ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.588: 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ И ВЫРАБОТКА СТРАТЕГИЙ ЗАЩИТЫ ШКОЛЬНИКОВ ОТ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ[1]

Статья поступила в редакцию 31.03.2020, в окончательном варианте – 19.04.2020

Ажмухамедов Искандар Маратович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

доктор технических наук, профессор кафедры информационной безопасности, e-mail: aim_agtu@mail.ru

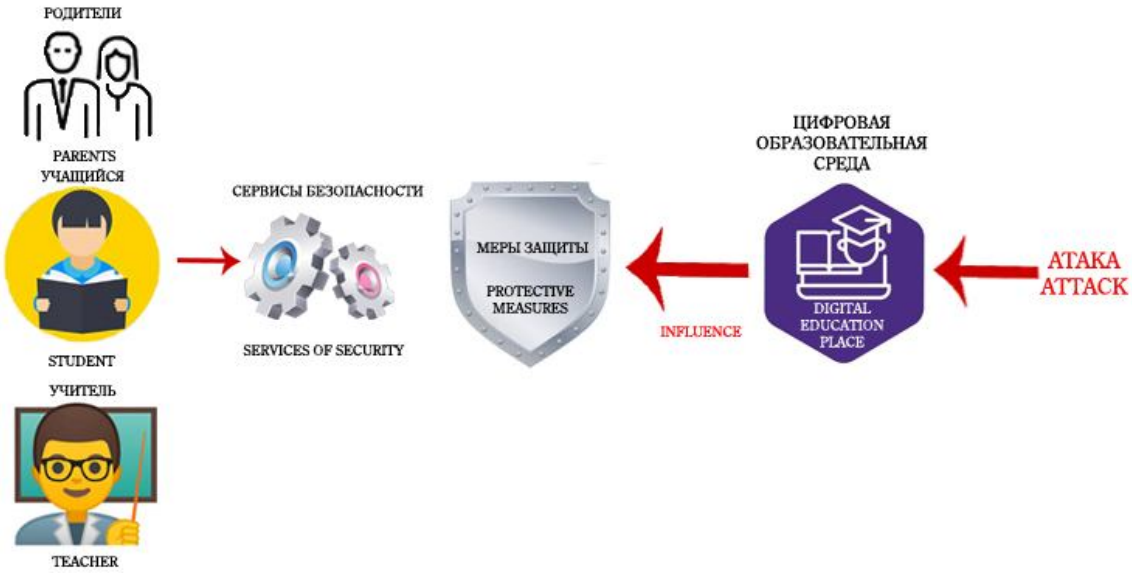
Кузнецова Валентина Юрьевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

ассистент, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru

Приведен краткий обзор этапов цифровизации российского образования в контексте реализации приоритетных федеральных целевых программ и стратегии развития цифровой экономики; определены основные проблемы, связанные с тенденцией перехода к дистанционному обучению, в том числе показана актуальность рисков использования цифровой образовательной среды в отношении обеспечения информационной безопасности участников образовательного процесса – учащихся, преподавателей, родителей. Приведен перечень актуальных рисков, связанных с нарушением конфиденциальности, целостности, доступности, аутентичности и неотказуемости использования цифровой образовательной среды. Также даны основные рекомендации по возможной минимизации этих рисков. Актуальность использования таких рекомендаций подтверждается результатами проведенного авторами опроса преподавателей, работающих в учреждениях среднего и высшего образования. Результаты исследования целесообразно учитывать в работе администраторов и менеджеров цифровых образовательных платформ с целью повышения качества сервиса.

Ключевые слова: цифровизация образования, цифровая образовательная среда, информационная безопасность, стратегии защиты, цифровая школа, участники образовательного процесса, персональные данные

Графическая аннотация (Graphical annotation)



[1] Статья выполнена при поддержке гранта РФФИ, проект № 19-29-14007 мк «Оценка влияния цифровизации образовательного и социального пространства на человека и разработка системы безопасной коммуникативно-образовательной среды».

INFORMATION SECURITY IN THE DIGITAL EDUCATIONAL ENVIRONMENT: ANALYSIS OF INFORMATION RISKS AND DEVELOPMENT OF STRATEGIES TO PROTECT SCHOOLCHILDREN FROM NEGATIVE CONSEQUENCES OF DIGITALIZATION OF EDUCATION

Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

Doct. Sci. (Engineering), Professor of the Department of Information Security, e-mail: aim_agtu@mail.ru

Kuznetsova Valentina Yu., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

assistant, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru

The paper shows an overview of the stages of digitalization of Russian education in the context of the implementation of priority federal target programs and the development strategy of the digital economy is given; identified the main problems associated with the trend of transition to distance learning, including the relevance of the risks of using the digital educational environment in relation to ensuring the information security of the participants in the educational process - students, teachers, parents. The list of actual risks associated with the violation of confidentiality, integrity, availability, authenticity, and non-repudiation of the use of the digital educational environment is given. The main recommendations on the possible minimization of these risks are also given. The relevance of using such recommendations is confirmed by the results of a survey of teachers working in secondary and higher education institutions conducted by the authors. The results of the study should be taken into account in the work of administrators and managers of digital educational platforms in order to improve the quality of service.

Keywords: digitalization of education, digital educational environment, information security, protection strategies, digital school, participants in the educational process, personal data

Введение. Приоритетный проект в области образования «Современная цифровая образовательная среда в Российской Федерации» был утвержден Правительством Российской Федерации 25 октября 2016 г. в целях реализации государственной программы «Развитие образования» на 2013–2020 гг. [13].

Данный проект был представлен на заседании президиума Совета при Президенте Российской Федерации по стратегическому развитию и приоритетным проектам премьер-министром Дмитрием Медведевым. Он в своем докладе указал ведомствам на то, что «*создание цифровой образовательной среды – это стратегически важная государственная задача, определяемая необходимостью снабжения цифровой экономики молодыми квалифицированными кадрами*». А для их подготовки необходимо усовершенствовать систему образования и, в частности, профессиональной подготовки; привести существующие образовательные программы к требованиям цифровой экономики и разработать отсутствующие; повсеместно внедрить электронные инструменты учебной деятельности; обеспечить возможность обучения граждан Российской Федерации и граждан иностранных государств, выбравших нашу страну для получения образования, по индивидуальному учебному плану в течение всей жизни – в любое время и в любом месте.

В приоритетном проекте «Современная цифровая образовательная среда в Российской Федерации» предусматривается повышение качества и доступности образования в России за счет использования дистанционного обучения на всех уровнях образования. Поставлена достаточно амбициозная задача – достижение к 2025 г. числа обучающихся в образовательных организациях, прошедших обучение на онлайн-курсах для формального и неформального обучения, – 11 млн человек. Из них студенты средних профессиональных образовательных организаций и образовательных организаций высшего образования должны составить 5 млн человек.

Реализация приоритетных проектов в области образования предусматривает ряд ключевых направлений, реализация которых идет параллельно:

- разработка и принятие нормативно-правовых актов, необходимых для развития онлайн-обучения (в частности, фиксирующих статус дистанционных курсов в качестве равноправных элементов образовательных программ);
- создание информационного ресурса, который будет обеспечивать доступ к онлайн-курсам по принципу «единого окна» и объединять существующие разрозненные платформы онлайн-обучения благодаря единой системе аутентификации пользователей;
- создание к 2020 г. 3,5 тысяч онлайн-курсов по программам среднего, высшего и дополнительного образования с привлечением ведущих разработчиков и педагогов как из государственных структур, так и бизнес-сообщества;
- подготовка и обучение не менее 10 000 преподавателей и экспертов в области онлайн-обучения [11].

Акцентируем внимание на техническую составляющую проекта – так называемую цифровую образовательную среду, которая по принципу «единого окна» будет обеспечивать учащихся на всех уровнях обучения образовательным контентом. Авторы проекта утверждают, что обучающимся такая система поможет на практике реализовать принцип виртуальной академической мобильности, предоставив им возможность получать качественный образовательный контент от ведущих учебных заведений страны. При этом результаты прохождения онлайн-курсов будут зачтены наравне с результатами очного обучения [1]. С другой стороны, преподавателям ресурс позволит изучить лучший отечественный педагогический опыт, внести в него свою лепту, а также даст возможность выделить больше времени на практические занятия со студентами и на повышение собственной квалификации. Работодатели смогут напрямую высказывать свои пожелания к обучающему контенту с целью приведения его в соответствие с требованиями рынка труда. В отношении образовательных платформ и создателей онлайн-курсов это будет способствовать расширению аудитории, повышению качества и востребованности созданных продуктов [8].

Согласно приоритетным государственным проектам [11, 14], образовательная среда должна быть безопасной для всех участников образовательного процесса, а также обеспечивать высокое качество и доступность образования всех видов и уровней. При этом само введение единой для всех граждан и организаций образовательной системы само по себе порождает ряд рисков, которые угрожают обеспечению безопасности участников образовательной деятельности (учащиеся, преподаватели) в отношении различных аспектов их жизнедеятельности (например, угрозы ослабления социальных и коммуникативных навыков [3], ухудшение физического и психоэмоциального здоровья и т.п.). Помимо всего прочего, имеют место и информационные риски, связанные с безопасностью образовательного процесса в условиях цифровой экономики [2].

В связи с этим становятся актуальными анализ и классификация информационных рисков, связанных с реализацией и внедрением единой цифровой образовательной среды (ЦОС) с точки зрения основных сервисов безопасности информации: конфиденциальности, целостности, доступности, аутентичности и неотказуемости. Рассмотрим их подробнее.

Конфиденциальность. Согласно статье № 2 Федерального закона «Об информации, информационных технологиях и защите информации» [9], конфиденциальность – «*обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя*».

Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации нелегитимным пользователям. В первую очередь к конфиденциальной информации, используемой в рамках учебного процесса, можно отнести персональные данные участников ЦОС:

- фамилия, имя, отчество;
- дата рождения;
- адрес места регистрации и проживания, контактные телефоны, адреса электронной почты;
- паспортные данные или данные свидетельства о рождении.

Данный список может быть скорректирован в зависимости от требований образовательного учреждения или единой образовательной платформы. Кроме того, исходя из определения, установленного ч. 1 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ [10], «*к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и могут быть использованы для установления личности субъекта*».

Использование фотографий участников образовательного процесса предполагается при реализации цифрового обучения в качестве аватаров для аккаунтов.

Риски нарушения конфиденциальности включают в себя нелегитимное распространение личной информации участников образовательного процесса, например, контактных данных, фотографий, а также результатов выполненных индивидуальных заданий и полученных баллов по ним.

Распространение личных данных может привести к проблемам не только в образовательной системе, но и за ее пределами, например, когда личными данными ребенка (обучающегося) могут воспользоваться злоумышленники с целью грабежа или травли его или родителей [5].

Опираясь на вышесказанное, можно сделать вывод, что система цифрового обучения должна всеми возможными способами обеспечивать конфиденциальность обрабатываемых сведений, в том числе согласно действующему законодательству в области защиты персональных данных [10].

Согласно требованиям законодательства РФ в сфере персональных данных (ПДн) [10] утверждены требования, распространяющиеся на защиту ПДн при их обработке в информационных системах обработки персональных данных (ИСПДн). С точки зрения обработки персональных

данных ЦОС также будет являться ИСПДн. Поэтому должна обеспечиваться защита ПДн всех участников образовательного процесса в соответствии с требованием этого постановления.

По требованиям указанного нормативного акта, для ЦОС характерен 3-й тип актуальных угроз и 3-й уровень защищенности (табл.).

Таблица – Определение уровня защищенности ИСПДн ЦОС

Тип ПДн	Категория субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	**3 тип**
Специальные	Не сотрудники	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудники	Любое	УЗ 1	УЗ 2	УЗ 3
Биометрические	**Любые**	**Любое**	УЗ 1	УЗ 2	**УЗ 3**
Иные	Не сотрудники	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудники	Любое	УЗ 1	УЗ 3	УЗ 4
Общедоступные	Не сотрудники	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудники	Любое	УЗ 2	УЗ 3	УЗ 4

Для обеспечения 3-го уровня защищенности требуется осуществление технической защиты помещений, в которых располагаются элементы ИСПДн, в том числе использование внутриобъектового режима с ограниченным доступом в помещения.

В состав мер по обеспечению 3-го уровня защищенности ПДн, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита ИСПДн, ее средств, систем связи и передачи данных;
- управление конфигурацией ИСПДн и системы защиты персональных данных.

Данные меры актуальны не только для защиты персональных данных, но и в целом для обеспечения конфиденциальности информации, хранящейся в системе.

Целостность. Этот термин в сфере информационных технологий обозначает, что данные не подвергались изменению при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

С учетом специфики используемых механизмов обеспечения целостности данных в ЦОС можно выделить три стороны этого понятия.

Правильность. Заключается в отсутствии логических ошибок в структуре и ошибок в содержании (в значениях) данных при их обработке.

Неискаженность. Заключается в отсутствии подделки исходных данных или возникновения ошибок в них при передаче по линиям связи, а также при хранении.

Неизменность. Заключается в тождественности данных определенному эталону, например, если речь идет о формулировке понятий из нормативно-правовых актов и т.п.

В рамках реализации ЦОС данный сервис безопасности информации актуален не менее чем конфиденциальность по нескольким причинам.

П1) Изменение и искажение образовательного контента недопустимо, за исключением тех случаев, когда преподаватель или системный администратор легитимно вносят правки в учебный материал с целью его уточнения, исправления ошибок или обновления контента в связи с изменениями в образовательных стандартах или других нормативно-правовых актах.

П2) Образовательный контент должен соответствовать требованиям нормативно-правовой базы, т.е. быть идентичным эталону; расхождения и приближенные данные неприемлемы.

П3) Критически важно отсутствие логических ошибок в структуре не только образовательного контента или всего курса, но и самой цифровой образовательной среды. В случае если имеются нарушения в логике работы образовательной платформы, то возможны технические проблемы, недоступность образовательных материалов, курсов или вспомогательных разделов среды.

Основными методами обеспечения целостности информации при хранении в информационных системах (в качестве которых выступает ЦОС) являются следующие.

М1) Обеспечение отказоустойчивости за счет резервирования, дублирования, зеркалирования оборудования и данных.

Резервирование и дублирование выполняют одну и ту же функцию при обеспечении отказоустойчивости – создание запасных элементов системы на случай, если основная система не сможет осуществлять работу в полной мере. Например, на случай нарушений в работе основной системы создается копия образовательной платформы, и образовательный процесс временно или постоянно переносится на нее.

М2) Обеспечение возможностей безопасного восстановления данных путем резервного копирования и электронного архивирования информации.

Данный метод включает в себя создание различного рода резервных копий для своевременного восстановления поврежденных данных или всей образовательной платформы в целом. Хранение созданных резервных копий необходимо обеспечивать в отдельных хранилищах, которые никак не связаны с основной системой.

М3) Обеспечение безопасной передачи данных с помощью средств криптографической защиты (шифрование, хеширование, применение электронной цифровой подписи).

Авторы считают, что совокупность перечисленных методов обладает свойством «необходимости и достаточности».

Чтобы избежать нарушения целостности данных при их передаче, например, в случае, когда преподаватель вносит изменения в контент учебного курса, расположенного на образовательной платформе, используются вышеуказанные средства криптографической защиты с целью обнаружения повреждения данных. Если будет выявлено, что данные после передачи оказались повреждены, то изменения в существующую систему вноситься не будут.

Доступность. Согласно стандарту Р 50.1.053-2005, данный термин обозначает «*состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно*».

К правам доступа относятся следующие: право на чтение, изменение, хранение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение информационных ресурсов.

Нарушение доступности представляет собой создание таких условий, при которых доступ к информации будет либо заблокирован, либо возможен за время, которое не обеспечит достижение тех или иных целей.

Например, одним из наиболее распространенных способов нарушения доступности является чрезмерная загрузка информационной системы (загрузка полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти – ddos-атака) или внедрение вредоносного кода в систему. Опасными являются и стихийные бедствия – пожары, наводнения, землетрясения, ураганы.

По статистике [4], на долю этих источников угроз с учетом перебоев электропитания приходится 13 % потерь, нанесенных информационным системам, коей является ЦОС. По этим же данным, техногенные угрозы (пожары, обрушение зданий, перебои в электропитании и пр.) тоже имеют место практически в 2 раза чаще.

Обеспечение доступности цифровой образовательной среды является актуальной и принципиально важной задачей, так как даже кратковременная блокировка образовательного контента нарушает основной принцип образования – принцип доступности обучения.

Кроме того, при угрозе доступности нарушается целостность образовательного процесса, который состоит из 4-х взаимосвязанных компонент:

- процесса освоения и конструирования содержания обучения и базы образовательных материалов;
- взаимодействия учителей и учеников в учебном процессе как части целостного педагогического процесса;
- личностного взаимодействия педагогов с обучаемыми;
- самостоятельного усвоения материала учащимися.

Выпадение любого из этих элементов приводит к существенному снижению результативности образовательного процесса и, как следствие, обучения.

Основными методами обеспечения доступности данных при хранении в автоматизированных системах является использование систем бесперебойного электропитания оборудования, а также резервирование и дублирование вычислительных мощностей, чтобы в случае реализации угроз своевременно восстановить работу системы.

Неотказуемость. Иначе данный сервис безопасности называется неотрекаемостью от авторства информации, а также факта её отправки или получения.

Риск нарушения неотказуемости включает в себя наличие возможности отказаться от факта создания, передачи или получения информации. В качестве примера можно привести отказ от факта отправки оскорбительного письма, от факта несвоевременной сдачи экзамена или выполнения тестовых заданий.

С целью минимизации риска нарушения данного сервиса безопасности в ЦОС должен быть реализован механизм обеспечения неотказуемости, который будет обеспечивать сбор, обработку, а также доступность и признание неопровержимости доказательства (свидетельства) относительно заявленного события или действия с целью урегулирования споров о произошедшем или непроизошедшем событии или действии.

Процедура обеспечения неотказуемости включает четыре фазы: формирование доказательства; доставка, хранение и извлечение; проверка (подтверждение подлинности) доказательства; разрешение спора в установлении авторства. Технически реализация данных процедур осуществляется путем использования электронной подписи и процедур логирования.

Аутентичность. Под термином «аутентичность» понимается возможность однозначно идентифицировать автора или источник информации. В некоторых других литературных источниках этот сервис безопасности называют «подлинность».

Аутентичной является информация, в отношении которой доказано следующее:

- она не подвергалась изменению;
- она была создана или послана именно тем пользователем, который указан в качестве ее создателя или отправителя;
- она была создана или послана именно в то время, которое для нее указано.

Также риск нарушения аутентичности подразумевает под собой возможность субъекта выдавать себя за другого пользователя. Этим субъектом может быть и участник образовательной платформы, и внешний злоумышленник. Результатом такой деятельности, к примеру, может стать несанкционированное изменение контента, мошеннические действия при получении образования с целью пройти экзаменацию ТЕРМИН за обучающегося, внесение изменений в балльно-рейтинговую систему оценки результатов и т.п. Также могут быть скомпрометированы личные данные участников образовательного процесса (нарушение конфиденциальности), или организована рассылка нелегального контента, оскорбительных сообщений от лица других людей.

Обеспечение аутентичности неразрывно связано с идентификацией и аутентификацией пользователей. Проверка подлинности (аутентификация) может проводиться различными методами и средствами. В настоящее время в автоматизированных системах используются три основных способа аутентификации по следующим методам:

1. Парольная защита**.** Реализуется программными средствами аутентификации, которые существуют в большинстве операционных систем, системах управления базами данных путем выдачи зарегистрированному пользователю индивидуального пароля, который должен держаться в секрете и использоваться для каждого входа в систему. Программы парольной защиты сравнивают введенный пароль с эталоном, хранящимся в базе данных системы, и в случае совпадения паролей запрос пользователя на вход в систему принимается к исполнению.

2. Использование индивидуальных носителей**.** В качестве предмета, имеющегося у пользователя, применяются идентификационные карты (ИК), в которые заносятся данные, позволяющие идентифицировать пользователя: персональный номер, специальный код и т.п. Эта информация заносится на ИК в зашифрованном виде, причем ключ шифрования может являться дополнительным идентифицирующим параметром, поскольку он может быть известен только пользователю, вводится им каждый раз при обращении к системе и уничтожается сразу же после использования.

3. Использование физиологических признаков легальных пользователей системы (скан сетчатки глаза, отпечатков пальцев, Face-ID). Существует достаточно много физиологических признаков, однозначно указывающих на конкретного человека. К ним относятся: отпечатки ног и рук, строение челюстно-лицевой области [7], радужная оболочка глаз, черты лица, голос и т.д. Для аутентификации пользователей терминалов автоматизированных систем наиболее приемлемыми

считаются отпечатки пальцев (расположение папиллярных узоров на них), голос, личная подпись. При непосредственном сравнении изображений устройство аутентификации определяет схожесть двух изображений и вырабатывает сигнал, определяющий степень совпадения сравниваемых объектов. Сравнение отпечатков обычно выполняется непосредственно на месте установки рабочей станции, доступ к которой ограничивается описываемым способом. Передача изображения отпечатка по каналам связи не применяется из-за ее сложности, высокой стоимости и необходимости дополнительной защиты этих каналов.

Необходимо отметить, что все рассмотренные методы аутентификации в случае неподтверждения подлинности должны осуществлять временную задержку перед обслуживанием следующего запроса. Это необходимо для снижения угрозы подбора идентифицирующих данных (особенно паролей) в режиме реального времени. При этом все неудачные попытки входа в систему должны регистрироваться в целях обеспечения эффективного контроля над безопасностью системы.

В связи с вышесказанным становится оптимальным использование нескольких методов аутентификации, в том числе двухфакторная авторизация.

Результаты анонимного анкетирования. Оценка актуальности указанных выше рисков невозможна без учета мнения самих участников образовательного процесса. В связи с этим было проведено анкетирование преподавателей школ, колледжей и университетов, результаты которого были обработаны статистически.

В основу расчета необходимого объема репрезентативной выборки (РВ) была положена формула, учитывающая уровень доверия к результатам, полученным при исследовании РВ, а также допустимый предел погрешности. Данная формула используется ВЦИОМом при расчете объема выборки, если не известна доля лиц в генеральной совокупности, обладающих искомым признаком. Впервые данную формулу в русскоязычной литературе привел В.И. Паниотто [12]:

$$V_{\text{РВ}} = \frac{\frac{Z^2 p(1-p)}{e^2}}{1+\left(\frac{Z^2 p(1-p)}{e^2 N}\right)} = \frac{Z^2 p\, N(1-p)}{Z^2 p(1-p)+e^2 N}, \quad (1)$$

где N – численность генеральной совокупности; e – предел погрешности в виде десятичной дроби; Z – уровень доверия (Z-оценка); p – процентная доля интересующей исследователя части выборки, продемонстрировавшей определенное поведение в ходе предыдущих испытаний (также в виде десятичной дроби). При первичном исследовании рекомендуемое значение $p = 0{,}5$.

Предел погрешности – это процентное значение, показывающее, с какой вероятностью мнения и поведение респондентов из выборки отклоняются от мнения и поведения респондентов из общей *(генеральной)* совокупности.

Уровень доверия указывает, насколько достоверными являются полученные результаты. Общепринятые стандарты, используемые исследователями: 90 %, 95 % и 99 % (фактически уровень доверия 95 % означает, что если повторить одно и то же исследование при одинаковых условиях 100 раз, то в 95 случаях из 100 результаты будут находиться в пределах погрешности). При определении размера выборки используется Z-оценка уровня доверия – мера стандартного отклонения определенной доли от средней величины (значение критерия Стьюдента при указанных уровнях значимости равно 1,65; 1,96 или 2,58 соответственно).

Объем репрезентативной выборки определяется на основе статистических данных и методологических рекомендаций по организации выборочных наблюдений Федеральной службы государственной статистики (Росстат). По ее данным за 2018 г., в Российской Федерации насчитывается 1,711 миллионов педагогических работников (школы, колледжи, вузы).

$$V_{\text{РВ}} = \frac{1{,}96^2 \cdot 0{,}5 \text{ x } 1711000 \text{ x } (1-0{,}5)}{1{,}96^2 \cdot 0{,}5 \text{ x } (1-0{,}5)+0{,}05^2 \text{ x } 1711000} = 384.$$

Таким образом, был рассчитан объем репрезентативной выборочной совокупности, которая оказалась равна 384 опрошенным при уровне доверия 95 %.

Именно это количество было опрошено в результате анкетирования. Оно проходило в бумажном и электронном виде. Бумажные анкеты были распространены среди учителей 14 средних школ города Астрахани и преподавателей Астраханского государственного университета. Электронная анкета, реализованная в сервисе Google.Forms, была размещена в закрытом федеральном педагогическом сообществе в социальной сети «ВКонтакте». В этом сообществе состоит свыше 300 тысяч участников, при этом доли преподавателей высших и средних учебных учреждений примерно одинаковые.

При анкетировании респондентам было предложено выбрать наиболее актуальные риски из числа вышеперечисленных при реализации ЦОС.

Результаты опроса в наглядном виде приведены на рисунке.

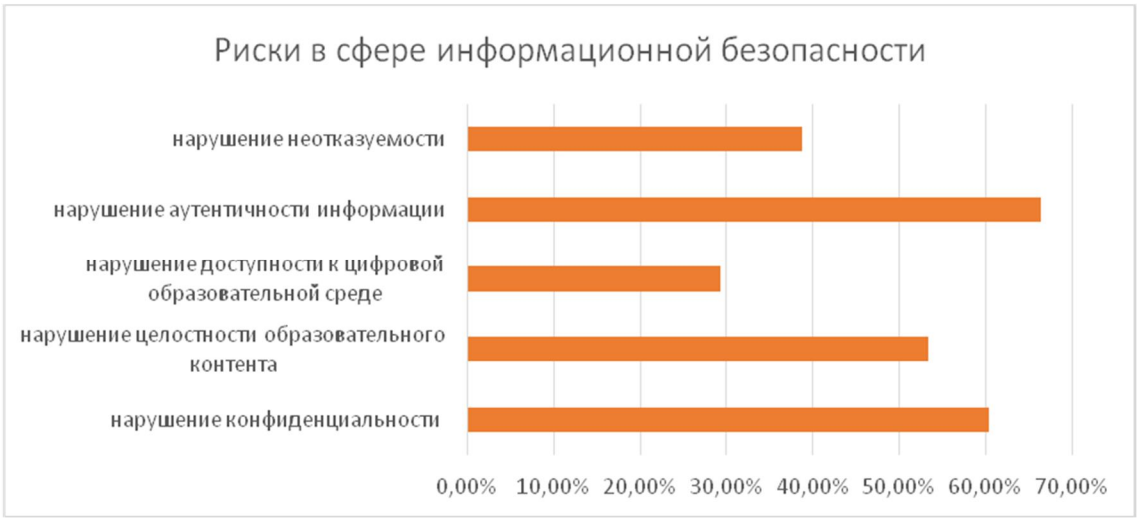


Рисунок – Диаграмма, иллюстрирующая мнение опрошенных об актуальности рисков информационной безопасности при реализации ЦОС

На диаграмме видно, что наибольшие опасения среди педагогического сообщества при реализации ЦОС вызывают риски нарушения конфиденциальности, целостности и аутентичности (свыше половины опрошенных отметили данные варианты ответов при участии в анкетировании). При этом наибольшее количество ответов получил риск, связанный с аутентичностью. Примечательно, что этот риск также наиболее актуален и при реализации классической классно-урочной формы обучения (опасность того, что один ученик напишет контрольную за другого или «подрисует» оценки в учительском журнале). Это говорит о том, что риски реализации ЦОС имеют те же самые базисы, что и при классической форме организации образовательного процесса.

Заключение. Информатизация образовательной сферы играет важную роль в повышении качества и доступности образования. Внедрение новых технологий в процесс обучения позволяет наряду с традиционными учебными материалами использовать современные электронные средства поддержки и сопровождения образовательного процесса. Однако при переходе к цифровому образованию возникают угрозы, которые вызваны именно организацией единой цифровой образовательной среды (информационные риски), и их нельзя игнорировать. По мнению российских преподавателей школ, вузов и ссузов, которые участвовали в опросе в рамках данного исследования, этот тип рисков является наиболее актуальным. При этом респондентами наиболее актуальными были признаны риски нарушения конфиденциальности, аутентичности и целостности, так как они наиболее явно оказывают деструктивное влияние на участников образовательного процесса.

Поэтому при внедрении ЦОС необходимо тщательно оценить последствия такого вида обучения с точки зрения безопасности, принять и реализовать оптимальную стратегию защиты от вызываемых ею угроз.

Библиографический список

1. Абдрахманова Г. И. О чем говорят цифры / Г. И. Абдрахманова, Г. Г. Ковалева // Народное образование. – 2011. – № 10. – С. 48–51.

2. Аетдинова Р. Р. Анализ и классификация рисков цифровизации образования / Р. Р. Аетдинова // Образование через всю жизнь: непрерывное образование в интересах устойчивого развития : материалы XVII Международной конференции. – Санкт-Петербург : Издательство Санкт-Петербургского государственного экономического университета, 2019. – С. 145–148.

3. Баева Л. В. Социокультурные и философские проблемы развития информационного общества / Л. В. Баева. – Астрахань : Издательский дом «Астраханский университет», 2019. – 137 с.

4. Балановская А. В. Источники возникновения и последствия реализации угроз информационной безопасности промышленных предприятий / А. В. Балановская. – Режим доступа: https://cyberleninka.ru/article/n/istochniki-vozniknoveniya-i-posledstviya-realizatsii-ugroz-informatsionnoy-bezopasnosti-promyshlennyh-predpriyatiy/viewer, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 20.01.2020).

5. Зленко Н. С. Почему образование в России нуждается в цифровизации? / Н. С. Зленко // Сборник статей по материалам LXX студенческой Международной научно-практической конференции. – Москва, 2020. – С. 72–77.

6. Майкулов Ж. Ж. Преступления против детей с использованием Интернета / Ж. Ж. Майкулов // Концепт. – 2017. – Т. 39. – С. 2636–2640. – Режим доступа: http://e-koncept.ru/2017/970854.htm, свободный. – Заглавие с экрана. – Яз. рус.

7. Манин А. И. Виды экспертиз, проводимых при использовании аномалий отдельных зубов для идентификации личности / А. И. Манин. – Режим доступа: https://www.mediasphera.ru/issues/rossijskaya-stomatologiya/2016/1/082072-64062015018, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

8. Маркелов К. А. Анализ существующих и перспективных направлений использования дистанционных образовательных технологий в российских региональных государственных вузах / К. А. Маркелов, Ю. М. Брумштейн, И. М. Ажмухамедов // Дистанционные образовательные технологии : материалы IV Всероссийской научно-практической конференции (с международным участием). – 2019.

9. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ от 27 июля 2006 г. : принят Государственной Думой 8 июля 2006 г. // Собрание законодательства Российской Федерации. – 2006.

10. О персональных данных : Федеральный закон № 149-ФЗ от 27 июля 2006 г. : принят Государственной Думой 8 июля 2006 г. // Собрание законодательства Российской Федерации. – 2006.

11. Описание проекта «Современная цифровая образовательная среда». – Режим доступа: http://neorusedu.ru/about, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

12. Паниотто В. И. Количественные методы в социологических исследованиях / В. И. Паниотто, В. С. Максименко. – Киев : Наукова Думка, 1982. – 272 с.

13. Приоритетный проект «Современная цифровая образовательная среда в Российской Федерации», утвержденный Президиумом Совета при Президенте РФ по стратегическому развитию и приоритетным проектам (протокол от 25 октября 2016 г. № 9) // Консультант. – Режим доступа: http://www.consultant.ru/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 20.01.2020).

14. Приоритетный проект «Цифровая школа». – Режим доступа: http://government.ru /projects/selection/693/30822/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

15. Реализация доступа к онлайн-курсам по принципу «одного окна». – Режим доступа: http://neorusedu.ru/activity/realizatsiya-dostupa-k-onlayn-kursam-po-printsipu-odnogo-okna, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.04.2020).

References

1. Abdrahmanova G. I., Kovaleva G. G. O chem govoryat tsifry [What are the numbers talking about?]. *Narodnoe obrazovanie* [Public Education], 2011, no. 10, pp. 48–51.

2. Aetdinova R. R. Analiz i klassifikatsiya riskov tsifrovizatsii obrazovaniya [Analysis and classification of the risks of digitalization of education] // *Obrazovanie cherez vsyu zhizn: nepreryvnoe obrazovanie v interesakh ustoychivogo razvitiya : materialy XVII Mezhdunarodnoy konferentsii* [Education Throughout Life: Continuing Education for Sustainable Development : materials of the XVII International Conference]. St. Petersburg, Saint Petersburg State University of Economics, 2019, pp. 145–148.

3. Baeva L. V. *Sotsiokulturnye i filosofskie problemy razvitiya informatsionnogo obshchestva* [Sociocultural and philosophical problems of the development of the information society]. Astrakhan, Publishing House “Astrakhan University”, 2019. 137 p.

4. Balanovskaya A. V. *Istochniki vozniknoveniya i posledstviya realizatsii ugroz informatsionnoy bezopasnosti promyshlennykh predpriyatiy* [Sources of emergence and consequences of the implementation of threats to the information security of industrial enterprises]. Available at: https://cyberleninka.ru/article/n/istochniki-vozniknoveniya-i-posledstviya-realizatsii-ugroz-informatsionnoy-bezopasnosti-promyshlennyh-predpriyatiy/viewer (accessed 20.01.2020).

5. Zlenko N. S. Pochemu obrazovanie v Rossii nuzhdaetsya v tsifrovizatsii? [Why does education in Russia need digitalization?]. *Sbornik statey po materialam LXX studencheskoy mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Collection of articles on materials of the LXX student international scientific-practical conference]. Moscow, 2020, pp. 72–77.

6. Maykulov Zh. Zh. Prestupleniya protiv detey s ispolzovaniem Interneta [Crimes against children using the Internet]. *Kontsept* [Concept], 2017, vol. 39, pp. 2636–2640. Available at: http://e-koncept.ru/2017/970854.htm.

7. Manin A. I. *Vidy ekspertiz, provodimykh pri ispolzovanii anomaliy otdelnykh zubov dlya identifikatsii lichnosti* [Types of examinations carried out when using anomalies of individual teeth to identify a person]. Available at: https://www.mediasphera.ru/issues/rossijskaya-stomatologiya/2016/1/082072-64062015018 (accessed 20.01.2020).

8. Markelov K.A., Brumshteyn Yu.M., Azhmuhamedov I.M. Analiz sushchestvuyushchikh i perspektivnykh napravleniy ispolzovaniya distantsionnykh obrazovatelnykh tekhnologiy v rossiyskikh regionalnykh gosudarstvennykh vuzakh [Analysis of existing and promising areas of the use of distance learning technologies in Russian regional state universities]. *Distantsionnye obrazovatelnye tekhnologii : materialy IV Vserossiyskoy nauchno-prakticheskoy konferentsii (s mezhdunarodnym uchastiem)* [Remote educational technology : materials of the All-Russian Scientific and Practical Conference IV (with international participation)], 2019.

9. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii : Federalnyy zakon № 149-FZ ot 27 iyulya 2006 g. : prinyat Gosudarstvennoy Dumoy 8 iyulya 2006 g. [On information, information technologies and information protection : Federation law no. 149-FL of 27 July 2006 : adopted by State Duma 8 July 2006]. *Sobranie zakonodatelstva Rossiyskoy Fedieratsi* [Collection of legislation of the Russian Federation], 2006.

10. O personalnykh dannykh: Federalnyy zakon № 149-FZ ot 27 iyulya 2006 g. : prinyat Gosudarstvennoj Dumoj 8 iyulya 2006 g. [On personal data : Federation law no. 149-FL of 27 July 2006 : adopted by State Duma 8 July 2006]. *Sobranie zakonodatelstva Rossiyskoy Federatsii* [Collection of legislation of the Russian Federation], 2006.

11. *Opisanie proekta «Sovremennaya tsifrovaya obrazovatelnaya sreda»* [Description of the project “Modern digital educational environment”]. Available at: http://neorusedu.ru/about (accessed 20.01.2020)

12. Paniotto V. I., Maksimenko V. S. *Kolichestvennye metody v sotsiologicheskikh issledovaniyakh* [Quantitative methods in sociological research]. Kiev, Naukova Dumka Publ., 1982. 272 p.

13. Prioritetnyy proekt «Sovremennaya tsifrovaya obrazovatelnaya sreda v Rossiyskoy Federatsii», utverzhdennyy Prezidiumom Soveta pri Prezidente RF po strategicheskomu razvitiyu i prioritetnym proektam (protokol ot 25 oktyabrya 2016 g. № 9)], [Priority project "Modern digital educational environment in the Russian Federation"]. *Konsultant* [Consultant]. Available at: http://www.consultant.ru/ (accessed 20.01.2020)

14. *Prioritetnyy proekt «Tsifrovaya shkola»* [Priority project "Digital school"]. Available at: http://government.ru/projects/selection/693/30822/ (accessed 20.01.2020)

15. *Realizatsiya dostupa k onlayn-kursam po printsipu «odnogo okna»* [Realization of access to online courses on a one-stop basis]. Available at: http://neorusedu.ru/activity/realizatsiya-dostupa-k-onlayn-kursam-po-printsipu-odnogo-okna (accessed 10.04.2020).

DOI 10.21672/2074-1707.2020.51.1.083-093
УДК 004.056

ИССЛЕДОВАНИЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ И ПОДТВЕРЖДЕНИЯ ЛЕГИТИМНОСТИ ДОСТУПА НА ОСНОВЕ ДИНАМИЧЕСКИХ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ[1]

Статья поступила в редакцию 19.04.2020, в окончательном варианте – 10.09.2020.

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент, ORCID: https://orcid.org/0000-0001-9974-7144, e-mail: putyato.m@gmail.com

***Макарян Александр Самвелович*,** Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент, e-mail: msanya@yandex.ru

Чич Шамиль Муратович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

студент, e-mail: shama_chich@icloud.com

Маркова Валентина Константиновна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

студентка, e-mail: markokovt@yandex.ru

Биометрические методы основаны на определении личности человека по присущим только ему признакам. В статье рассматриваются характеристики клавиатурного прочерка как динамической биометрической характеристики личности. Осуществляется анализ и выбор характеристик, необходимых для идентификации. Алгоритм процесса формирования эталонного образца клавиатурного почерка основан на основе фиксации временных параметров. Рассматриваются классические статистические подходы идентификации пользователей по клавиатурному почерку. Исследованиями установлено, что подходы для сбора и анализа параметров подходят и для формирования клавиатурного почерка на мобильных устройствах. Отмечено, что использование клавиатурного почерка в качестве единственного фактора аутентификации на мобильном устройстве пока не достигает достаточной точности, но вполне приемлемо в качестве дополнительного фактора аутентификации. Для решения задачи идентификации предложено использовать клиент-серверное приложение, дана его характеристика, проведены тестовые испытания и проведен анализ полученных результатов.

Ключевые слова: кибербезопасность, форензика, динамические биометрические характеристики, идентификация, биометрия, защита данных, клавиатурный почерк, защита информации, база данных

[1] Статья подготовлена в рамках исследований, проводимых при реализации гранта РФФИ (2.10.187 «Разработка теоретических основ и алгоритмов функционирования адаптивных систем управления ситуационных центров на основе методов искусственного интеллекта»).