ПРОБЛЕМЫ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056.57

НЕКОТОРЫЕ ВОПРОСЫ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, СВЯЗАННЫЕ С ДЕЯТЕЛЬНОСТЬЮ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

Дмитриев Александр Александрович, Журавлева Виктория Владимировна, Поляков Виктор Владимирович

Алтайский государственный университет, Барнаул
dmitriev.542@gmail.com, torinka8@gmail.com, pvv@asu.ru

SOME ISSUES OF CRITICAL INFORMATION INFRASTRUCTURE PROTECTION RELATED TO THE ACTIVITIES OF HIGHER EDUCATION INSTITUTIONS

Dmitriev Alexander A., Zhuravleva Victoria V., Polyakov Viktor V.

Altai State University, Barnaul
dmitriev.542@gmail.com, torinka8@gmail.com, pvv@asu.ru

Аннотация. Рассмотрены различные аспекты деятельности вузов в сфере защиты критической информационной инфраструктуры. Выявлены и описаны особенности вузов как специфического представителя объектов этой инфраструктуры. Приведены примеры применения средств защиты компьютерных систем вуза от преступного посягательства. Описана типичная локальная информационная сеть крупного вуза. Установлены особенности подготовки специалистов, призванных обеспечивать защиту критической информационной инфраструктуры, и выработан ряд рекомендаций по повышению качества этой подготовки. Обращено внимание на значимость непрерывного повышения квалификации и переподготовки специалистов-практиков.

Ключевые слова: критическая информационная инфраструктура, информационная безопасность, средства защиты информации, учреждение высшего образования

Abstract. Various aspects of universities' activities in the field of critical information infrastructure protection are considered. The features of universities as a specific representative of the objects of this infrastructure are identified and described. Examples of the use of means to protect university computer systems from criminal encroachment are given. A typical local information network of a large university is described. The specifics of the training of specialists designed to protect critical information infrastructure have been identified, and a number of recommendations have been developed to improve the quality of this training. Attention is drawn to the importance of continuous professional development and retraining of practitioners.

Keywords: critical information infrastructure, information security, information security tools, institution of higher education

Для цитирования: *Дмитриев А.А., Журавлева В.В., Поляков В.В.* Некоторые вопросы защиты критической информационной инфраструктуры, связанные с деятельностью высших учебных заведений // Проблемы правовой и технической защиты информации. 2025. № 13. С. 7–11.

For citation: *Dmitriev A.A., Zhuravleva V.V., Polyakov V.V.* Some issues of critical information infrastructure protection related to the activities of higher education institutions. *Legal and Technical Problems of Information Security.* 2025. No. 13. P. 7–11.

Цифровая трансформация общественных отношений одним из негативных последствий имела появление качественно нового вида угроз. Среди этих угроз на одно из первых мест вышли неправомерные воздействия на критическую информационную инфраструктуру государства. В связи с высокой опасностью последствий такого воздействия в последние годы был разработан подробный комплекс мер по защите объектов такой инфраструктуры, включавшей как меры правового регулирования (прежде всего Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ[1]), так и широкий спектр мероприятий технического характера.

Особое место в государственной системе поддержания безопасности критической информационной инфраструктуры занимают вузы. Это обусловлено тем, что вузы выступают в двух различных качествах. Во-первых, вузы отнесены к организациям, попадающим в перечень объектов субъектов этой инфраструктуры. Обоснованность данного решения не вызывает сомнений и связана с важностью проводимых в вузах научных исследований, с использованием в научной деятельности наукоемких технологий и разработанных технологий в жизненно важные отрасли экономики и в сферы управления. Во-вторых, важнейшей задачей вузов является подготовка кадров, призванных обеспечивать защиту критической информационной инфраструктуры государства путем привлечения комплекса технических и организационно-методических мер, а также разрабатывать эффективные инновационные технологии и методы такой защиты. Кроме того, в связи со стремительным внедрением инновационных цифровых технологий во все сферы жизни общества вузы призваны обеспечивать систему непрерывной переподготовки и повышения квалификации специалистов по информационной безопасности, ответственных за поддержанием систем обеспечения защиты критической информационной инфраструктуры.

Рассмотрим ряд вопросов, относящихся к деятельности вузов с позиций функционирования систем критической информационной инфраструктуры.

1. Спецификой информационной системы современного вуза является обязательный доступ к ней большого числа студентов, преподавателей, сотрудников связанных с вузом организаций, а также необходимость обеспечения доступа к этой системе многочисленных внешних по отношению к вузу граждан. Это предъявляет повышенные требования к корпоративной информационной сети вуза и ее защищенности от внешних и внутренних угроз. Кроме того, необходимо учитывать весьма значительный (в крупных вузах — многотысячный) объем обрабатываемых и защищаемых персональных данных [1].

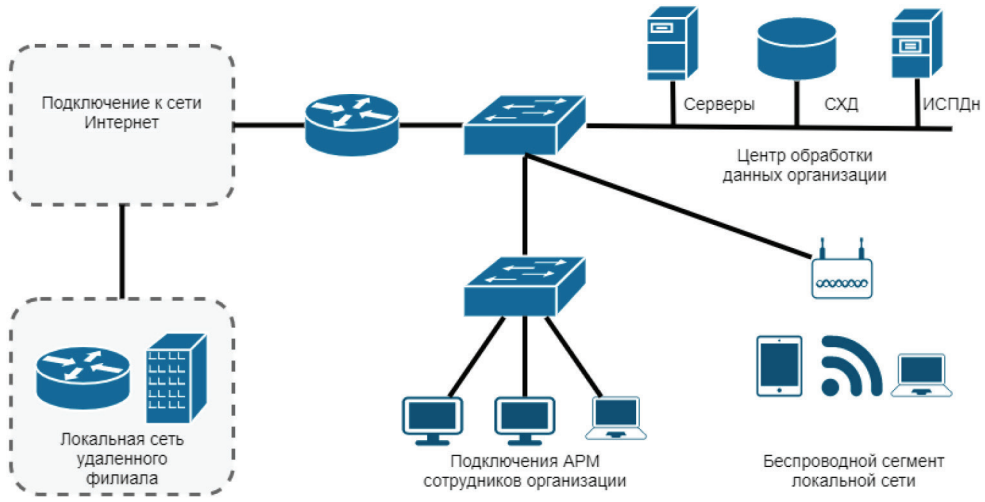
Прежде всего при организации защиты критической информационной структуры вуза необходимо учитывать специфику построения его локальной компьютерной сети [2]. Как правило, типичная корпоратив-

1 Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (с изменениями и дополнениями). URL: https://base.garant.ru/71730198/ (дата обращения: 26.03.2025).

ная сеть вуза основывается на основе применении архитектуры с выделением центрального маршрутизатора (обобщенная структура корпоративной сети приведена на рисунке). Этот маршрутизатор обеспечивает выход в сеть Интернет и доступ к внешним информационным ресурсам сотрудникам и учащимся, он же отвечает за сетевой трафик при подключении внешних пользователей [3]. Внутреннюю часть сети образуют автономные сегменты, объединяемые посредством виртуальных локальных сетей. Системы управления и базы данных, расположенные на специальных серверах, образуют отдельные подсети. Для контроля сетевого трафика применяются средства фильтрации доступа, настроенные на маршрутизаторе. Крупные вузы обычно имеют филиалы, расположенные в других городах. В этом случае возникает задача поддержания постоянной надежной связи с филиалами, что обеспечивается с помощью внешнего оператора связи.

Особая роль возлагается на защиту информационных ресурсов вуза от неправомерного воздействия злоумышленников [4]. Это, как правило, достигается традиционным способом — на основе применения антивирусного программного обеспечения отечественного производства. При организации защиты нужно учитывать, что вредоносным атакам подвергаются в первую очередь те сервера, которые предназначены для взаимодействия с внешними пользователями.

Полагаем также, что отдельно нужно отметить такие проблемы, как, во-первых, комплектование отделов защиты информации достаточным количеством профессионально компетентных и опытных сотрудников, во-вторых — обеспечение этих отделов самыми современными программными и программно-аппаратными средствами защиты компьютерной информации. В силу ограниченности возможностей успешность решения этих задач требует немалых финансовых и организационных усилий.



Типичная локальная сеть вуза

В связи с быстрой эволюцией программных средств, применяемых в преступных целях, для эффективной защиты вузовских объектов информатизации необходимо постоянно обновлять используемые программные и программно-аппаратные средства защиты информации. В качестве центрального маршрутизатора может быть рекомендован межсетевой экран Usergate E1000, предоставляющий возможность фильтрации сетевого трафика. Для подключения к сети вуза удаленных филиалов целесообразно при-

менение комплекса ПАК ViPNet Coordinator HW100. Контроль событий и возможных компьютерных инцидентов путем применения специализированного программного обеспечения Zabbix.

Отметим также важность постоянного контроля изменяющихся рисков критической информационной инфраструктуры [5, 6] и целесообразность разработки прогностической модели защиты компьютерных систем вуза от внешних и внутренних угроз.

Кроме того, необходимо постоянно контролировать соблюдение правил защиты информационных ресурсов при внутреннем доступе к ним со стороны сотрудников и студентов, проводить обучение и тренинги этих пользователей по соблюдению требований информационной безопасности.

2. Для эффективного обеспечения защиты различных объектов критической информационной инфраструктуры необходимо развивать и совершенствовать подготовку специалистов соответствующего профиля. Эта задача является относительно новой и ее решение находится в стадии становления. Представляется, что кроме общих знаний в сфере информационной безопасности такие специалисты должны владеть специфическими компетенциями, заключающимися в понимании специфики конкретных объектов критической информационной инфраструктуры, их общности и различий между ними, и. как следствие, в умении применить средства защиты, соответствующие охраняемому объекту [7]. В то же время развитие у студентов соответствующих компетенций проводится в соответствии с устоявшимися Федеральными образовательными стандартами, полностью регламентирующими подготовку специалистов по информационной безопасности, в которых эти компетенции в связи с новизной задачи представлены явно не в полной мере.

Формирование соответствующих знаний и умений требует разработки новых образовательных компонентов, которые должны претворяться в новых учебных дисциплинах [8, 9]. В качестве примера, целесообразно ввести в учебный процесс дисциплины, обеспечивающие учащихся компетенциями в сфере методов искусственного интеллекта и возможности его использования в задачах защиты информации. Представляется также целесообразным формирование у будущих специалистов знаний о тех приемах, методах и технологиях, которые применяются в преступных целях, и способам противодействия преступным посягательствам, направленным против критической информационной инфраструктуры.

При реализации основных образовательных программ и программ дополнительного профессионального образования должны учитываться передовые разработки в сфере высшего образования и хорошо зарекомендовавшие себя новые подходы [10, 11]. К ним можно отнести практикоориентированность обучения, интердисциплинарный подход, использование методов проектного обучения [12, 13]. Важное значение имеет также формирование адаптации к условиям усиливающихся информационных войн.

Рассматривая вопросы подготовки специалистов по защите критической информационной инфраструктуры различных объектов, нужно подчеркнуть особую роль деятельности вузов по повышению квалификации специалистов-практиков [14]. Новой особенностью этой деятельности, отвечающей вызовам времени, является реализация концепции непрерывного повышения квалификации. Только такая система подготовки и переподготовки кадров может обеспечить соответствие уровня профессиональных компетенций возрастающим угрозам и быстрым изменением в сфере цифровых технологий. Именно этим целям служит программа профессиональной переподготовки «Информационная безо-

пасность. Безопасность значимых объектов критической информационной инфраструктуры», базовые принципы которой были разработаны специалистами ФСТЭК России. Отметим, что на практике при повышении квалификации и переподготовке определенную сложность создает учет специфики конкретного объекта критической информационной инфраструктуры (например, организации здравоохранении, финансовой организации, промышленного предприятия, транспорта и т.п.).

Рассмотренные в работе вопросы, описанные проблемы и предложенные рекомендации могут быть применены в сфере деятельности вузов по защите критической информационной инфраструктуры.

Библиографический список

1. Ромашкова О.Н., Каптере А.И. Анализ угроз и рисков информационной безопасности в вузе // Вестник МГПУ. 2023. № 1(63). С. 37–47.

2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ИНФРА-М, 2011. 416 с.

3. Дмитриев А.А., Дмитриев Д.А. Метод фильтрации трафика на основе анализа сетевых взаимодействий устройств // Проблемы правовой и технической защиты информации. 2023. № 11. С. 16–20.

4. Garber L. Denial-of-Service Attacks Rip the Internet // IEEE Computer. 2000. Vol. 33, Iss. 4. P. 12–17.

5. Вульфин, А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных: автореф. дис. ... д-ра техн. наук. Уфа, 2022. 36 с.

6. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные продукты и системы. 2016. № 3(115). С. 42–50.

7. Поляков В.В., Дмитриев А.А., Рудер Д.Д., Салита Д.С. Система непрерывной многоуровневой подготовки специалистов в сфере информационной безопасности. Современное профессиональное образование. 2025. № 4. С. 89–92.

8. Белов Е.Б., Лось В.П., Малюк А.А. Цифровая экономика и актуальные проблемы совершенствования системы подготовки кадров в области информационной безопасности // Безопасность информационных технологий. 2018. Т. 25, № 4. С. 6–22.

9. Поляков В.В., Журавлева В.В. Подготовка специалистов по информационной безопасности в условиях цифровой экономики / // Проблемы правовой и технической защиты информации. 2019. Вып. 7. С. 39–41.

10. Малюк А.А. Кадровое обеспечение инфор-мационной безопасности // Государственная служба. 2011. № 5. С. 75–79.

11. Микиденко Н.Л., Сторожева С.П., Струкова Е.Г. Кадровое обеспечение образовательных программ в области информационной безопасности: проблемы проектирования и развития // Вестник СибГУТИ. 2022. № 3(59). С. 84–100.

12. Сизов В.А., Малиничев Д.М., Кучмезов Х.Х., Мочалов В.В. Применение метода проблемного обучения в изучении дисциплины «Информационная безопасность» // Открытое образование. 2021. Т. 25, № 3. С 36–45.

13. Степанова О.М., Козлова Н.В., Крючков Ю.Ю., Соловьев М.А. Внедрение проблемно-ориентированных технологий в практику обучения студентов технических вузов // Известия Томского политехнического университета. 2006. Т. 309, № 1. С. 242–246.

14. Малюк А.А., Малюк З.П. Актуальные вопросы создания системы массового обучения культуре информационной безопасности // Безопасность информационных технологий. 2021. № 28(4). С. 6–21.