DOI 10.37882/2223-2982.2024.11.15

КИБЕРБЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОЙ СИСТЕМЫ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

CYBERSECURITY OF THE EDUCATIONAL SYSTEM IN THE AGE OF DIGITAL TRANSFORMATION

N. Eremina
A. Kupriyanov
A. Gatina
N. Kharchenko
T. Goltseva

Summary: In the modern era of rapid technological change and rapidly developing digital transformation of education, the issues of personal data security are becoming increasingly important. The huge amount of information that is constantly circulating in the digital space today makes students' personal data vulnerable to many threats. People use digital devices everywhere in the process of work and study, connect to the Internet through various networks, share personal information and conduct business online. Therefore, ensuring information security has become a key factor in protecting personal data in the context of digital transformation. This requires constant attention and updating of measures to protect personal and public information.

Keywords: digital transformation, education, digital environment, cybersecurity.

Еремина Наталья Владимировна
Кандидат педагогических наук, доцент, Оренбургский государственный университет
nataly-eremina@mail.ru
Куприянов Алексей Викторович
Кандидат сельскохозяйственных наук, доцент, Оренбургский государственный университет
cuprum@rambler.ru
Гатина Алсу Махмутовна
Старший преподаватель, Нефтекамский Филиал Уфимского Университета Науки и Технологий
alsu.gatina2015@yandex.ru
Харченко Николай Леонидович
Старший преподаватель, Российская академия народного хозяйства и государственной службы при Президенте РФ (г. Москва)
m-rh@mail.ru
Гольцева Татьяна Львовна
Старший преподаватель, Российский государственный университет им. А.Н. Косыгина (Технологии. Дизайн. Искусство) (г. Москва)
goltseva-tl@rguk.ru

Аннотация: В современной эпохе быстрых технологических изменений и быстроразвивающейся цифровой трансформации образования вопросы безопасности личных данных приобретают все большую значимость. Огромный объем информации, который сегодня постоянно циркулирует в цифровом пространстве, делает персональные данные обучающихся уязвимыми перед множеством угроз. Люди повсеместно используют цифровые устройства в процессе работы и обучения, подключаются к интернету через различные сети, делятся личной информацией и ведут дела онлайн. Поэтому обеспечение безопасности информации стало основным фактором в защите персональных данных в условиях цифровой трансформации. Это требует постоянного внимания и обновления мер по защите личной и общественной информации.

Ключевые слова: цифровая трансформация, образование, цифровая среда, кибербезопасность.

Кибербезопасность образовательной системы в эпоху цифровой трансформации предстает перед нами как один из наиболее актуальных и сложных вызовов. С переходом учебных заведений к цифровым технологиям всё более очевидным становится стремительное увеличение рисков, связанных с киберугрозами. При этом, задачи, которые решает эта область, выходят далеко за рамки технической безопасности и включают в себя аспекты управления, политики, культуры и образа жизни образовательных учреждений.

Необходимость обеспечения кибербезопасности в школах и университетах носит явный и многогранный характер. С внедрением электронных образовательных ресурсов, онлайн-платформ для дистанционного обучения и облачных решений для хранения данных учащихся и преподавателей, каждое звено цепочки стало уязвимым для кибератак. Сами угрозы разнообразны — от фишинга и взломов до сложных целенаправленных атак и внутреннего саботажа. Предполагается, что проблема это не только технологического уровня, но и человеческого фактора. Например, случаи, когда студенты и сотрудники становятся жертвами социальной инженерии, вызывают не меньше беспокойства.

Согласно исследованиям О.К. Губарева и В.В. Храмова, основные компоненты кибербезопасности образовательных систем включают: защиту данных, идентификацию и аутентификацию, управление доступом, мониторинг и анализ активности, реагирование на инциденты и восстановление после них. Часто пренебрежение хотя бы одним из этих компонентов может привести к серьезным последствиям. Важно принимать во внимание, что учебные заведения нередко становятся мишенью хакеров из-за обширных баз данных, содержащих личную информацию учащихся и сотрудников, финансовые детали и исследования [4, с. 56; 18, с. 115].

Первым шагом на пути к улучшению кибербезопасности является создание осознанности и культуры безопасности среди всех участников образовательного процесса, что включает проведение регулярных тренингов по безопасности, информирование о последних угрозах и методах защиты, а также создание политики безопасности, обязательной для соблюдения. На уровне учебных заведений должны быть внедрены планы реагирования на инциденты, чтобы в случае атаки сотрудники знали, как минимизировать вред и оперативно восстановиться [16, с. 45].

Не менее важно внедрение комплексного подхода к использованию технологий защиты, что включает в себя установку антивирусного ПО, межсетевых экранов, систем обнаружения вторжений, шифрование данных и инвентаризацию сетевых устройств. Со временем следует обновлять технологии и регулярно проводить аудиты безопасности. Важно понимать, что в условиях текущей цифровой трансформации безопасность является процессом, требующим постоянного внимания и адаптации к новым угрозам [21, с. 132].

Особое место занимает защита мобильных устройств и платформ, которые становятся всё более популярными в учебных процессах, что подразумевает необходимость внедрения стратегий по управлению мобильными устройствами, таких как MDM (Mobile Device Management), позволяющим контролировать и ограничивать использование личных устройств для учебных целей. Это особенно актуально в условиях пандемии COVID-19, когда дистанционное обучение стало повсеместным. Роль облачных технологий в образовательных системах также не должна быть проигнорирована. Хотя облачные решения часто предлагают множество преимуществ, включая гибкость и масштабируемость, они также несут новые риски. При выборе облачного поставщика важно оценивать его систему безопасности, проводить независимые аудиты и использовать шифрование данных. Двухфакторная аутентификация и контроль доступа к данным являются необходимостью для предотвращения возможных угроз. Существуют и правовые аспекты кибербезопасности, которые нельзя игнорировать. Защита данных учащихся и сотрудников находится под регулированием таких законов, как GDPR в Европейском Союзе и CIPA в США. Невыполнение требований данных законодательных актов может привести к юридическим последствиям и потерям репутации. Поэтому учебные заведения должны ориентироваться в регуляторных требованиях и следить за их изменениями [20, с. 263].

Проблемы кибербуллинга и защиты детей от онлайн-угроз являются не менее важными составляющими кибербезопасности в образовательной сфере. Для создания безопасной онлайн-среды необходимо разработать и внедрить политику по предотвращению и борьбе с кибербуллингом. Такая политика должна учитывать современные угрозы и методы, используемые злоумышленниками. Кроме того, обучение учащихся и преподавателей надлежащему онлайн-поведенческому этикету играет ключевую роль в профилактике. Комплексный подход включает установление четких правил поведения в сети, систему мониторинга и реагирования на инциденты, а также предоставление психологической поддержки пострадавшим от кибербуллинга [22, с. 207].

Мировой опыт реализации решений в области кибербезопасности носит обширный и многогранный характер. В некоторых частях мира уже реализованы успешные решения в области кибербезопасности в образовательных учреждениях. Например, университеты и школы инвестируют в создание собственных центров кибербезопасности. Эти центры функционируют как площадки для обучения и тренировки специалистов. Здесь студенты и преподаватели могут моделировать кибератаки и разрабатывать методы защиты от них в контролируемой среде. Такой подход не только повышает общий уровень безопасности образовательного учреждения, но и предоставляет уникальный практический опыт. Эти центры также играют важную роль в проведении исследовательской работы, помогая внедрять новейшие достижения в области кибербезопасности [2, с. 170].

Высшие учебные заведения играют стратегическую роль в подготовке следующего поколения специалистов в области кибербезопасности. Чтобы эффективно справляться с растущими вызовами цифровой эпохи, необходимо интегрировать курсы по кибербезопасности в как основные, так и дополнительные образовательные планы. Введение курсов по кибербезопасности на всех уровнях высшего образования позволяет студентам с самого начала знакомиться с ключевыми аспектами этой важной области. На уровне бакалавриата такие курсы могут охватывать основы кибербезопасности, расширяя знания о методах защиты информации, принципах криптографии и основных уязвимостей систем. На уровне магистратуры и аспирантуры акцент может быть сделан на более специализированные темы, такие как противо-

действие кибератакам, анализ угроз, безопасность сетей и систем, а также правовые и этические аспекты кибербезопасности [1, с. 91].

Некоторые образовательные учреждения уже сделали значительные шаги в этом направлении, предлагая специализированные степени и сертификаты в области кибербезопасности. Согласно Н.Н. Кузиной, такие программы часто включают комплексные курсы, посвященные актуальным вопросам и технологиям, а также практические лабораторные работы и проекты, которые позволяют студентам применять теории и методы на практике [6, с. 97].

Освоение таких курсов делает выпускников более конкурентоспособными на рынке труда. Работодатели ценят специалистов, которые уже обладают глубокими знаниями в области кибербезопасности и способны применять эти знания для защиты данных и инфраструктуры организаций. Более того, выпускники программ по кибербезопасности оказываются подготовленными к конкретным профессиональным вызовам, что повышает их востребованность и упрощает процесс трудоустройства [8, с. 154].

Одним из ключевых аспектов кибербезопасности является идентификация и управление уязвимостями. Регулярный мониторинг и анализ систем позволяют своевременно выявлять слабые места, которые могут быть использованы злоумышленниками для нанесения ущерба. Важно внедрять эффективные методы шифрования данных, что позволяет защитить информацию даже в случае её утечки. Контроль доступа и управление правами пользователей также играют важную роль в снижении рисков несанкционированного доступа к данным [10, с. 52].

Сфера образования и цифровая образовательная среда являются одним из фундаментальных элементов в повышении уровня кибербезопасности. Формирование у обучающихся навыков и знаний в этой области становится неотъемлемой частью образовательных программ. Специально разработанные курсы и тренинги позволяют подготовить следующую генерацию специалистов, способных эффективно реагировать на киберугрозы и защищать информационные системы. Такие образовательные инициативы включают в себя изучение основ информационной безопасности, теории и практики шифрования данных, управления сетевой безопасностью и анализа киберугроз [12, с. 310].

Внедрение уроков по так называемой «кибергигиене» для всех уровней образования, начиная с начальной школы, важно потому, что это поможет формировать у молодого поколения осознанное отношение к безопасности в цифровом мире. Дети с раннего возраста познакомятся с основами кибербезопасности, что позволит им лучше понимать, какие угрозы существуют в онлайн-среде и как их избегать. Это станет основой для их дальнейших знаний и навыков в области безопасного использования интернета и технологий [9, с. 313].

Обучение и осведомленность пользователей также играют значительную роль в обеспечении кибербезопасности. Каждый пользователь должен понимать важность соблюдения основных правил безопасности, таких как создание надежных паролей, избегание сомнительных ссылок и приложений, а также регулярное обновление программного обеспечения. Органы власти и частные компании активно разрабатывают и внедряют многочисленные политики и стандарты, направленные на защиту персональных данных и повышение общей киберзащиты, что позволяет создать более безопасную онлайн-среду для всех пользователей [13, с. 135].

В современном мире, где онлайн-сервисы и интернет становятся неотъемлемой частью повседневной жизни, защита личной информации становится всё более актуальной. Такая защита предохраняет такие данные, как финансовую информацию, личные сведения, медицинские записи, логины и пароли от различных аккаунтов, от несанкционированного доступа и различных форм мошенничества. Люди все больше совершают важные действия онлайн – от банкинга до общения и обмена файлами, и до безопасности в психологической практике. Таким образом, защита этих действий является приоритетным направлением в сфере кибербезопасности [7, с. 10].

Особенно важным аспектом кибербезопасности является использование антивирусных программ. Эти программы проверяют файлы и приложения на наличие вирусов и другого вредоносного ПО. Они регулярно обновляются, чтобы противостоять новым угрозам, и обеспечивают дополнительный уровень защиты для вашего устройства. Без антивирусных программ устройства остаются уязвимыми перед множеством зловредных программ, которые могут похищать данные или наносить другой ущерб [11, с. 143].

Технические меры предотвращения негативных последствий имеют первостепенное значение в вопросе защиты данных. Антивирусные программы играют важную роль в выявлении и удалении вредоносного ПО, которое может нанести ущерб компьютеру или сети. Так называемые «фаерволы» (межсетевые экраны) действуют как барьеры между достоверными и недостоверными сетями, контролируя входящий и исходящий трафик и предотвращая несанкционированный доступ. Системы обнаружения вторжений осуществляют мониторинг сетевого трафика в реальном времени, выявляя и реагируя на подозрительные активности. Кроме того,

шифрование данных является важным методом защиты информации, делая ее недоступной для неавторизованных пользователей [17, с. 33].

Административные меры направлены на установление и поддержание правил и процедур, которые регулируют безопасность информации. Четкие политики безопасности определяют, как данные должны обрабатываться, кто имеет к ним доступ и какие меры должны быть приняты для их защиты. Инструкции для сотрудников помогают обучить персонал правильным практикам безопасности, поощряя принятие мер для предотвращения утечек данных. Регулярное проведение обучающих программ помогает повысить осведомленность о современных угрозах и действиях, которые могут минимизировать риски [19, с. 226].

Брандмауэры являются ещё одним ключевым инструментом в кибербезопасности. Они действуют как барьеры между вашим компьютером и интернетом, контролируя входящий и исходящий трафик. Таким образом, они предотвращают несанкционированный доступ к сети и системе. Брандмауэры особенно важны для защищенной работы организаций, где они помогают предотвратить попытки взлома корпоративных сетей [15, с. 116].

Шифрование данных играет важнейшую роль в защите информации. Оно преобразует данные в форму, которая не может быть прочитана без специального ключа. Это особенно важно при передаче конфиденциальной информации через интернет, так как шифрование создаёт высокий уровень защиты от перехвата. Использование шифрования важно как для личных целей, так и для бизнеса, где защита корпоративных данных является критическим аспектом.

Аутентификация пользователей – ещё одна критическая мера в обеспечении безопасности [14]. Она включает использование паролей, биометрических данных и других методов проверки, которые подтверждают, что доступ к информации получает только уполномоченный пользователь. Это особенно актуально в условиях, когда доступ к системам и данным может быть осуществлен с различных устройств и точек входа [3].

Не менее важным является резервное копирование информации. Оно предусматривает создание дублирующих копий данных, которые хранятся в отдельном безопасном месте. В случае взлома, потери или порчи данных, резервные копии позволяют быстро восстановить всю критически важную информацию, что помогает избежать серьёзных потерь и минимизировать время простоя в работе с данными.

Обучение пользователей основным правилам безопасности в сети – ещё один неотъемлемый аспект кибербезопасности. Пользователи должны знать, как создавать сложные и надёжные пароли, уметь распознавать и избегать подозрительных ссылок и файлов, а также понимать основы безопасного поведения в интернете. Подсознание пользователей должно быть настроено на постоянную настороженность и осторожность при обращении с личной информацией в сети. Регулярные обновления знаний и навыков помогут им быть защищёнными от киберугроз и снизят вероятность компрометации их данных. Всё это создаёт комплексную систему защиты, где каждый элемент играет свою роль в общей кибербезопасности [5, с. 40].

Международное сотрудничество также играет важную роль в укреплении кибербезопасности образовательных учреждений. Обмен опытом с коллегами из других стран помогает разрабатывать и внедрять стандарты и мероприятия, которые доказали свою эффективность в других контекстах. Сети и ассоциации по кибербезопасности в сфере образования позволяют обмениваться лучшими практиками и разрабатывать совместные инициативы для усиления защиты образовательных систем. Безопасность образовательной системы в эпоху цифровой трансформации представляет собой многогранную задачу, требующую всестороннего подхода. В первую очередь необходимо обращать внимание на технические меры, такие как внедрение современных антивирусных решений, межсетевых экранов и систем мониторинга. Эти технологии помогают защитить данные студентов и преподавателей от кибератак, вредоносных программ и других угроз. Однако одного лишь технического оснащения для предотвращения угроз явно недостаточно.

Существенная часть обеспечения кибербезопасности связана с образовательными мероприятиями. Важно обучать студентов, преподавателей и административный персонал основам информационной безопасности. Семинары, курсы и тренинги помогут повысить осведомленность и навыки в области защиты данных, что, в свою очередь, уменьшит риски, связанные с человеческим фактором.

Кроме того, правовые меры играют важную роль. Подготовка и соблюдение законодательства в сфере защиты информации позволяет создавать четкие рамки и стандарты, которым должны следовать все образовательные учреждения. Это включает, например, разработку политик конфиденциальности, правил использования данных и внедрение санкций за нарушение этих правил.

Не менее важны социальные меры, направленные на формирование культуры безопасности внутри образовательных учреждений. Это могут быть программы по поддержке ответственного поведения в цифровой сре-

де, мероприятия по предотвращению кибербуллинга и других видов онлайн-насилия.

Таким образом, только через интеграцию всех этих элементов – от технических решений и образовательных программ до правовых рамок, социальной культуры – можно создать действительно устойчивую и безопасную цифровую образовательную среду. Такая комплексная защита станет прочным фундаментом для успешного и безопасного цифрового будущего в образовательной системе. Интеграция курсов по кибербезопасности в образовательные программы высших учебных заведений не только способствует защите информационной безопасности на глобальном уровне, но и открывает перед обучающимися широкий спектр карьерных возможностей, делая их значительно более подготовленными к профессиональной деятельности в цифровую эпоху. Кибербезопасность является комплексной и многогранной областью, требующей внимания и усилий на всех уровнях – от индивидуальных пользователей до больших корпораций и государственных структур. Только совместными усилиями можно создать надёжную систему защиты личных данных в условиях быстро меняющейся цифровой образовательной среды.

ЛИТЕРАТУРА

1. Аншаков, А.С. Публично-правовые аспекты информационной безопасности в образовании / А.С. Аншаков // Вестник Поволжского института управления. – 2024. – Т. 24, № 2. – С. 91-98. – DOI 10.22394/1682-2358-2024-2-91-98. – EDN LUPTBI.
2. Бочкина, Е.В. Педагогическое тестирование: от истоков до создания современных тестов / Е.В. Бочкина, В.Н. Ханчас // Педагогика и просвещение. – 2024. – № 1. – С. 170-182. – DOI 10.7256/2454-0676.2024.1.69243. – EDN BDGXVU.
3. Воробьева, А.Г. Социологическая оценка изменения восприятия профессии педагога в обществе / А.Г. Воробьева // Дневник науки. – 2021. – № 7(55). – DOI 10.51691/2541-8327_2021_7_3. – EDN HADHSB.
4. Губарев, О.К. Способ повышения безопасности программных средств и пути его реализации / О.К. Губарев, В.В. Храмов // Тематический научно-технический сборник. – Пущино: Издательство Пущинского научного центра Российской Академии наук, 1994. – С. 56-61. – EDN YWTBVE.
5. Дидактический потенциал ИКТ в обучении иностранному языку в юридическом вузе / М.В. Боровкова, Н.В. Ялаева, Н.В. Садыкова, С.В. Павлова // Современное педагогическое образование. – 2019. – № 6. – С. 40-43. – EDN OJCLME.
6. Кузина, Н.Н. Информационная безопасность: основополагающий аспект цифровизации образования / Н.Н. Кузина, К.И. Корчак // Вестник Прикамского социального института. – 2021. – № 1(88). – С. 97-99. – EDN CFPRWV.
7. Любачевский, И.А. Безопасность в психологической практике / И.А. Любачевский // Смысл, функции и значение разных отраслей практической психологии в современном обществе: сборник научных трудов, Хабаровск, 22–25 ноября 2016 года / под ред. Е.Н. Ткач. – Хабаровск: Тихоокеанский государственный университет, 2017. – С. 10-16. – EDN XPGODZ.
8. Митченко, В.А. управление организационным совершенствованием предприятия / В.А. Митченко, И.В. Воробьева // Региональная экономика: проблемы и перспективы развития в современных условиях: Сборник научных трудов по материалам Международной научно-практической конференции, Невинномысск, 12 декабря 2019 года. – Невинномысск: Общество с ограниченной ответственностью фирма «Ставрополь-сервис-школа», 2020. – С. 154-159. – EDN NODTDR.
9. Овдиенко, Д.А. Профилактика информационной зависимости у подростков / Д.А. Овдиенко, М.В. Сомов // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований: Материалы II Всероссийской национальной научной конференции студентов, аспирантов и молодых ученых. В 4-х частях, Комсомольск-на-Амуре, 08–12 апреля 2019 года / Ответственный редактор Э.А. Дмитриева. Том Часть 4. – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2019. – С. 313-316. – EDN ZUBLLK.
10. Пекарева, В.В. Содержание фундаментальных категорий обеспечения информационной безопасности / В.В. Пекарева // Актуальные вопросы науки и образования: Сборник материалов IV Международной научно-практической конференции. Москва, 15 января 2024 года. – Москва: Центр развития образования и науки, ООО «Издательство АЛЕФ», 2024. – С. 52-56. – EDN KWECHS.
11. Пекарева, В.В. Характеристика явления фишинга в сетевом пространстве: гражданско-правовой аспект и его проблемное определение / В.В. Пекарева, И.В. Бондаренко // Аграрное и земельное право. – 2023. – № 10(226). – С. 143-144. – DOI 10.47643/1815-1329_2023_10_143. – EDN AVLHAE.
12. Полякова, Т.А. Образование и культура информационной безопасности граждан Российской Федерации: научно-правовые аспекты / Т.А. Полякова, Н.А. Троян // Образование и право. – 2023. – № 3. – С. 310-317. – DOI 10.24412/2076-1503-2023-3-310-317. – EDN ROFGQT.
13. Развитие информационной безопасности личности обучающегося в условиях цифровой трансформации образования / О.Ю. Герасимова, О.П. Михайлова, Ю.В. Власова [и др.] // Вестник педагогических наук. – 2023. – № 7. – С. 135-142. – EDN YQEBPU.
14. Родюкова, Т.Н. Социокультурное управление в современных российских организациях: специальность 22.00.08 «Социология управления»: диссертация на соискание ученой степени кандидата социологических наук / Родюкова Татьяна Николаевна. – Москва, 2006. – 162 с. – EDN NNXXYN.
15. Система кибербезопасности современного образовательного учреждения / И.Д. Алекперов, Э.А. Алекперова, А.И. Алекперова, В.В. Храмов // Интеллектуальные ресурсы - региональному развитию. – 2020. – № 2. – С. 116-122. – EDN BSLVOC.
16. Сомов, М.В. Информационная безопасность подрастающего поколения в контексте системно-структурного подхода / М.В. Сомов // Общество: социология, психология, педагогика. – 2022. – № 11(103). – С. 45-49. – DOI 10.24158/spp.2022.11.6. – EDN RNMAZC.
17. Томин, В.В. О проблемах машинного перевода научно-технического текста в информационном поле кросс-культурного взаимодействия / В.В. Томин // Вестник Оренбургского государственного университета. – 2015. – № 1(176). – С. 33-39. – EDN TWQXXL.

18. Храмов, В.В. Основы методологии синтеза средств защиты информации / В.В. Храмов // Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем: Материалы XXI Межведомственной научно-технической конференции, Серпухов, 01–30 июня 2002 года. Том Часть 3. – Серпухов: Серпуховской военный институт ракетных войск, 2002. – С. 115-120. – EDN WDOQMP.
19. Ялаева, Н.В. Применение технологий адаптивного компьютерного обучения при подготовке студентов-юристов / Н.В. Ялаева, Н.В. Садыкова, Т.В. Кудинова // Современное педагогическое образование. – 2023. – № 9. – С. 226-231. – EDN SGGMTZ.
20. Culturological and axiological issues of students' cross-cultural interaction in the information field / V.V. Tomin, T.S. Bochkareva, A.Y. Bogomolova [et al.] // Man in India. – 2017. – Vol. 97, No. 25. – P. 263-283. – EDN RXYFCX.
21. Trufanov, G.A. Crisis and conflict in Russian contemporary social media / G.A. Trufanov // Конфликтология. – 2021. – Vol. 16, No. 1. – P. 132-158. – EDN DZCTXE.
22. Trufanov, G.A. Governmental control over information distribution as a basis of the social conflict / G.A. Trufanov // Конфликтология. – 2019. – Vol. 14, No. 3. – P. 207-221. – EDN SMRPDE.

Журнал «Современная наука: актуальные проблемы теории и практики»