ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОГО ОБЩЕСТВА

Научная статья
УДК 37.07:004.056
DOI: 10.17853/2587-6910-2024-15-70-77

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

Ольга Александровна Караулова
старший преподаватель o.karaulova@psuti.ru ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, Самара

Наталья Валерьевна Киреева
кандидат технических наук, доцент n.kireeva@psuti.ru ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия, Самара

Аннотация. Для успешной реализации образовательного процесса и подготовки высококвалифицированных специалистов необходимо использовать современные цифровые информационные технологии и системы. При этом важной задачей является правильная организация учебного процесса с учетом современных подходов и киберугроз. Использование современных средств защиты на различных уровнях образовательного процесса с учетом контингента и решаемых задач является приоритетным направлением в обеспечении информационной безопасности информационных систем и учебного процесса университета, а также для обеспечения безопасности персональных данных сотрудников и студентов. В статье рассматриваются приоритетные задачи и подход для обеспечения информационной безопасности информационной системы вуза.

Ключевые слова: несанкционированный доступ, система, процесс, киберугрозы, образовательная организация

Для цитирования: Караулова О. А., Киреева Н. В Вопросы обеспечения информационной безопасности в образовательном учреждении // Новые информационные технологии в образовании и науке. 2024. № 3 (15). С. 70-77 https://doi.org/10.17853/2587-6910-2024-15-70-77

ISSUES OF ENSURING INFORMATION SECURITY IN AN EDUCATIONAL INSTITUTION

Olga Aleksandrovna Karaulova
Povolzhskiy State University of Telecommunication and Informatics, Russia, Samara

Natalya Valeryevna Kireeva
Povolzhskiy State University of Telecommunication and Informatics, Russia, Samara

Abstract For the successful implementation of the educational process and the training of highly qualified specialists, it is necessary to use modern digital information technologies and systems. At the same time, an important task is the correct organization of the educational process, taking into account modern approaches and cyber threats. The use of modern means of protection at various levels of the educational process, taking into account the population and the tasks being solved, is a priority in ensuring the information security of information systems and the educational process of the university, as well as in ensuring the security of personal data of employees and students. The article discusses the priority tasks and approach to ensuring information security of a university information system.

Keywords: unauthorized access, system, process, cyber threats, educational organization

For citation: Karaulova OA, Kireeva NV. Issues of ensuring information security in an educational institution *New information technoljgies in tducftion and science*. 2024;3(15): 70-77. (In Russ.). doi:10.17853/2587-6910-2024-15-70-77

为了成功实施教育过程和培养高素质专门人才，必须使用现代数字信息技术和系统。**重要的是使用**现代方法组织教育过程并考虑到网络威胁。教育过程各个层面的现代化保护手段对于保证教育过程的信息安全和保护大学员工和学生的个人数据具有重要意义。**文章探**讨了保障高校信息系统信息安全的办法和**重点任**务。

Введение

В современных реалиях очень важным и актуальным является вопрос обеспечения информационной безопасности в образовательной организации высшего образования, как важного этапа в становлении мировоззрения и гражданской позиции молодежи.

Когда встает вопрос об обеспечении информационной безопасности, то, как правило, наибольшее внимание уделяется средствам технического обеспечения безопасности. Но данный вопрос гораздо шире.

Если говорить об угрозах информационной безопасности в образовательных учреждениях, то нужно учитывать следующие угрозы:

- несанкционированный доступ к информационным данным;
- защита и отсеивание нежелательной информации;
- проблемы общения в социальных сетях;
- кибератаки.

Литературный обзор

Обеспечение информационной безопасности в образовательных учреждениях — одна из ключевых задач цифровой трансформации. Современные вызовы, связанные с киберугрозами, требуют применения организационных, технических и правовых методов защиты. Анализ научных исследований и методических рекомендаций, посвященных данной проблематике, показывает актуальность и своевременность рассмотрения комплексных подходов к обеспечению безопасности, включая политику информационной безопасности, использование передовых технологий защиты данных и повышение уровня киберграмотности среди студентов и сотрудников образовательных учреждений.

Согласно исследованию Киреевой Н. В., Поздняка И. С. и Салмина А. А. [1], ключевыми угрозами для образовательных учреждений являются:

- несанкционированный доступ к данным;
- кибератаки на университетские серверы;
- фишинговые атаки и социальная инженерия;
- вредоносное ПО и утечка персональных данных.

Ромашкова О. Н. и Каптерев А. И. [2] отмечают, что низкая цифровая грамотность персонала и студентов увеличивает риск реализации киберугроз. Кроме того, отсутствие централизованной политики защиты информации усугубляет ситуацию.

Анализ международного опыта по обеспечению кибербезопасности в образовательной сфере, представленный в исследованиях [10; 11], подтверждает важность внедрения комплексных стратегий защиты информационных систем.

Методические рекомендации Л. Л. Тимофеевой [3] предлагают внедрение следующих мер:

- проведение регулярного аудита безопасности;
- контроль доступа к информационным ресурсам;
- разработка политики управления инцидентами информационной безопасности.

Согласно Виннику Е. А. [6], для защиты образовательных систем рекомендуется:

- использование сертифицированного программного обеспечения;
- ограничение применения личных устройств в университетской сети;
- внедрение систем мониторинга сетевой активности.

В публикации SearchInform [4] анализируется эффективность использования DLP-систем, межсетевых экранов и SIEM-решений для защиты университетских информационных систем.

Дополнительно в международных источниках [10; 11] рассматриваются передовые технологии защиты образовательных учреждений, включая комплексные системы управления информационной безопасностью (ISMS) и современные инструменты анализа угроз.

Согласно рекомендациям Центра информационной безопасности [5], образовательные учреждения должны соблюдать федеральные стандарты защиты персональных данных и учитывать международный опыт в области кибербезопасности.

Основные проблемы, выявленные в ходе анализа источников:

- недостаточное финансирование программ информационной безопасности [2];
- использование устаревшего ПО и слабая защита серверов университетов [3];
- неосведомленность персонала о современных угрозах и методах их предотвращения [8].

Перспективными направлениями являются внедрение системы риск-менеджмента в цифровой образовательной среде [10] и повышение уровня осведомленности пользователей [7; 11].

Обзор представленных исследований показывает, что обеспечение информационной безопасности в образовательных учреждениях требует комплексного подхода. Внедрение организационных, технических и правовых механизмов, а также повышение цифровой грамотности студентов и сотрудников являются ключевыми аспектами эффективной защиты информационных систем вузов. Международный опыт [10; 11] демонстрирует важность интеграции передовых технологий и стратегии киберустойчивости в систему высшего образования.

Методология

Рассмотрим данные угрозы по порядку. При оценке несанкционированного доступа к различным типам данных нужно учитывать особенности данных в образовательном учреждении. Это могут быть изменение информации в журналах, ведомостях, зачетных книжках и студенческих билетах, внесение несанкционированных данных, уничтожение или похищение информации о паспортных данных, дате рождения, месте регистрации и т. д. Цифровое современное общество не может обходиться без информационных технологий, которые развивают общество и в то же время приводят к появлению и совершенствованию новых угроз безопасности. Это, в свою очередь, приводит к снижению личной безопасности физического лица и безопасности на государственном уровне. Мероприятия по защите от несанкционированного доступа в вузе позволяют обеспечить безопасность как личной, так и информации регионального/федерального значения. При этом всегда нужно учитывать, что никакие способы не гарантируют полную защиту информации, но применение криптографических методов шифрования, разграничение доступа к информации позволяет существенно снизить риск несанкционированного доступа к информации учебного заведения.

Фильтрация нежелательной информации прежде всего должна предотвращать распространение информации экстремистского характера, а также информации провокационного характера. Для этого используются как технические средства, так и организационные.

Еще одной важной проблемой является общение в социальных сетях. В современных условиях, когда манипуляция направлена на молодежь, очень важно донести, что нужно быть внимательным к собеседникам при общении, что нужно ограничить размещение личной информации и персональных данных и что твой собеседник может быть не тем, за кого себя выдает. К сожалению, в силу неопытности молодые люди более подвержены влиянию, поэтому в задачу учебного заведения входит информирование и максимальное разъяснение ситуаций, ведение просветительской работы, пояснение методов социальной инженерии.

Вопросы киберугроз решаются на уровне соответствующих ведомств, но и на уровне образовательных организаций можно проводить мероприятия по защите от киберугроз, особенно это касается создания безопасной информационной среды для обучающихся, так как в последнее время информационные системы высших учебных заведений все больше подвергаются кибератакам.

Результаты

Очень часто в образовательных организациях возникают проблемы с информационными ресурсами в связи с отсутствием обновлений, установкой нелицензионных программ, использованием личных ноутбуков студентов в информационной системе вуза, недостаточным финансированием.

Описанные проблемы требуют решения на всех уровнях. Одним из решений является возможность создания единой информационной платформы на базе вузов для обеспечения доступа преподавателей и студентов к ресурсам университета, взаимодействия внутри сети, и регулярные обновления программного обеспечения, и высокая квалификация специалистов по информатизации учебного заведения.

Другой возможностью решить вопрос обеспечения информационной безопасности является проведение регулярного аудита информационных систем в образовательной организации. Кроме этого, необходимо обратить внимание на организацию доступа в информационные системы, формирование паролей, отслеживание контингента.

Современные университеты содержат и обрабатывают огромное количество информации, используя для этого собственные информационные ресурсы, которыми пользуется большое количество постоянно меняющейся аудитории, которая, как правило, находится в возрасте, который входит в группу потенциальных нарушителей безопасности, и студенты могут «запросто» заблокировать выход в интернет, «наказать преподавателя», создать вирусную программу, чтобы продемонстрировать свои способности. Это накладывает дополнительные обязательства по обеспечению безопасности информационных ресурсов образовательной организации.

Все рассмотренные особенности требуют безотлагательного соблюдения определенных условий и требований:

- всестороннюю комплексную оценку и проработку задач обеспечения информационной безопасности в образовательной организации с учетом развития информационных систем и цифровых технологий;

- использование в управлении информационной системы вуза высококвалифицированных специалистов;
- необходимость применения сертифицированных приложений на модульной основе для обеспечения безопасного использования информационных ресурсов;
- обеспечение документооборота с учетом киберугроз и современных реалий;
- гибкость и масштабируемость технических и программно-аппаратных средств защиты информации.

Помимо указанных требований важной составляющей является управление операционной системой в образовательной организации, своевременное обновление и устранение недостатков и ошибок. Конечно, данные задачи характерны и для других областей деятельности, но именно в образовательной сфере их решение встает остро, в связи с особенностями аудитории, пользующейся информационными технологиями, и наличием большого количества различного программного обеспечения и информационных систем для решения задач в процессе образовательного процесса, а также внеучебного и удаленного использования.

Заключение

Таким образом, в качестве актуальных угроз информационной безопасности в вузе следует выделить:

- попытки несанкционированного доступа, в том числе удаленного;
- попытки взлома информационной системы университета;
- исследование сетей на предмет уязвимостей;
- несанкционированная установка нелицензионного или несертифицированного программного обеспечения и установка его на рабочие станции сети университета.

В качестве основных источников угроз выступают компьютерные аудитории учебного процесса, использование сети Интернет, личные ноутбуки студентов и преподавателей, некомпетентность при установке и настройки необходимого программного обеспечения.

Данные вопросы и задачи требуют серьезного подхода как в отдельно взятой образовательной организации, так и во всей образовательной сфере. Использование цифровых технологий и современной информационной среды в учебных заведениях высшего образования, обучение персонала и обучающихся, разработка результативной политики безопасности требуют незамедлительного, но бережного и внимательного отношения, с точки зрения информационной безопасности, так как именно вуз является гарантом формирования высококвалифицированных специалистов с высокими морально-этическими нормами.

Список источников

1. Киреева Н. В., Поздняк И. С., Салмин А. А. Вопросы реализации национальной программы «Цифровая экономика» в области информационной безопас-

ности // Наука. Информатизация. Технологии. Образование: материалы XV международной научно-практической конференции, Екатеринбург, 28 февраля – 04 марта 2022 г. Екатеринбург: Рос. гос. проф.-пед. ун-т, 2022. С. 201–210. URL: https://elar.rsvpu.ru/handle/123456789/40565 (дата обращения: 16.05.2024).

2. Ромашкова О. Н., Каптерев А. И. Анализ угроз и рисков информационной безопасности в вузе // Вестник МГПУ. Серия: Информатика и информатизация образования. 2023. № 1 (63). С. 37–47. https://doi.org/10.25688/2072-9014.2023.63.1.03.

3. Методические рекомендации по обеспечению информационной безопасности в образовательной организации / сост. Л. Л. Тимофеева. Орёл: Ин-т развития образования, 2020. 58 с. URL: https://xn--h1albh.xn--p1ai/wp-content/uploads/2021/06/Metodicheskie-rekomendacii-po-obespecheniju-informacionnoj-bezopasnosti-v-obrazovatelnoj-organizacii.pdf (дата обращения: 09.10.2024).

4. Информационная безопасность образовательных учреждений // СерчИнформ. URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/?utm_source=chatgpt.com (дата обращения: 09.10.2024).

5. Рекомендации по обеспечению информационной безопасности в образовательной организации // УИБ. URL: https://uibcom.ru/articles/informatsionnaya-bezopasnost/rekomendatsii-po-obespecheniyu-informatsionnoy-bezopasnosti-v-obrazovatelnoy-organizatsii-/?utm_source=chatgpt.com (дата обращения: 09.10.2024).

6. Винник Е. А. Обеспечение защиты информации в образовательных организациях // Молодой ученый. 2023. № 7 (454). С. 3–6. URL: https://moluch.ru/archive/454/100167/ (дата обращения: 09.10.2024).

7. Информационная безопасность детей в образовательной организации // ИКС. URL: https://xserver.a-real.ru/blog/useful/informatsionnaya-bezo8.pasnost-detey-v-obrazovatelnoy-organizatsii/?utm_source=chatgpt.com (дата обращения: 09.10.2024).

8. Cybersecurity Compliance in the Educational Services Sector: How to Protect Students' Personal Data. URL: https://www.syteca.com/en/blog/cybersecurity-in-educational-institutions?utm_source (дата обращения: 09.10.2024).

9. Cybersecurity for Educational Institutions. URL: https://www.cisecurity.org/industry/education?utm_source (дата обращения: 09.10.2024).

10. Sapanca H. F., Kanbul S. Risk management in digitalized educational environments: Teachers' information security awareness levels // Frontiers in Psychology. 2022. Vol. 13. P. 986561. https://doi.org10.3389/fpsyg.2022.986561.

11. Cybersecurity in Education levels. URL: https://www.intel.com/content/www/us/en/education/it-in-education/cyber-security.html?utm_source (дата обращения: 09.10.2024).

References

1. Kireeva NV, Pozdnyak IS, Salmin AA. Voprosy realizatsii natsional'noy programmy «Tsifrovaya ekonomika» v oblasti informatsionnoy bezopasnosti. *Nauka. Informatizatsiya. Tekhnologii. Obrazovanie: materialy XV mezhdunarodnoy nauchno-prakticheskoy konferentsii, Yekaterinburg, 28 fevralya – 04 marta 2022 g.* Yekaterinburg:

Rossiyskiy gosudarstvennyy professional'no-pedagogicheskiy universitet; 2022:201-210. (In Russ.). Accessed May 16, 2024. https://elar.rsvpu.ru/handle/123456789/40565

2. Romashkova ON, Kapterev AI. Analiz ugroz i riskov informatsionnoy bezopasnosti v vuze. *Vestnik MGPU. Seriya Informatika i informatizatsiya obrazovaniya*. 2023;1(63):37-47. (In Russ.). doi:10.25688/2072-9014.2023.63.1.03

3. Timofeeva LL. Metodicheskie rekomendatsii po obespecheniyu informatsionnoy bezopasnosti v obrazovatel'noy organizatsii. Oryol: Institut razvitiya obrazovaniya; 2020. 58 p. (In Russ.). Accessed October 09, 2024. https://xn--h1albh.xn--p1ai/wp-content/uploads/2021/06/Metodicheskie-rekomendacii-po-obespecheniju-informacionnoj-bezopasnosti-v-obrazovatelnoj-organizacii.pdf

4. Informatsionnaya bezopasnost' obrazovatel'nykh uchrezhdeniy. *Searchinform*. (In Russ.). Accessed October 09, 2024. https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij

5. Rekomendatsii po obespecheniyu informatsionnoy bezopasnosti v obrazovatel'noy organizatsii. *UIB.* (In Russ.). Accessed October 09, 2024. https://uibcom.ru/articles/informatsionnaya-bezopasnost/rekomendatsii-po-obespecheniyu-informatsionnoy-bezopasnosti-v-obrazovatelnoy-organizatsii

6. Vinnik EA. Obespechenie zashchity informatsii v obrazovatel'nykh organizatsiyakh. *Molodoy uchenyy*. 2023;7(454):3-6. (In Russ.). Accessed October 09, 2024. https://moluch.ru/archive/454/100167/

7. Informatsionnaya bezopasnost' detey v obrazovatel'noy organizatsii (In Russ.). *Xserver*. Accessed October 09, 2024. https://xserver.a-real.ru/blog/useful/informatsionnaya-bezopasnost-detey-v-obrazovatelnoy-organizatsii

8. Cybersecurity Compliance in the Educational Services Sector: How to Protect Students' Personal Data. Accessed October 09, 2024. https://www.syteca.com/en/blog/cybersecurity-in-educational-institutions?utm_source

9. Cybersecurity for Educational Institutions. Accessed October 09, 2024. https://www.cisecurity.org/industry/education?utm_source

10. Sapanca HF, Kanbul S. Risk management in digitalized educational environments: Teachers' information security awareness levels. *Front Psychol.* 2022;13:986561 doi: 10.3389/fpsyg.2022.986561.

11. Cybersecurity in Education levels. Accessed October 09, 2024. https://www.intel.com/content/www/us/en/education/it-in-education/cyber-security.html?utm_source