенко Н.В. Администрирование и информационных системах. М.: Горячая линия-Телеком, 2011. 400 с.
2. Владимир Шаньгин, Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2017. 544 с.
3. А. А. Гладкий // «Безопасность и анонимность работы в Интернете. Как защитить компьютер от любых посягательств извне» - 2012г. - С. 301-304.
4. Гордейчик С. // Cross-site request forgery [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/analytics/292473.php
5. Лаборатория защиты // Классификация угроз безопасности Web-приложений 2013 [Электронный ресурс]. - Режим доступа: http://www.f1consulting.ru/websec/classification/
6. Мельников В.П., С.А. Клейменов, А.М. Петраков //«Информационная безопасность и защита информации», - 2019г. - С. 184-186.
7. Олифер В.Г.. Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-ое. М.: Питер, 2016. 992 с.
8. Уэнделл Одам. CCNA. Официальное руководство но подготовке к сертификационным экзаменам. М,: Издательский дом «Вильяме». 2014. 736 с.
9. Шаньгин В.Ф. //«Информационная безопасность компьютерных систем и сетей», - 2008г. - С. 123-125.
10. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / Щеглов А.Ю. - СПб: Наука и Техника, 2015. - С. 89-91.

Legal and Organizational Challenges of Network Security in Educational Institutions: Improving Management and Regulatory Frameworks

Laura K. Khadzhieva

Senior Lecturer,
Department of Computer Science and Computing,
Grozny State Oil Technical University named
after Academician M.D. Millionshchikov,
364051, 100, Isaev ave., Grozny, Russian Federation;
e-mail: laura.hadjieva3009@mail.ru

Akhmed K. Chadaev

Student,
Grozny State Oil Technical University named
after Academician M.D. Millionshchikov,
364051, 100, Isaev ave., Grozny, Russian Federation;
e-mail: khadjiev.a@mail.ru

Abstract

In recent years, network security management in colleges and universities has faced growing challenges, including the emergence of "zones of uncontrolled risks," which reduces the effectiveness of protecting the information infrastructure of educational organizations. The purpose of this study is to analyze the current state of legal and technical regulation of network security in universities, as well as to identify key problems related to regulatory support, interdepartmental

interaction and cyber risk management. The article uses a systems approach based on the analysis of legislation in the field of information security, as well as the practice of its application in educational institutions. The scientific novelty of the study lies in the development of mechanisms for overcoming legal and organizational gaps, including proposals for improving the regulatory framework, creating a coordinated management system with a clear distribution of responsibilities and optimizing interaction between structural divisions. The practical significance of the work is that the proposed solutions are aimed at strengthening the compliance of universities with the requirements of legislation on information protection, as well as improving the effectiveness of response to cyber incidents. The results of the study can be used to develop comprehensive legal and organizational measures to ensure network security in the educational sphere.

For citation

Khadzhieva L.K., Chadaev A.K. (2025) Pravovye i organizatsionnye problemy obespecheniya setevoy bezopasnosti v obrazovatelnykh organizatsiyakh: puti sovershenstvovaniya upravleniya i normativnogo regulirovaniya [Legal and Organizational Challenges of Network Security in Educational Institutions: Improving Management and Regulatory Frameworks]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (3A), pp. 344-350.

Keywords

legal regulation, network security, colleges and universities, management, university intellectualization

References

1. Belenkaya, M. N., Malinovsky, S. T., & Yakovenko, N. V. (2011). Administrirovanie v informatsionnykh sistemakh [Administration in information systems]. Goryachaya liniya-Telekom. (Original work published 2011, 400 pp.)
2. Shangin, V. (2017). Zashchita kompyuternoy informatsii. Effektivnye metody i sredstva [Computer information protection: Effective methods and tools]. DMK Press. (Original work published 2017, 544 pp.)
3. Gladkiy, A. A. (2012). Bezopasnost i anonimnost raboty v Internete. Kak zashchitit kompyuter ot lyubykh posyagatelstv izvne [Security and anonymity of work on the Internet: How to protect your computer from any external intrusions] (pp. 301-304).
4. Gordeichik, S. (n.d.). Cross-site request forgery [Electronic resource]. SecurityLab. http://www.securitylab.ru/analytics/292473.php
5. Laboratoriya zashchity. (2013). Klassifikatsiya ugroz bezopasnosti Web-prilozheniy [Classification of web application security threats] [Electronic resource]. F1 Consulting. http://www.f1consulting.ru/websec/classification/
6. Melnikov, V. P., Kleymenov, S. A., & Petrakov, A. M. (2019). Informatsionnaya bezopasnost i zashchita informatsii [Information security and information protection] (pp. 184-186).
7. Olifer, V. G., & Olifer, N. A. (2016). Kompyuternye seti. Printsipy, tekhnologii, protokoly [Computer networks: Principles, technologies, protocols] (4th ed.). Piter. (Original work published 2016, 992 pp.)
8. Odom, W. (2014). CCNA. Ofitsialnoe rukovodstvo po podgotovke k sertifikatsionnym ekzamenam [CCNA: Official certification guide]. Vil'yams. (Original work published 2014, 736 pp.)
9. Shangin, V. F. (2008). Informatsionnaya bezopasnost kompyuternykh sistem i setey [Information security of computer systems and networks] (pp. 123-125).
10. Shcheglov, A. Yu. (2015). Zashchita kompyuternoy informatsii ot nesanktsionirovannogo dostupa [Protection of computer information from unauthorized access]. Nauka i Tekhnika. (Original work published 2015, pp. 89-91).