МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Обеспечение информационной безопасности при использовании социальных сетей и мессенджеров в образовательном процессе профессиональной образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
84,63% авторского текста

Работа рекомендована к защите
«24» января 2024 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Левитин Радий Валерьевич

Научный руководитель:
кан.пед.н., доцент кафедры АТ,ИТиМОТД
Гафарова Елена Аркадьевна

Челябинск
2024

Содержание

ВВЕДЕНИЕ

Актуальность исследования. Образовательная среда в настоящий момент характеризуется высоким уровнем конкуренции и сталкивается с рядом вызовов со стороны постоянно развивающегося мира и изменяющихся настроений общества. Знания быстро устаревают, как и педагогические технологии для их преподавания.

Внедрение новых информационных технологий в современную жизнь меняет традиционные формы общения людей. Особенно это заметно с появлением и развитием социальных сетей, позволяющих использовать интернет-технологии для общения людей разных стран, культур и конфессий. Огромная популярность социальных сетей в молодежной среде и практически стопроцентная обеспеченность обучающихся персональными средствами вычислительной техники позволяет перевести на новый уровень обмен образовательной информацией как между педагогом и студентами, так и между самими студентами. Все это не только способствует активизации и модернизации процесса обучения, но и создает новые угрозы безопасности личности, связанные с бесконтрольным распространением контента сомнительного содержания.

Однако главная опасность, которую порождает использование социальных сетей – вовсе не распространение нежелательной информации и формирование огромного простора для деятельности злоумышленников. По нашему мнению, основной проблемой является обеспечение безопасности личных данных пользователя.

Следует отметить, что добровольное предоставление пользователями значительного объема идентификационной, визуальной и прочей персональной информации делает эти сети потенциальным источником угроз информационной безопасности личности. Соответственно, представляется интересным не только изучить дидактический потенциал этого современного средства коммуникации, но и рассмотреть социальные сети как объект защиты

при использовании социальных сетей и мессенджеров в образовательном процессе.

Социальные сети и мессенджеры давно стали неотъемлемой частью нашей жизни. Практически каждый имеет, как минимум один, а чаще несколько аккаунтов в социальных сетях. На данный момент насчитывается порядка десятка социальных сетей, охватывающих по общей численности более 70% населения земного шара. Социальные сети используются для совершенно различных целей и задач: продажи, образование, маркетинг и продвижение, самовыражение, коммуникации, места. Хотя изначально они предназначались исключительно для оперативного общения, знакомств и обмена новостями.

Другими словами, первичная фундаментально-базовая функция социальных сетей и сообществ – коммуникативная, а следующая по значимости – развлекательная. Именно поэтому наиболее популярные сообщества в социальных сетях и мессенджерах посвящены различного рода обсуждениям и площадкам для продвижения развлекательного контента. Поскольку аудитория социальных сетей и мессенджеров постоянно растет, то не удивительно, что туда пришла сфера товаров и услуг, которая прочно заняла свою нишу.

Другим важным аспектом является то обстоятельство, что по большей части аудитория социальных сетей – это возрастная категория от 12 до 35 лет. С мессенджерами дела обстоят не так радикально, но все равно основная доля пользователей относится к указанной выше категории. Это стимулирует к активному развитию в социальных сетях проектов. Объяснение этому заключается в том, что молодежь наиболее восприимчива и активна в социальной среде, особенно в сети Интернет.

С развитием технологий в отношении гаджетов, которые прочно вошли в наш обиход, возросла и вовлеченность в использование сетевых ресурсов в общем, и социальных 12 сетей, а также мессенджеров в частности. Появился даже такой термин, как «экранное время», который характеризует

длительность пребывания пользователя в обществе своего гаджета [15]. Это привело к тому, что пользователи социальных сетей стали не только общаться там, но и совершать покупки, организовывать мероприятия, проводить тренинги, консультации, обмениваться опытом. Сам интерфейс социальных сетей своим развитием располагал к этому. Это выражалось в ряде новых инструментов: «сообщества», «диалоги», «онлайн-трансляции» и «стримы» и т.п. Другими словами, с развитием технологий резко расширилась область профилизации социальных сетей.

Следовательно, ученые, преподаватели также стали рассматривать данную среду как потенциальную площадку для реализации обучения. Первые обращения в сторону социальных сетей, как дополнительного педагогического ресурса в трудах зарубежных ученых датируются 2010 годом. Ученые стали рассматривать социальные сети как дополнительный ресурс в области дистанционного образования. Также они, предполагали, что из педагогических ресурсов при правильном подходе возможно сделать хорошо посещаемые сетевые ресурсы, где будет не только образовательная, но и некая социально-корпоративная среда. Другими словами, первоначально ученые рассматривали социальные сети не как территорию для реализации педагогических инициатив, а, наоборот, возможность трансформации педагогических образовательных ресурсов в профильные социальные сети «по интересам». Но важно отметить, что современные социальные сети выросли из профессиональных форумов, и инициатива трансформации сетей является своего рода возрождением форумов на ином уровне.

Если рассматривать с точки зрения органичного развития, то необходимо оценить возможность использования уже известных социальных сетей в качестве дидактического средства обучения. Тем не менее, социальные сети обладают рядом особенностей, которые могут не просто осложнять их применение в образовательных целях, но и рассматриваться как косвенные и даже прямые источники угроз информационной безопасности (ИБ) как образовательного процесса в целом, так и личностям его участников.

Угрозы ИБ имеют различную природу и могут быть реализованы с применением специальных программных средств или технологий, недоступных подавляющему большинству пользователей социальных сетей в силу отсутствия у них соответствующей профессиональной компетенции.

В связи с тем, что социальные сети с каждым годом становятся все популярнее и более востребованными, усиливается общественный запрос на обеспечение их безопасного использования и защиты от связанных с ними рисков, вызовов и угроз. Преподаватели, инициирующие применение социальных сетей в образовательном процессе, не обладают профессиональными компетенциями в области информационной безопасности и, в силу этого, чаще всего оказываются не в состоянии обеспечить требуемый уровень защищенности пользователей созданных ими сообществ от несанкционированного доступа к персональной информации и от других информационных угроз. Для решения этой проблемы в масштабах всей отечественной образовательной системы необходима модернизация образовательного процесса подготовки специалистов по информационной безопасности, направленная на обучение сопровождению социальных сетей. Осуществление такой подготовки в образовательных организациях среднего профессионального образования позволит оперативно удовлетворять спрос на таких специалистов и, тем самым, повысит конкурентоспособность организаций СПО на рынке образовательных услуг.

Это определило *проблему исследования*, заключающуюся в необходимости снижения остроты существующего противоречия, когда, с одной стороны, имеется социальная и образовательная потребность в использовании социальных сетей и мессенджеров в образовательном процессе, а, с другой стороны, отсутствует системное обеспечение информационной безопасности участников и пользователей названных сетевых коммуникационных платформ.

Таким образом, можно сделать вывод, что *тема исследования* «Обеспечение информационной безопасности при использовании социальных

сетей и мессенджеров в образовательном процессе профессиональной образовательной организации» является актуальной, а полученные результаты имеют важное практическое значение.

Цель исследования: теоретико-методическое обоснование и разработка рекомендаций по использованию социальных сетей и мессенджеров в образовательном процессе в условиях информационной безопасности (на базе исследования - ГБПОУ «Челябинский профессиональный колледж»).

Объект исследования: использование социальных сетей и мессенджеров в образовательном процессе профессиональной образовательной организации.

Предмет исследования: обеспечение информационной безопасности при использовании социальных сетей и мессенджеров в образовательном процессе профессиональной образовательной организации.

Гипотеза исследования: состоит в предположении об эффективности обеспечения информационной безопасности при использовании социальных сетей и мессенджеров в образовательном процессе профессиональной образовательной организации при условии выполнения разработанных рекомендаций.

Задачи исследования:

– проанализировать понятия «социальные сети» и «мессенджеры»;

– описать обеспечение информационной безопасности в социальных сетях и мессенджерах;

– проанализировать педагогическую практику по применению мессенджеров и социальных сетей в образовательном процессе;

– разработать рекомендации по использованию социальных сетей и мессенджеров в образовательном процессе на базе исследования - ГБПОУ «Челябинский профессиональный колледж».

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод (анализ документации образовательной организации); анализ и сопоставление

имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты и выбора средств; метод апробации результатов.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Кривоухов А.А., Тумбинская М.В., Муромцева А.В.

Практическая значимость работы заключается в разработке рекомендаций по использованию мессенджеров и социальных сетей в образовательном процессе и выборе средств защиты для обеспечения информационной безопасности ГБПОУ «Челябинский профессиональный колледж»; возможности применения разработанных рекомендаций в других учебных заведениях СПО.

Апробация результатов исследования и их внедрение. Результаты докладывались и обсуждались:

− на Международной научно-практической конференции «Султангазинские чтения-2023» «Актуальные вопросы развития современного образования», 2023 г.,

− на Международной научно-практической конференции «Фундаментальные научно-практические исследования: актуальные тенденции и инновации», 2023 г.

База исследования: ГБПОУ «Челябинский профессиональный колледж».

Структура магистерской диссертации: работа состоит из введения, двух глав, заключения, списка использованных источников.

ГЛАВА 1 НАУЧНО-МЕТОДИЧЕСКИЕ ОСНОВАНИЯ ДЛЯ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

1.1 Мессенджеры и социальные сети – новое явление информатизации образования и новые дидактические средства

На современном этапе наблюдается всестороннее массовое внедрение информационных технологий во все сферы образования. Ведущей целью цифровизации системы образования является превращение современных информационных ресурсов и информационно-коммуникационных технологий в ресурс образовательного процесса, обеспечивающий формирование качественно новых результатов образования. Появление информационно-коммуникационных технологий не могло не повлиять на изменение стратегии управления образовательным учреждением. Это означает, что необходимы организационные изменения по всем направлениям деятельности образовательного учреждения, обеспечивающие введение современных технологий в систему учебной, воспитательной, методической и управленческой деятельности, формирование цифровой образовательной среды образовательной организации.

Информационные и коммуникационные технологии сегодня стали одним из важнейших факторов, влияющих на развитие общества. Они не только прочно закреплены в государственных структурах, институтах гражданского общества, в экономической и социальной областях, науке и образовании, культуре, но и в повседневной жизни людей. Движение к информационному обществу - это путь вперед для человеческой цивилизации. За последние несколько лет изменились способы и формы общения в Интернете. Сегодня наиболее распространенным и доступным средством коммуникации и самой популярной услугой, привлекающей внимание большей части интернет-аудитории, являются социальные сети [1].

С появлением социальных сетей и различных мессенджеров их востребованность у пользователей только растет. Возможности применения постоянно множатся и уже присутствуют во всех сферах нашей жизни.

Социальные сети - достаточно недавнее, но популярное явление в Интернете. Социальная сеть (от англ. social networking service) - платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений. Поскольку социальная сеть состоит из людей и «сообществ», а люди и сообщества в социальной сети связаны отношениями, другими словами, социальная сеть - это интернет-сервис, целью которого является создание онлайн-сообщества пользователей, объединенных определенными признаками: хобби, интересы или профессиональная принадлежность.

Сам термин «социальная сеть» был введен в 1954 г. английским социологом Джеймсом Барнсом. Так, ученый определил совокупность узлов, которыми являются социальные объекты (общность, социальная группа, индивид). Более точная формулировка встречается у Д. М. Бойд и Н. Б. Элисон, которые называют виртуальной социальной сетью (social network site) базирующийся на интернет-технологиях сервис, который позволяет отдельным пользователям: — создавать открытые (публичные) или частично открытые профили пользователей; — создавать список пользователей, с которым они состоят в социальной связи; — иметь доступ к спискам коммуникаций «друзей», то есть к социальным сетям других пользователей внутри системы. Ученый Д. Гилпин определяет социальные сети как интерактивные онлайн-СМИ, которые выступают в качестве каналов для 11 отношений и передачи информации. А. Хэндли и А. Чапмэн под социальными сетями понимают неуклонно растущую и развивающуюся коллекцию онлайновых инструментов, платформ и приложений, которые позволяют всем нам взаимодействовать и обмениваться информацией.

Под термином «социальная сеть» в области информационных технологий понимают интерактивный многопользовательский веб-сайт,

контент которого наполняется самими участниками сети. Это определение отличается от используемого в социологии, где под термином «социальная сеть» принято понимать социальную структуру, состоящую из группы узлов, которыми являются социальные объекты, и связей между ними.

Основными принципами социальной сети являются:

− идентификация – возможность указать информацию о себе (школу, институт, дату рождения, любимые занятия, книги, кинофильмы, умения и т. п.);

− присутствие на сайте – возможность увидеть, кто в настоящее время находится на сайте, и вступить в диалог с другими участниками;

− отношения – возможность описать отношения между двумя пользователями (друзья, члены семьи, друзья друзей и т. п.);

− общение – возможность общаться с другими участниками сети (отправлять личные сообщения, комментировать материалы);

− группы – возможность сформировать внутри социальной сети сообщества по интересам;

− репутация – возможность узнать статус другого участника, проследить его поведение внутри социальной сети;

− обмен – возможность поделиться с другими участниками значимыми для них материалами (фотографиями, документами, ссылками, презентациями и т. д.).

Мессенджер — это программа или веб-сервис для быстрого обмена сообщениями. Обычно речь идет не только о текстовых сообщениях, но и о текстовых файлах, картинках, видео; некоторые мессенджеры позволяют проводить голосовые и видеоконференции. Таких программ сейчас очень много, и самые популярные из них — Viber, WhatsApp, Facebook Messenger, Skype, ICQ, Telegram.

Использование мессенджеров и социальных сетей в обучающих целях становится новой социальной практикой и привлекает внимание ученых [6].

Опыт использования социальной сети в обучении описан многими исследователями. Например, Н. В. Родионова и М. Н. Яранская внедряют социальные сети в учебный процесс в качестве средства для постоянного взаимодействия преподавателей и студентов. Ими отмечены широкие и разнообразные функциональные ресурсы сети Вконтакте, а именно — организация групп, отслеживание активности студентов, размещение информации различных форматов. Помимо этого, преподаватели имеют возможность провести различные контрольные мероприятия, такие как тестирование, опрос, коллективное обсуждение темы [9, с. 66-69].

Значение социальных сетей для обучения и развития пока не определено, так методисты скептически относятся к возможности использования данного объекта информационных технологий, как педагогического средства обучения. В обществе сложилась четкая позиция: социальные сети – среда для развлечений и траты свободного времени от учебы и работы. Однако в педагогической деятельности устройство социальных сетей можно использовать для ряда организационных задач:

– эффективная организация групповой учебной работы;

– долгосрочную проектную деятельность;

– международные обмены, в том числе научно-образовательные, мобильное непрерывное образование и самообразование;

– организация работы людей, находящихся в разных городах или даже странах.

Можно выделить следующие преимущества использования именно социальной сети в качестве учебной площадки [3].

1. Привычная среда для обучающихся.

2. В социальной сети человек выступает под своим именем-фамилией.

3. Технология Wiki позволяет всем участникам сети создавать сетевой учебный контент.

4. Возможность совместной работы.

5. Наличие форума, стены, чата.

6. Каждый обучающийся – участник может создать свой блог, как электронную тетрадь.

7. Активность участников прослеживается через ленту друзей.

8. Удобно использовать для проведения проекта.

9. Подойдет в качестве портфолио как для обучающегося, так и для педагога.

Среди преимуществ использования мессенджеров в учебном процессе можно выделить следующие:

– привычность интерфейса и самой коммуникативной среды для обучающихся позволяет сэкономить время на их адаптацию к новому образовательному пространству;

– многие ресурсы, являясь бесплатными, тем не менее, обладают значительным функционалом для реализации образовательных задач;

– функционал социальных сервисов позволяет не только хранить, но и создавать цифровой контент, а также делиться им; в конечном счете обучающиеся участвуют в процессе создания знаний и обмена ими;

– мультимедийные возможности видео-, аудио-, интерактивных социальных сервисов позволяют значительно разнообразить представление учебного материала;

– учебная деятельность с помощью мессенджеров способствует развитию мотивов обучения, связанных с самореализацией, самовыражением, отсутствием боязни потерпеть неудачу, просоциальным поведением и т. д.;

– применение технологий форумов, блогов, вики, других средств позволяет обучающимся самостоятельно или совместно создавать учебный материал, что, в свою очередь, стимулирует самостоятельную познавательную деятельность, способствует вовлечению обучающихся в образовательный процесс, развивает критическое мышление, рефлексию и др.;

– обучение с помощью мессенджеров позволяет формировать у обучающихся XXI века навыки, связанные с умением не только найти информацию, но и переработать ее и на ее основе создать новую;

– поддержка обучения в среде социальных сервисов позволяет не ограничиваться только формальными занятиями в аудитории, а расширить образовательное пространство, предоставляя педагогическую поддержку во внеаудиторное время.

Существует ряд проблем, связанных с использованием мессенджеров и социальной сети в образовательном процессе. Например, отсутствие сетевого этикета участников, невысокий уровень мотивации и ИКТ-компетенций преподавателя, высокая степень трудозатрат по организации и поддержке учебного процесса для преподавателя, частое отсутствие открытого доступа к социальным сетям из учебных аудиторий.

Кроме того, преподаватель должен интуитивно чувствовать обучаемую аудиторию и целесообразно подбирать под нее учебную площадку и инструменты. Для решения названных проблем нужно создавать условия для повышения ИКТ-квалификации преподавателей, осуществлять материальное и моральное поощрение педагогов, активно использующих новые технологии, разрабатывать эффективные методики применения социальных сетей в образовательном пространстве.

Партнерское сотрудничество педагогического сообщества с разработчиками социальных медиа и законодательное регулирование этой сферы может обеспечить условия для принятия конструктивных решений проблемы информационной безопасности виртуальных сетей. Конечно, социальные сети не являются основным средством сетевого обучения, но их возможности в решении образовательных задач сегодня недооцениваются профессиональным сообществом.

Социальные сети предлагают отличные возможности для социализации, например, такие как возможность общаться с людьми, живущими по всему миру, развитие способности быть членом группы, что невозможно в реальной жизни из-за географических и физических ограничений, способствует самовыражению и способности не только получать информацию, но и делиться ею. Конечно, есть проблемы с конфиденциальностью информации и

зависимостью от социальных сетей, однако правильное использование предоставляемых ими возможностей имеет огромное положительное значение. Сегодня можно говорить об интенсификации процесса использования интернет-технологий в непрерывном образовании. В связи с этим возникает ряд острых проблем, которые являются предметом обсуждения ученых, сочетающих развитие образования с активным использованием Интернет-технологий, создание единого неформального образовательного пространства.

Любой мессенджер — неформальная, всегда доступная площадка, канал связи между директором организации и руководителями структурных подразделений. В целом мессенджер — универсальный канал связи, который можно использовать для общения и с родителями, и с коллегами, и с обучающимися. Если беспокоит необходимость получать обилие обратной связи в группе, можно завести в мессенджере свой канал [7].

Зарубежные авторы выделяют следующие преимущества использования социальных сетей в качестве дополнительного инструмента профессионального обучения:

− индивидуализировать обучение;

− дать слушателю возможность повторять содержание курса столько, сколько ему нужно;

− независимость от времени и места;

− повысить успешность, качество и эффективность образования за счет использования ИКТ в образовательном процессе;

− возможность учиться более систематично и за меньшее время благодаря достижениям компьютерных технологий;

− позволяет создавать визуальный и слуховой дизайн учебной среды;

− приложения для архивирования содержания курса и синхронизации занятий (виртуальный класс);

− возможность формирования добровольного поведения обучаемыми с целью улучшения исследовательских навыков и знаний по сравнению с традиционными программами;

− возможность повышения навыков обучающихся и педагогов для достижения, оценки и эффективного использования полученных знаний.

Важным преимуществом социальных сетей является то, что пользователь определяется одновременно как потребитель и как создатель информации. Он занимает активную позицию, то есть создает и потребляет контент.

Следует отметить, что социальные сети не предоставляют слушателю тех же возможностей для объяснения и уточнения, которые возникают при личном общении. Поэтому они сталкиваются с некоторыми трудностями при письменно выражении своих взглядов и идей в социальных сетях, поскольку многие участники курсов предпочитают выражать свои мысли устно. В то же время, чтобы успешно учиться через социальные сети, пользователям необходимо приобрести навыки письма, чтобы иметь возможность свободно выражать свои идеи и мнения.

Сети можно разделить на:

− социальные сети общего формата;

− профессиональные социальные сети;

− социальные сети по интересам.

В электронной сети каждый имеет возможность выразить свою точку зрения, встретить единомышленников, пообщаться на любую тему, поделиться опытом, научить других, позволить вам стать тем, кем хотел бы быть человек; можно заводить новые знакомства; можно найти знакомых и друзей, контакты, которые давно утеряны, а люди навсегда остались в памяти. Но у социальных сетей есть не только преимущества, но и недостатки. Слово «сеть» невольно появляется в связи с рыболовной сетью или паутиной. И это, в общем, недалеко от истины. В социальных сетях пользователи надолго пропадают. Прежде всего, это психологическая зависимость от них, потому

что многие пользователи проводят на сайте дни, заменяя виртуальное общение реальным.

Споры о том, вредны или полезны социальные сети, также не утихают среди педагогов и психологов, но однозначного мнения по этому поводу до сих пор нет. По мнению некоторых психологов, в социальных сетях нет необходимости, а некоторые считают, что социальные сети опасны, это просто онлайн-наркотик.

Пришло время для новых социальных сетей, которые будут более эффективно выполнять образовательные функции за счет структурирования информации, за счет введения определенных правил, соблюдения внутрисетевой этики. Основная задача этих сетей - обеспечить вхождение мирового сообщества, в том числе России, в шестой технологический уклад. Функцией этих сетей будет не только информация и коммуникация, но и полноценное информальное образование взрослого населения. По определению О.В. Павловой, информальное образование представляет собой процесс формирования активной жизненной позиции, условие социальной адаптации.

Научные междисциплинарные исследования человека, при котором «отношения и социальные связи становятся более независимыми и основываются на индивидуальных характеристиках человека, его творческого поиска, возросших возможностях выбора своей социальной ниши, на основе усиления социальной мобильности, снижения зависимости человека от определенных обстоятельств» [3].

Основными проблемами использования социальных сетей в образовании можно считать:

1. Педагоги часто имеют низкий уровень мотивации и навыков использования ИКТ, что не позволяет им активно использовать социальные сети в своей профессиональной деятельности.

2. Высокий уровень трудозатрат на организацию и сопровождение учебного процесса в среде непрерывного обучения педагога;

3. Отсутствие открытого доступа к социальным сетям из аудиторий в образовательных организация.

Использование форумов и вики-технологий в виртуальных учебных группах позволяет всем участникам независимо или совместно создавать онлайн-образовательный контент, стимулирующий независимую познавательную деятельность. Возможность совмещения индивидуальных и коллективных форм работы способствует лучшему пониманию и усвоению материала, и построению индивидуальных образовательных траекторий. Коммуникативное пространство, общее для всех участников образовательного процесса, позволяет коллективно оценивать процессы и результаты работы, наблюдать за развитием каждого участника и оценивать его вклад в коллективное творчество. Высокий уровень взаимодействия гарантирует непрерывность учебного процесса, выходящего за рамки аудиторных занятий.

Не каждый преподаватель способен создать сайт или написать программу для компьютера (смартфона). Когда мы говорим о цифровизации образования, речь должна идти не только (и даже не столько) о создании новых цифровых продуктов, но и об использовании уже существующих, тех, к которым мы привыкли в повседневной жизни. Их применение не требует специальных навыков, продолжительного обучения, специализированных классов, разработки (покупки) и установки программного обеспечения, выделения дополнительных часов в программе. Полагаем, что именно такое решение — использовать уже существующие мессенджеры и социальные сети — является методически правильным. Речь должна идти в первую очередь о новых принципах организации учебного процесса.

Таким образом, сегодня мессенджеры и социальные сети — это новая среда обучения, где студенты в основном читают или просматривают учебный контент, делятся комментариями или аудио- и видеоматериалами собственного производства, при создании которых применяются те знания, которые ранее были приобретены. Не следует игнорировать современную тенденцию, которая заключается в том, что процесс обучения в наши дни

происходит не только в стенах образовательной организации, но и после аудиторных занятий, а возможно, и одновременно.

Использование мессенджеров и социальных сетей расширяет возможности педагога, как для организации аудиторной работы, так и для эффективной организации самостоятельной работы. Они помогают увеличить скорость коммуникации преподавателя и студентов, с другой стороны, требует дополнительных временных затрат на подготовку контента, выкладываемого в Сети, и модерацию аккаунта. Необходимо подчеркнуть, что использование социальной сети повышает авторитет педагога и способствует созданию доверительных отношений.

Социальные сети имеют и свои недостатки: переизбыток развлекательной информации, отсутствие жесткого контроля, игнорирование этических моментов, а также неточность содержания. В целом, использование социальных сетей в образовательном контексте имеет спорный характер и следует учитывать как преимущества, так и недостатки, для того чтобы сделать его более эффективным как для педагогов, так и для студентов. Однако социальные сети могут стать дополнительным средством обучения.

Таким образом, в современном обществе актуализируется проблема повышения эффективности и доступности образования путем использования информационных технологий, в частности, мессенджеров и социальных сетей.

1.2 Обеспечение информационной безопасности в популярных мессенджерах и социальных сетей

Современный период трансформации мировой и отечественной экономики способствует усилению интеграционных процессов между деятельностью и цифровыми технологиями. В рамках данной тенденции прослеживаются такие процессы, как развитие информационных технологий, разработка интеллектуальных технологий, практическое применение высокоинтеллектуальных инноваций в рамках совершенствования процессов образовательной организации и развитие мессенджеров и социальных сетей,

которые используются как населением (как средство коммуникации и связи), так и субъектами образовательного процесса.

Одним из последних процессов выступает и развитие цифровых технологий в составе комплексной системы информационной безопасности образовательной организации, которые совершенствуют деятельность образовательных организаций по сбору, обработке, анализу и хранению информационных данных. Их задачей выступает формирование основы и фундамента информационной безопасности организации, что крайне актуально в виду развития цифровой экономики Российской Федерации.

Актуальность заключается в том, что при развитии социальных сетей, образовательные организации сталкиваются с новой технологией, где основы информационной безопасности еще не сформированы. При этом, социальные сети, а именно информация в ее рамках, становится желаемым объектом мошеннических операций и незаконных действий по краже личных данных, которые могут быть использованы при аутентификации на различных ресурсах и площадках.

Проблемой исследования выступает низкий уровень обеспечения информационной безопасности в мессенджерах и социальных сетях, который приводит к возможным негативным последствиям, среди которых потеря конфиденциальной информации и кража персональных данных пользователей.

Обеспечение информационной безопасности в мессенджерах и социальных сетях - актуальная проблематика не только для корпоративных структур, коммерческая информация и интеллектуальный капитал которых находится в поле поиска злоумышленников, но и для образования.

Исходя из этого, важно определить то, какие инструменты и механизмы необходимо применять, чтобы формировать информационную безопасность виртуального пространства социальных сетей, сохраняя интересы всех его участников.

Кривоухов А.А. в ходе своей научной работы установил, что социальные сети имеют низкий уровень безопасности информации и данных их пользователей. По этой причине, необходимо формирование компетенций в области информационной безопасности, как составляющей информационной культуры современного человека [7].

Тумбинская М.В. описывает, что ключевой причиной информационной небезопасности пользователей социальных сетей является таргетированная информация, вызывающая информационные атаки на мнение людей [8].

Муромцева А.В. рассматривая особенности построения, взаимодействия и характеристики социальных сетей в Интернете, выявила основные проблемы информационной безопасности участников социальных сетей [2].

При этом, ключевым объектом информационной безопасности в социальных сетях выступает защита личных и персональных данных, которые выступают набором организационных, технических и организационно - технических мероприятий, направленных на защиту информации, что относится к конкретной личности.

Очевидно, что публикация персональных данных в социальных сетях, а также их изменение без согласия субъекта, приводит к негативным последствиям для последнего.

Анализ состояния исследований показал, что известные работы в основном направлены на обеспечение нормативно-правовых или информационно-технических аспектов информационной безопасности в информационном пространстве, а также на мониторинг инцидентов информационной безопасности, на анализ качественных или количественных характеристик связей узлов в социальных сетях, кластеризацию полученных данных, систематизацию, хранение и пр.

Вредоносная информация, нежелательная информация, информационное воздействие, противоправная информация все эти понятия рассматриваются экспертами зачастую как синонимы.

Рассмотрим понятие «информация» (I – information). В общем представлении – это сведения об объектах и явлениях, их параметрах, свойствах и состоянии, которые подлежат сбору, накоплению, хранению, предобработке, обработке, преобразованию, непосредственному использованию и передаче [20].

Информация входит в понятия информационная сфера, информационное пространства.

Согласно Доктрине РФ, «информационная сфера» (IR – information realm) – это совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений [21].

Понятие «информационного пространства» (IA – information area) трактуется как сфера человеческой деятельности, связанная с созданием, преобразованием и потреблением информации, включающая в себя всю совокупность информационных ресурсов данного общества [22, 23].

Зачастую вредоносная информация воспринимается в современном научном сообществе как элемент информационной атаки (воздействия). Понятие «информационного воздействия» (IE – information effect) трактуется как основной поражающий фактор информационной войны, представляющий собой воздействие информационным потоком на объект атаки – информационную систему или ее компонент, с целью вызвать в нем в результате приема и обработки данного потока заданные структурные и/или функциональные изменения [24].

Информационный объект (IO – information object) – это логически цельный блок информации, представленный в определенной фиксированной

форме, который создан и используется в ходе информационной составляющей деятельности человека [25].

В связи с необходимостью классификации вредоносной информации, сформулируем определение, опираясь на классификацию типов информации в сети Интернет (Int) в общем.

Классификация типов информации в сети Интернет основана на понятии информационного объекта, который является логически цельным блоком информации, представленным в определенной фиксированной форме, созданным и используемым в ходе информационной составляющей деятельности человека.

Введем понятие вредоносной информации – это отдельный информационный объект и/или совокупность объектов в сети Интернет, содержащий запрещенную или ограниченную к распространению информацию. В дальнейшем предполагается, что понятие вредоносная информация включает в себя все множество опасной информации.

С точки зрения обеспечения государственной безопасности под категорию вредоносной информации попадают следующие виды информации:

1) информация, попадающая под критерии оценки материалов и (или) информации, позволяющие идентифицировать ее, как запрещенную к распространению в Российской Федерации [26];

2) информация, включенная в федеральный список экстремистских материалов [27];

3) информационный объект, включенный в реестр блокировок.

На примере образовательной организации:

1) конфиденциальная информация;

2) персональные данные;

3) информация для служебного пользования.

На примере системы родительского контроля:

1) информация, имеющая возрастные ограничения;

2) информация, ресурсы, доступ к которым ограничен со стороны родителя.

В рамках исследования использованы следующие определения.

«Информация» – сведения (сообщения, данные) независимо от формы их представления [20]. Понятие «материалы», которое часто встречается в современном законодательстве, приравнивается по смыслу к понятию «информация».

В п. 6 ст. 10 ФЗ от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) «Об информации, информационных технологиях и о защите информации» говорится о том, что запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность [28].

«Распространение информации» – это все действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

«Источник» (Source) – это страница в социальной сети, на котором опубликована информация доступная неопределённому кругу лиц.

«Сообщение» – это информационный объект, содержащий текст, созданный и опубликованный в процессе информационного обмена в социальной сети.

Виды вредоносной информации в социальных сетях.

Из множества классификаций видов вредоносной информации в социальных сетях можно выделить 2 основные концепции:

Классификация информационных объектов по содержанию [28-32]:

1) пропаганда либо оправдание войны;

2) пропаганда или оправдание терроризма и экстремизма;

3) пропаганда или оправдание правонарушений;

4) пропаганда расизма;

5) пропаганда национальной ненависти;

6) пропаганда религиозной ненависти;

7) осквернение, оскорбление исторической памяти, символов воинской славы;

8) осквернение, оскорбление государственных символов;

9) оскорбление религиозных чувств верующих;

10) пропаганда деструктивных, нетрадиционных ценностей, установок;

11) оправдание насилия, жестокости;

12) оправдание девиантного поведения;

13) пропаганда, оправдание действий опасных для жизни человека;

14) заведомо ложная информация;

15) клевета;

16) информация, содержащая сведения о способах изготовления чего-то запрещенного;

17) рекламные объявления о покупке, продаже запрещенных товаров.

Классификация информационных объектов по дискретным признакам [33-36]:

1) дата регистрации в социальной сети;

2) время сообщений;

3) частота сообщений;

4) длина сообщений;

5) частота действий;

6) уникальность контента на странице профиля в социальной сети;

7) связь с другими участниками в социальной сети;

8) связь с сообществами;

9) география профиля;

10) география сообществ, с которыми связан профиль;

11) степень влияния;

12) количество просмотров;

13) интересы профиля;

14) история содержания профиля.

В рамках защиты информации и персональных данных со стороны пользователя - физического лица, необходимо применение следующих рекомендаций [6]:

− нельзя оставлять социальные страницы в сетях заброшенными, и в случае их неиспользования - важно удалять профиль и личные данные аккаунта;

− не принимать заявки от страниц/фейков, поскольку те могут быть использованы для кражи личных данных пользователя;

− необходимо использование сложных паролей;

− важно настроить двухфакторную аутентификацию при входе на страницу в социальной сети;

− нельзя делиться конфиденциальной информацией и важно ознакомиться со всеми пунктами пользовательского соглашения, поскольку многие социальные сети, как владельцы аккаунтов имеют право продавать личные данные третьим лицам-сторонам.

Также следует отметить следующее: что необходимо соблюдать простые требования безопасности для защиты данных от вредоносного программного обеспечения. Так, существует некоторое количество вирусов, которые перенаправляют информацию из мессенджеров с компьютеров и смартфонов. В случае, если на компьютере обрабатывается информация, содержащая персональные данные третьих лиц, необходимо соблюдать требования ФСТЭК по защите такой информации [4].

1.3 Педагогическая практика по применению мессенджеров и социальных сетей в образовательном процессе

Развитие веб-технологий и их влияние на современное общество привело к изменению традиционных сфер коммуникаций, изменению способов и форм коммуникации в интернете. Интернет стал площадкой для

безбарьерной передачи и обмена информацией, знаниями и общения людей разных городов и стран.

Темп роста всемирной сети высок и продолжает нарастать как за счёт увеличения количества пользователей глобальной сети Интернет, так и за счёт роста объёмов информации в самом Интернете.

Общение в социальных сетях сегодня стало частью повседневной жизни миллионов людей во всем мире. Интернет сделал возможным общение людей в любой момент времени и в глобальном масштабе, а социальные сети представляют собой конкретный инструмент, позволяющий выстраивать взаимосвязи между людьми, активизировать социальную составляющую взаимодействия онлайн

В последнее время исследователи стараются найти новые сферы применения мессенджеров и социальных сетей в различных направлениях деятельности человека, максимально используя все возможности данного объекта информационных технологий.

Социальные сети не являются основным средством обучения, однако их возможности в решении образовательных задач недооцениваются профессиональным сообществом.

Стремительный прогресс и постоянное обновление в области информационных технологий дает возможность использовать возможности интернет технологий в качестве эффективного средства обучения. При использовании глобальной интернет сети происходит формирование информационно-образовательной среды, которая позволяет в полной мере реализовать современные технологии обучения. Использования социальных сетей как педагогического инструмента становится крайне актуальной.

Социальные сети и мессенджеры отличаются друг от друга своей общей направленностью, различными возможностями для пользователей, разными требованиями и интерфейсом. Однако есть и общие черты, присущие многим мессенджерам, социальным сетям и выделяющие их из других средств сетевого общения, таких, как блоги, форумы, чаты и гостевые книги. В

некоторых социальных сетях встроены блоги и форумы, однако в данном случае мы будем рассматривать только особенности социальной сети. Понимание этих специфических черт важно для выявления возможностей использования социальных сетей как образовательного инструмента.

Исследуя эту тему, можно выявить отличительную особенность обучения посредством социальных сетей, которую можно назвать дистанционно-интерактивным обучением, которая выражается в возможности приобретения знаний за счет интерактивности, т. е. взаимодействия с другими участниками образовательного процесса «на расстоянии», т. е. на дистанции.

Можно согласиться с мнением А.В. Хуторского: «...сегодня понятие «дистанционное образование», насыщено другим смыслом – это использование новейших телекоммуникационных технологий – интернета, сетей и так далее. Под дистанционным обучением можно понимать обучение, при котором удаленные друг друга субъекты обучения, то есть ученики и преподаватели, они осуществляют образовательный процесс с помощью этих средств телекоммуникаций».

Сегодня в современной теории дистанционного обучения существуют разнообразные модели дистанционного обучения, интеграция очных и дистанционных форм обучения; сетевое обучение (автономные сетевые курсы; информационно-предметная среда); сетевое обучение и кейс-технологии, дистанционное обучение на базе интерактивного телевидения (Two-way TV) или компьютерных видеоконференций.

Наиболее приемлема модель, основанная на интеграции аудиторных занятий (лекции, семинары, практические занятия и т. д.) и дистанционно-интерактивных форм обучения (вебинары, видеозаписи, видеоконференции, форумы, обсуждения, дискуссии, телеконференции и т. д.). Такая модель предполагает индивидуализацию и в то же время широкую интерактивность в обучении, что в современном вузовском образовании представляется наиболее перспективным, поскольку увеличивает возможности самостоятельного и группового углубления в изучаемый материал, создает условия использования

исследовательских подходов в обучении, самостоятельного и группового поиска информации для решения проблемы, умения работать с информацией индивидуально, в команде, в коммуникации.

Изучение исследований в области использования информационных технологий обнаруживает проблему организационного характера: на какой базе может быть организовано дистанционно-интерактивное обучение. Мессенджеры и социальная сеть интернета становится одной из наиболее приемлемой и применяемой платформой для данной модели обучения.

На современном этапе наблюдается всесторонне массовое внедрение социальных платформ в процесс обучения, поэтому интеграция социальных сервисов и сетей в обучение находиться на пике популярности. Не теряют своей активности и интерактивные мультимедийные технологии. Следующим шагом в интеграции социальных сетей станет создание специализированных платформ, которые позволят сформировать «социальную экосистему» внутри сайтов.

Одной из главных задач современных педагогов является поиск новых форм и методов обучения, которые были бы более эффективными, интересными и понятными для обучающихся. В этом контексте использование мессенджеров и социальных сетей может стать очень полезным инструментом для осуществления образовательного процесса.

Один из позитивных аспектов применения мессенджеров и социальных сетей – это возможность использования новых форм обратной связи между обучающимся и педагогом. Благодаря таким приложениям возможно быстро и просто делиться информацией, задавать вопросы и получать ответы на них. Это помогает преподавателю усилить контроль над образовательным процессом и оперативно отреагировать на возникающие проблемы.

Например, преподаватель может создать группу на социальной сети, где обучающиеся смогут задавать вопросы, размещать материалы и комментировать их. Также может быть использован мессенджер для организации консультаций между преподавателем и обучающимся. Это

подходит для таких занятий, как дистанционное обучение, когда необходимо обеспечить максимально быстрый и удобный доступ к материалам и консультациям.

Кроме того, использование мессенджеров и социальных сетей может стать отличной возможностью для создания проектов и участия в них. Например, в социальной сети можно создать группу для обсуждения какой-либо темы и совместной работы над проектом. Это поможет студентам развивать социальные навыки, учиться работать в команде и освоить новые знания.

Примером использования социальных сетей в обучении может быть обучение при помощи блогов и вики, где обучающиеся могут делать обзоры, создавать, комментировать, редактировать собственные и совместные письменные сетевые проекты. Кроме того, социальные сети могут использоваться для поддержания отношений между участниками конференций, семинаров, летних школ, что позволит не только улучшить эмоциональный климат группы, но и повысить качество проводимых мероприятий путем обмена идеями и замечаниями.

Применение в виртуальных учебных группах технологий форумов и вики позволяет всем участникам самостоятельно или совместно создавать сетевой учебный контент, что стимулирует самостоятельную познавательную деятельность. Возможность совмещения индивидуальных и групповых форм работы способствует большей степени понимания и усвоения материала, а также выстраиванию индивидуальных образовательных траекторий. Общее для всех участников учебного процесса коммуникативное пространство дает возможность коллективной оценки процессов и результатов работы, наблюдения за развитием каждого участника и оценки его вклада в коллективное творчество. Высокий уровень взаимодействия обеспечивает непрерывность учебного процесса, выходящего за рамки занятий. Понятность идеологии и интерфейса социальных сетей большей части Интернет-аудитории позволяет сэкономить время, минуя этап адаптации обучающихся

к новому коммуникативному пространству. Мультимедийность коммуникативного пространства предельно облегчает загрузку и просмотр в виртуальной учебной группе видео и аудиоматериалов, интерактивных приложений.

С помощью средств социальных сетей можно организовать клубную деятельность, объединив обучающихся различных регионов. Использование социальных сетей в учебно-воспитательном процессе способствует обмену информацией, повышает мотивацию обучающихся в учебной деятельности, стимулирует развитие творческих способностей и познавательный интерес. Все эти факторы положительно влияют на формирование знаний и умений.

Не стоит забывать и о таком важном моменте образовательного процесса, как связь педагога и родителей. В условиях современного жизненного ритма родители не всегда имеют возможность быть в курсе всех событий учебной жизни ребенка. Использование сетевого пространства позволит не потерять связь педагога с родителями. Социальные сети дают возможность непосредственного участия в образовательном процессе, в управлении, в оценке качества образования, в обсуждении и создании проектов, концепций, которые определяют стратегию развития образования в стране.

Сегодня в глобальной сети Интернет находятся технологии, которые можно активно использовать в процессе обучения. Одной из наиболее известных является создание учебных блогов. Легкость ведения, а также доступа позволяет публиковать информацию не только при помощи персонального компьютера, но и посредством мобильных телефонов, смартфона. Каждый студент может выложить информацию, точку зрения и другие материалы. В процессе учебы также можно делиться информацией, обсуждать конкретные детали, получать комментарии на опубликованный материал. Не менее популярны преподавательские блоги, при помощи которых можно эффективно управлять самостоятельной внеаудиторной работой обучаемых, а также создавать задания, направленные на

совершенствование навыков речевой деятельности. Обучению разным видам письма (поискового, просмотрового, ознакомительного и изучающего) способствует неограниченная возможность размещать ссылки в любом количестве на отличные друг от друга материалы. Также блоги ничем не уступают в возможности приобретения навыков говорения и аудированию. Это происходит при помощи использования подкастов, через учебные тексты радиопередач, видеосюжетов, которые находятся в свободном доступе в Интернете.

Создать учебный блог можно на следующих сайтах:

1. www.blogger.com – веб-сервис для ведения блогов, с помощью которого пользователь может завести блог, пренебрегая навыками программирования.

2. www.blog.ru – бесплатная платформа для ведения блога в рамках портала www.mail.ru. Есть один недостаток: нет возможности размещать ссылки.

3. www.myspace.ru – международная социальная сеть, где есть возможность выкладывать фото – и видео-контент. Приоритет использования этого блога: много информации на английском языке.

4. www.ya.ru – массовый портал от компании Яндекс (www.yandex.ru).

Все вышеуказанные блоги помогают выстраивать процесс обучения и коммуникации всех участников процесса.

Закономерную популярность набирает еще один вид обучения в социальной сети – это eLearning (ElectronicEducation, система электронного обучения при помощи информационных технологий). Прогрессивные возможности дистанционного обучения делают процесс более простым и понятным для юного поколения. Российским лидером в сфере eLearning является интернет-портал www.dnevnik.ru. Дистанционное обучение в качестве образовательной цели, направленной на развитие личности, помогает обучающимся реализовывать личные образовательные цели и внимательно

следить за мировыми тенденциями в данной сфере. Открывается возможность совмещать очное образование с дистанционным.

Выбор мессенджеров и социальных сетей в качестве платформы для организации дистанционно-интерактивного обучения имеет ряд аргументов. Принципы построения многих социальных сетей, как идентификация, общение, присутствие на сайте, взаимоотношения, группы, репутация, обмен, поиск, интеграция с другими предложениями очень хорошо подходят для создания учебной группы, класса в он-лайн пространстве, в социальной сети. Размещение образовательного ресурса на базе социальных сетей автоматически устанавливает прямую эффективную коммуникацию между преподавателем и студентом, между студентом и студентом. Сегодня образовательные организации должны использовать различные системы управления образованием. С их помощью образовательные организации будут конкурентоспособными и предоставят студентам интерактивную, мобильную и вовлекающую в обучение и общение среду, соответствующую глобальным трендам на рынке. Все эти тенденции развития социальных сетей создают ситуацию, когда всеохватность аудитории и одновременное использование максимального количества предоставляемых современными интернет-технологиями возможностей переводят образовательную активность на абсолютно другой, значительно более высокий уровень. Социальные сети – это не просто возможность пообщаться, это важный образовательный инструмент школы, колледжа и вуза.

Приведем примеры мессенджеров и социальных сетей:

1.Электронная почта.

2.Мессенджеры: «WhatsApp», Telegram, Zoom.

3.Социальные сети «ВКонтакте».

4.Яндекс.

5.Online Test Pad, Сферум, Учи.ру, Мультиурок, Интернет урок и многие другие.

Социальная сеть Вконтакте является одним из сервисов Интернета нового поколения Веб 2.0, представляя собой систему, позволяющую пользователям отправлять текстовые сообщения (до 700 символов), создавать Сообщества (группы, официальные страницы и встречи), размещать аудиозаписи, видеозаписи, фотографии; пользователь получает право самостоятельно в личных целях создавать, использовать и определять содержание собственной персональной страницы и условия доступа других пользователей к ее содержанию, а также получает возможности доступа и размещения информации на персональных страницах других пользователей. Перечисленные права для пользователей и определяют различные методы, которые могут быть использованы для обучения.

Минпросвещения РФ рекомендовало ограничить применение в рамках образовательного процесса иностранных мессенджеров и обеспечить апробацию информационно-коммуникационной образовательной платформы («Сферум») с использованием российского мессенджера – VK Мессенджер.

«Сферум» — это многофункциональная онлайн-платформа, разработанная в рамках проекта «Цифровая образовательная среда». Систему разработали VK (ранее— Mail.ru) и «Ростелеком». «Сферум» — часть эксперимента по внедрению цифровой образовательной среды (ЦОС). ЦОС — масштабный федеральный проект, входящий в состав национальной программы «Образование». Его суть заключается в создании информационных систем, цифровых сервисов и различных ресурсов для государственной системы образования. К ЦОС должны подключиться школы, колледжи, техникумы, училища и университеты.

В средствах массовой информации она позиционируется, как универсальная платформа для дистанционного образования, которая призвана сделать обучение, в том числе дистанционное, более гибким, технологичным и удобным. «Сферум» предназначена для проведения видеоуроков в онлайн режиме**.** По функциональности она похожа на приложение Zoom и будет доступна как на ПК, так и через мобильное приложение с телефона. Сервис

«Сферум» разрабатывается по заказу Минпросвещения и Минцифры в соответствии с постановлением Правительства РФ.

В учебном профиле Сферум в VK Мессенджере можно создавать чаты, проводить видеоуроки в высоком качестве, а также хранить полезные материалы и делиться ими с учениками. В Сферуме нет рекламы, спама и платных сервисов, а попасть в учебные чаты можно только по приглашению от педагога.

«Сферум» запущена в тестовом режиме в первом квартале 2021 года сразу в 15 регионах России, выбранных в соответствии с порядком отбора субъектов РФ, на территории которых проводится эксперимент по внедрению цифровой образовательной среды (утвержденного Приказом Министерства просвещения РФ от 22 декабря 2020 г. № 761): Астраханской, Калининградской, Калужской, Кемеровской, Московской, Нижегородской, Новгородской, Новосибирской, Омской, Сахалинской, Тюменской, Челябинской областях, Алтайском и Пермском краях, Ямало-Ненецком автономном округе. По состоянию на 31 марта к платформе подключены более 1000 школ и колледжей из указанных регионов, общее число пользователей – свыше 28 тыс. человек. После подключения всех образовательных организаций, находящихся на территории пилотных субъектов РФ, это позволит в том числе протестировать работу платформы в условиях высокой нагрузки. Программа адаптирована для российской аудитории.

«Сферум» фактически представляет собой образовательную социальную сеть: для каждой образовательной организации, использующей платформу, создается сообщество, участниками которого смогут стать педагоги, обучающиеся и их родители, – модерация осуществляется непосредственно выбранным образовательной организацией администратором (или несколькими).

Внутри этого сообщества создаются подгруппы – классы, а в них – отдельные беседы по предметам (групповые чаты для педагогов и обучающихся). Кроме того, платформа позволяет создавать общегрупповые

чаты – с выбором конкретных участников или всех зарегистрированных членов сообщества образовательной организации. В чатах можно обмениваться текстовыми сообщениями, файлами, осуществлять аудио- и видеозвонки. Пользоваться платформой можно через мобильное приложение «Сферума» для iOS и Android и на сайте — с компьютера.

Конечно, в использовании мессенджеров и социальных сетей есть и некоторые негативные стороны. Однако, если использовать эти инструменты грамотно и осмысленно, то можно добиться больших результатов в образовании. Использование мессенджеров и социальных сетей в образовательном процессе способствует обмену информацией, повышает мотивацию обучающихся в учебной деятельности, стимулирует развитие творческих способностей и познавательный интерес, а также может стать новым этапом развития образования, который позволит более эффективно осуществлять обучение и развитие студентов. Все эти факторы положительно влияют на формирование знаний и умений.

Выводы по первой главе

В первой главе «Научно-методические основания для использования социальных сетей и мессенджеров в образовательном процессе» рассматриваются научно-методические основы использования социальных сетей и мессенджеров в образовании, преимущества и недостатки использования этих инструментов, а также определяются основные принципы и подходы к их применению в учебном процессе.

Мессенджеры и социальные сети стали новым явлением в информатизации образования и представляют собой новые дидактические средства. Они позволяют преподавателям и студентам общаться в режиме реального времени, проводить онлайн-конференции, вебинары и другие образовательные мероприятия. Также позволяют создавать групповые чаты, что упрощает коммуникацию в рамках учебных проектов и обсуждение учебных материалов. Кроме того, социальные сети могут быть использованы для публикации новостей, объявлений и другой актуальной информации, для создания электронных портфолио, публикации проектов и презентаций.

Однако, необходимо учитывать ограничения и риски, связанные с их использованием, и обеспечивать правильную организацию и контроль их использования в учебном процессе.

Вопросы обеспечения информационной безопасности в мессенджерах и социальных сетях является важной задачей, которая требует особого внимания и подхода. Для управления защитой персональных и личных данных физического пользователя или целой организации необходимо принятие различных рекомендаций, методов и инструментов по обеспечению информационной безопасности в рамках пользования социальными сетями и мессенджерами. К основным аспектам данной задачи относится конфиденциальность данных, защита от вредоносных программ, контроль доступа, защита от фишинга, обучение пользователей правилам безопасности.

Обеспечение информационной безопасности в мессенджерах и социальных сетях требует комплексного подхода, который включает в себя защиту данных, защиту от вредоносных программ, контроль доступа, защиту от фишинга и обучение пользователей правилам безопасности.

Педагогическая практика по применению мессенджеров и социальных сетей в образовательном процессе представляет собой важную часть обучения студентов, направленную на развитие их практических навыков и расширение знаний в области использования современных технологий в обучении. Она требует организации и контроля со стороны преподавателя, учета индивидуальных потребностей и возможностей студентов, а также оценки результатов.

ГЛАВА 2 РАЗРАБОТКА И АПРОБАЦИЯ РЕКОМЕНДАЦИЙ ПО ИСПОЛЬЗОВАНИЮ СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

2.1. Текущее обеспечение информационной безопаности при использовании социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж»: актуальные уязвимости и риски

Базой исследования является Государственное бюджетное профессиональное образовательное учреждение «Челябинский профессиональный колледж», располагающийся по адресу: Челябинск, ул. Сулимова, 67.

Директор ГБПОУ «Челябинский профессиональный колледж»: Василяускене Елена Геннадьевна.

Адрес официального сайта в сети «Интернет»: https://челпк.рф.

В настоящее время колледж – это многоуровневое, многопрофильное образовательное учреждение города Челябинска, реализующее программы подготовки квалифицированных рабочих, служащих и программы подготовки специалистов среднего звена. Колледж готовит специалистов для сферы дошкольного образования, железнодорожного транспорта, строительства, общественного питания и др. За время своего существования колледж подготовил более 15 тысяч специалистов.

Образовательная деятельность в колледже ведется в соответствии с нормативно-правовыми актами системы образования, федеральными государственными образовательными стандартами СПО и СОО, локальными нормативно-правовыми актами образовательной организации, а также целями и задачами, обозначенными в Программе развития ГБПОУ «Челябинский профессиональный колледж» и перспективными планами работы. Стратегическая цель деятельности колледжа – обеспечение доступности и качества профессионального образования, отвечающего требованиям

инновационного развития Челябинской области, создание условий для реализации механизмов повышения эффективности профессионального образования в обеспечении социально-экономической сферы Челябинской области в высококвалифицированных рабочих специалистах для промышленности, сферы услуг, предприятий малого и среднего бизнеса региона.

Организация учебного процесса регламентируется учебными планами, календарными учебными графиками и расписанием учебных занятий. Расписание учебных занятий составляется в соответствии с календарными графиками и ежегодно утверждается директором. Расписание учебных занятий размещается на информационных стендах Колледжа, АСУ ProCollege.

Организационная структура управления ГБПОУ «Челябинский профессиональный колледж» представлена на рисунке 1.

В образовательную деятельность колледжа внедрена – автоматизированная система управления ProCollege. Более 150 наименований учебных пособий, тестов, задачников и т.д., разработаны преподавателями колледжа. Ведется работа по наполнению учебного портала образовательным контентом.

Доступ к информационным системам.

Все рабочие места объединены в единую компьютерную сеть по корпусам. Сегменты сети построены с использованием технологий FastEthernet и GigabitEthernet, со скоростью передачи 100 Мбит/сек. Центральный сервер сети колледжа совмещает функции файл-сервера. Со всех рабочих мест имеется выход в Internet. Подключение к Internet организовано по выделенной оптоволоконной линии. Скорость подключения – 15 Мбит/сек. Соединение имеет защищенный характер, используется сетевой экран. 100% студентов имеют доступ к сети Интернет во время обучения. Межсетевые экраны имеют сертификаты ФСТЭК. Доступ к ресурсам для обучающихся ограничивается в соответствии с ФЗ №№436, 139, ведётся фильтрация трафика

в соответствии со списками Роскомнадзора и Минюста, предоставляется провайдером ООО Дом.ru.

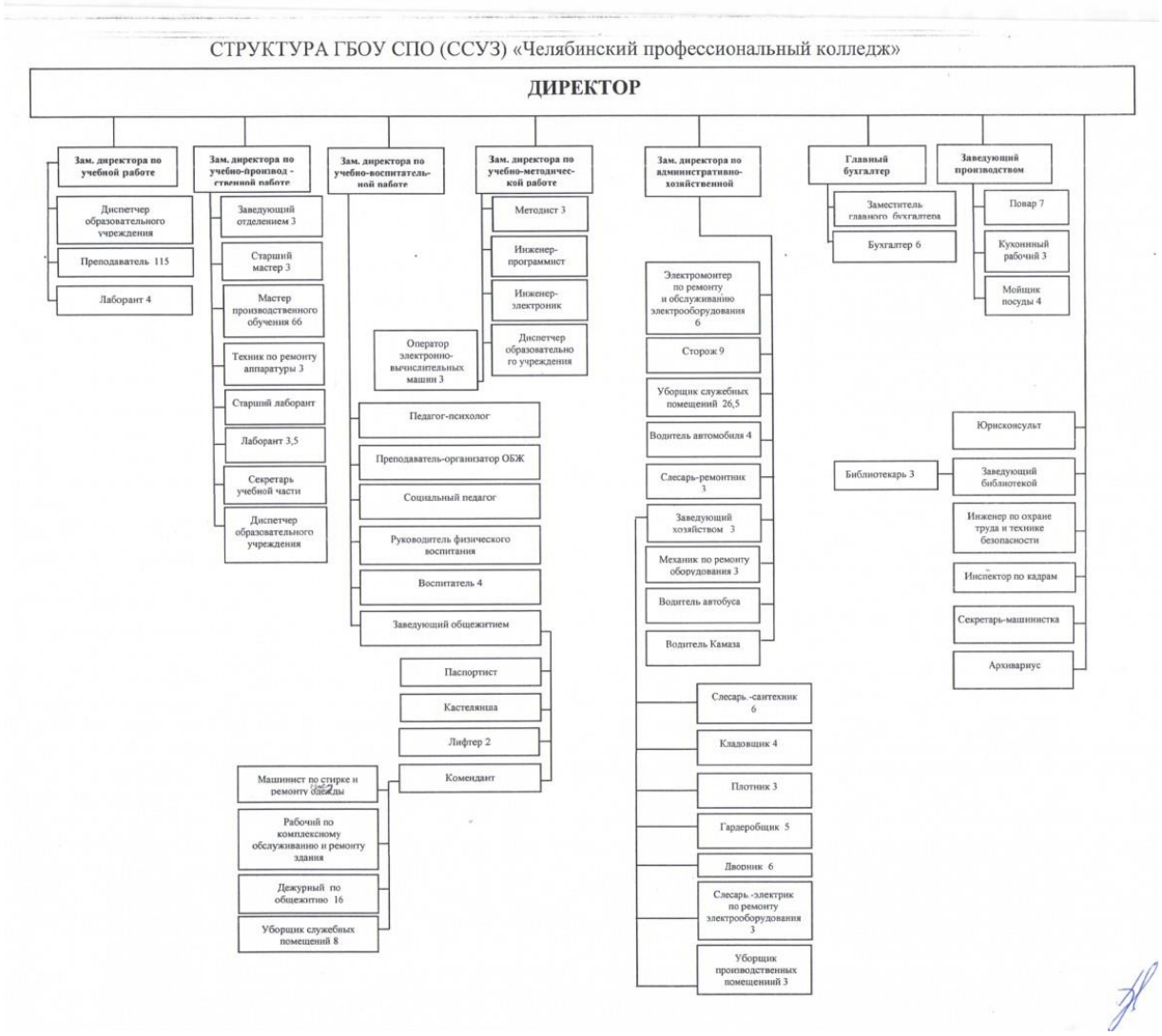

Рисунок 1 – Организационная структура управления ГБПОУ «Челябинский профессиональный колледж»

Организацией системы защиты данных в ГБПОУ «Челябинский профессиональный колледж»» занимается отдел информационной безопасности.

В структуру отдела входят:

1. Заместитель директора по информационной безопасности.
2. Инженер-программист 1 человек (ведение сайта, Администрирование Сферум, ProCollege, АИС «Сетевой город», обслуживание оргтехники и локальной сети.

3. Инженер- электроник 1 человек (обслуживание локальных сетей, обслуживание оргтехники, обслуживание систем видеонаблюдения, Сферум, АИС «Сетевой город»).

4. Операторы ЭВМ - 4 человека (приёмная комиссия, АИС «Сетевой город», ГИС Образование, Сферум, ProCollege, ФИС ФРДО).

Функции отдела:

1. Обеспечение подразделений колледжа доступом к ресурсам сети Интернет.

2. Поддержание в рабочем состоянии и совершенствование компьютерную сети колледжа. Обеспечение сотрудников колледжа услугами электронной почты. Обеспечение комплексной защиты сети от компьютерных вирусов разных видов.

3. Развитие информационных технологий в рамках административно-управленческой деятельности.

4. Обеспечение бесперебойной работы компьютеров, компьютерной сети колледжа, компьютерного периферийного оборудования и пользователей.

5. Внедрение проектов системы автоматизированного управления колледжа.

6. Выявление и оперативное устранение перебоев в работе оборудования и пользователей.

7. Анализ и изучение проблем автоматизированных систем управления колледжа и ее подразделений.

8. Участие в составлении технических заданий по внедрению автоматизированной системы управления колледжа.

9. Подготовка планов внедрения автоматизированных систем управления колледжем и контроль за их выполнением.

10. Определение задач, их алгоритмизация, увязка организационного и технического обеспечения автоматизированной системы управления колледжа.

11. Контроль состояния и безопасности сети и сетевого оборудования.

12. Назначение пользователям сети прав доступа.

13. Установка, настройка и управление программными и аппаратными системами колледжа.

14. Анализ и учет случаев отказа системы.

15. Разработка и проведение мероприятий по повышению качества и надежности автоматизированных систем управления колледжа.

16. Модернизация применяемых технических средств.

17. Составление заявок на необходимое оборудование, ведение учета его поступлений и использования средств, выделенных на эти цели. Подготовка документации на проведение конкурсов и аукционов при закупке компьютерной и оргтехники для нужд колледжа.

18. Обеспечивать своевременное и регулярное техническое обслуживание компьютерной техники и оргтехники подразделений колледжа.

19. Консультации пользователей информационно-вычислительной системы колледжа по вопросам использования компонентов системного программного обеспечения.

20. Техническая поддержка учебных компьютерных классов.

Ответственным за обеспечение безопасности персональных данных является заместитель директора по информационной безопасности.

Таким образом, отдел информационной безопасности выполняет возложенные на него функции в тесном сотрудничестве и взаимодействии со всеми структурными подразделениями колледжа и другими образовательными организациями: центрами дистанционного образования, центрами Интернет- тестирования, учебно-научными центрами по проблемам информационной безопасности в системе среднего профессионального образования.

Политика информационной безопасности колледжа (ГБПОУ «Челябинский профессиональный колледж») представляет собой совокупность мер организационного и программно-технического уровня,

направленных на защиту информационных ресурсов колледжа от угроз информационной безопасности. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных документированной политикой информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты информации.

Объектом защиты являются автоматизированные системы (как собственной, так и сторонней разработки), входящие в состав информационной системы колледжа.

Доступ педагогических работников и обучающихся к вышеперечисленным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной Уставом колледжа.

Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности.

Педагогические работники бесплатно пользуются образовательными, методическими и научными услугами колледжа. Пользование образовательными, методическими и научными услугами колледжа осуществляется через сайт и локальную сеть колледжа, а также методические кабинеты, учебную часть.

Доступ к информационно-телекоммуникационным сетям.

Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в колледже осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет.

Для доступа к информационно-телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные

данные (логин и пароль /учётная запись). Предоставление доступа осуществляется системным администратором колледжа.

Доступ к базам данных. Педагогическим работникам обеспечивается доступ к следующим электронным базам данных:

- профессиональные базы данных;
- информационные справочные системы;
- поисковые системы.

Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных колледжем с правообладателем электронных ресурсов (внешние базы данных).

Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте колледжа.

В колледже введены в эксплуатацию следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Обучающиеся и абитуриенты» ГБПОУ «ЧелПК» (далее - ИСПДн «Обучающиеся и абитуриенты»).
2. ИСПДн «Сотрудники» ГБПОУ «ЧелПК» (далее - ИСПДн «Сотрудники»).
3. ИСПДн «Библиотека» ГБПОУ «ЧелПК» (далее - ИСПДн «Библиотека»).
4. АСУ «ProCollege».
5. Региональная АИС «Сетевой город. Образования».
6. Информационно-коммуникационная образовательная платформа Сферум» (VK Мессенджер).
7. Социальные сети и мессенджеры: электронная почта, WhatsApp, Telegram, «ВКонтакте», Яндекс.

Для защиты информации в ИСПДн Колледжа используются следующие СКЗИ:

- «ViPNet Client 4», сертификат соответствия ФСБ России;
- «КриптоПро CSP 4.0», сертификат соответствия ФСБ России.

К объектам защиты относятся:

− ПДн;

− СКЗИ;

− среда функционирования СКЗИ (далее по тексту – СФ);

− информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

− носители защищаемой информации, используемые в ИС Сотрудники, ИС Обучающиеся и ИС Библиотека в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

− используемые в ИС каналы (линии) связи, включая кабельные системы;

− помещения, в которых находятся ресурсы ИС Сотрудники, ИС Обучающиеся и ИС Библиотека, имеющие отношение к криптографической защите ПДн.

Работа с понятием угрозы начинается с классификации нарушения.

Насколько актуальна проблема защиты информации от различных угроз, можно увидеть на примере данных, опубликованных Computer Security Institute (Сан - Франциско, штат Калифорния, США), согласно которым нарушение защиты компьютерных систем происходит по следующим причинам [15]:

– несанкционированный доступ - 2%;

– укоренения вирусов - 3%;

– технические отказы аппаратуры сети - 20 %;

– целенаправленные действия персонала - 20 %;

– ошибки персонала (недостаточный уровень квалификации) - 55 %.

Таким образом, одной из потенциальных угроз информации в информационных системах следует считать целенаправленные или случайные

деструктивные действия персонала (человеческий фактор), так как они составляют 75 % всех случаев [29, С. 7].

Рассматривая исходные ИСПДн на исходный уровень защищенности, берется в расчет технические и эксплуатационные характеристики.

Рассматриваемая ИСПДн имеет средний (Y1=5 - согласно Методике) уровень исходной защищенности, т.к. не менее 70% характеристик ИСПДн соответствуют уровню защищенности не ниже «средний».

Вероятность реализации угрозы безопасности персональных данных.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

1) маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2= 0);

2) низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

3) средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (У2 = 5);

4) высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (У2 = 10).

Показатель исходной защищенности ИСПДн.

Технические и эксплуатационные характеристики ИСПДн «Сотрудники»:

1. По территориальному размещению – локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий. Уровень защищенности – средний.

2. По наличию соединения с сетями связи общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования. Уровень защищенности – низкий.

3. По встроенным (легальным) операциям с записями баз персональных данных – модификация, передача. Уровень защищенности – низкий.

4. По разграничению доступа к персональным данным – ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн. Уровень защищенности – средний.

5. По наличию соединений с другими базами ПДн иных ИСПДн – ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн. Уровень защищенности – высокий.

6. По уровню обобщения (обезличивания) ПДн – ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн). Уровень защищенности – низкий.

7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки – ИСПДн, предоставляющая часть ПДн. Уровень защищенности – средний.

В таблице 1 представлен перечень автоматизированных информационных систем и ИСПДн колледжа.

Таблица 1 − Перечень ИСПДН и АИС, обрабатывающих КИ, КТ и ПДн в колледже

№ п/п	**Наименование информационной системы**	**Описание информационной системы**	**Перечень содержания информационной системы**
1	АСУ «ProCollege»	Программный продукт представляет собой комплексное решение для управления деятельностью учреждений начального и среднего профессионального образования и охватывает все уровни управленческой деятельности основных подразделений колледжа.	- Паспортные данные студента - Паспортные данные родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата студента - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, контактный телефон, стаж работы сотрудников образовательной организации - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов
2	Региональная АИС «Сетевой город. Образования»	Автоматизированная информационная система «Сетевой Город. Образование», модуль «Профессиональная образовательная организация Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса.	- Паспортные данные студента - Паспортные данные родителей студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, телефон, стаж работы сотрудников ОО - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов

Продолжение таблицы 1

3	ИСПДн «Обучающие и абитуриенты»	Системы предоставление социальных услуг	- Паспортные данные студента - Паспортные данные родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Контактный телефон - Электронная почта - Паспортные данные, СНИЛС, ИНН, контактный телефон сотрудников образовательной организации

Политика конфиденциальности Программного обеспечения «Информационно-коммуникационная образовательная платформа Сферум» (далее — Политика) является официальным документом Общества с ограниченной ответственностью «Компания ВК» (ОГРН: 1097746572813, адрес места нахождения: 125167, г. Москва. Ленинградский проспект, д.39, стр.79, далее — Компания), и определяет порядок обработки и защиты информации о физических лицах, пользующихся услугами Программного обеспечения «Информационно-коммуникационная образовательная платформа Сферум» (далее – Система) в информационно-телекоммуникационной сети «Интернет», с использованием которой осуществляется сбор (обработка) персональных данных (далее Пользователи).

В таблице 2 представлены показатели исходной защищенности ИСПДн и АИС в колледже.

Таблица 2 − Показатели исходной защищенности ИСПДн и АИС

Технические и эксплуатационные характеристики	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределенная, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная, охватывающая многие подразделения одной организации;	–	+	–

Продолжение таблицы 2

локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн*:*			
интегрированная ИСПДн (организация использует несколько баз ПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

В соответствии полученными данными устанавливается низкий показатель исходной защищенности. Устанавливается значение коэффициента Y_1=10.

Реализуемость угроз. По итогам оценки уровня защищенности и вероятности реализации угрозы, рассчитывается коэффициент реализуемости угрозы и определяется возможность реализации угрозы:

Y = (Y1 + Y2)/20,

где Y – коэффициент реализуемости угроз; Y1 – уровень защищённости; Y2 – вероятность реализации угроз [16].

Для большинства параметров, этот показатель не превышает значения в 0.35, что является хорошим исходным показателем.

Для ИСПДн «Сотрудники» актуальны угрозы 3 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн «Сотрудники».

Руководствуясь [3], учитывая исходные данные об ИСПДн «Сотрудники» и тип актуальных для неё угроз, необходимо обеспечить 4-ый уровень защищённости ПДн при их обработке в ИСПДн «Сотрудники».

В соответствии с [10], и определённым в модели нарушителя типом нарушителя – Н2, в ИСПДн «Сотрудники» для криптографической защиты ПДн должны применяться СКЗИ класса не ниже КС2.

Для ИСПДн «Обучающиеся и абитуриенты» актуальны угрозы 3 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн «Обучающиеся и абитуриенты».

Руководствуясь [3], учитывая исходные данные об ИСПДн «Обучающиеся и абитуриенты» и тип актуальных для неё угроз, необходимо обеспечить 4-ый уровень защищённости ПДн при их обработке в ИСПДн «Обучающиеся и абитуриенты».

В соответствии с [10], и определённым в модели нарушителя типом нарушителя – Н2, в ИСПДн «Обучающиеся и абитуриенты» для криптографической защиты ПДн должны применяться СКЗИ класса не ниже КС2.

Для ИСПДн «Библиотека» актуальны угрозы 3 типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном прикладном программном обеспечении, используемом в информационной системе.

Руководствуясь [3], учитывая исходные данные об ИСПДн «Библиотека» и тип актуальных для неё угроз, необходимо обеспечить 4-ый уровень защищённости ПДн при их обработке в ИСПДн «Библиотека».

Разработка документа «Актуальная модель угроз ИСПДн».

На основе полученных коэффициентов реализации угрозы и параметрах опасности угроз, делается вывод о актуальности данной угрозы.

Система защиты персональных данных при их обработке в информационных системах персональных данных в ГБПОУ «Челябинский профессиональный колледж» создана.

Эксплуатация используемых криптосредств, обращение с СКЗИ осуществляется с нарушениями требований нормативных документов в области защиты информации.

2.2. Разработка рекомендаций по использованию социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж»

Несмотря на все предпринимаемыми мессенджерами и социальными сетями усилия, направленные на предотвращение утечки персональных данных, защита информации в социальных сетях и мессенджерах становится все более актуальной с каждым годом.

На основе анализа рисков и уязвимостей системы защиты персональных данных и анализа нормативно-правовых требований действующего

законодательства нами были разработаны рекомендации по использованию социальных сетей и мессенджеров в образовательном процессе, что повысить эффективность противодействия вредоносной информации в социальных сетях и мессенджерах в ГБПОУ «Челябинский профессиональный колледж».

Для устранения недостатков в существующей системе защиты ПДн, необходимо предложить образовательной организации усовершенствовать организационные, технические и физические меры.

Основными задачами рекомендаций являются:

– улучшение организационного и технического уровня защиты информации;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению противодействия вредоносной информации в социальных сетях и мессенджерах;

– организация периодической проверки соблюдения информационной безопасности сотрудниками.

Объект защиты.

Объектом защиты являются персональные данные работников и обучающихся образовательной организации среднего профессионального образования:

1. Информационные ресурсы:

− персональные данные работников и обучающихся (исходная информация, информационные базы данных);

− инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн.

2. Технические информационные системы и средства Организации, в которых обрабатывается, хранится и передается информация ПДн.

3. Помещения объектов Организации, в которых размещаются информационные ресурсы, и обрабатываются ПДн.

4. Технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

Субъекты информационных отношений:

1. Субъектами информационных отношений являются:

− обучающиеся (субъекты персональных данных) - физические лица, родители (законные представители) которых состоят в договорных и иных гражданско-правовых отношениях с Организацией-оператором по вопросам оказания услуг в сфере образования, предусмотренных Уставом;

− сотрудники (субъекты персональных данных) - физические лица, состоящие или готовящиеся вступить в трудовые или иные гражданскоправовых отношениях с Организацией-оператором.

Проанализировав популярные на сегодняшний день технологии защиты информации в социальных сетях и мессенджерах, анализ рисков и уязвимостей системы защиты персональных данных, мы разработали рекомендации по использованию социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж» при соблюдении информационной безопасности.

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе это системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности [1].

Защита информации – совокупность методов и средств, направленных на обеспечение информационной безопасности. Наиболее распространенные угрозы:

1. Ошибки пользователей.

2. Кражи и подлоги.

3. Угрозы из внешней среды (поломки и аварии, отсутствие связи и т.д.).

4. Хакеры.

5. Программные вирусы [2].

Защита личной информации в мессенджерах и социальных сетях обеспечивается с помощью:

– предотвращения несанкционированного доступа к информации;

– выявления случаев несанкционированного доступа, определения причин произошедшей утечки данных и их устранения;

– предоставления владельцам аккаунтов возможности восстановить информацию, уничтоженную или измененную вследствие несанкционированного к ней доступа.

Для предотвращения ошибок и взломов системы предпринимаются меры программно-технической безопасности, указанные в таблице 3.

Таблица 3 – Описание мер программно-технической безопасности

Меры программно-технической безопасности	Описание
Идентификация и аутентификация	С помощью идентификации пользователь сообщает свое имя. С помощью аутентификации пользователя проверяют на подлинность.
Управление доступом	Пользователю определяется множество допустимых операций.
Протоколирование и аудит	Протоколирование – сбор и накопление информации о событиях, происходящих в системе. Аудит – анализ накопленной информации
Экранирование	Контроль и фильтрация всех информационных потоков между двумя множествами систем
Криптография	Шифрование и дешифрование информации с помощью соответствующего алгоритма.

Продвинутые социальные сети ввели двухфакторную аутентификацию. Она состоит из двух этапов: первый – вход с помощью логина и пароля, второй – уникальный код по смс или уникальный список кодов, которые действуют лишь единожды, или специальный код, который можно сканировать с помощью мобильного телефона.

Для обеспечения защиты личных данных используются программные и криптографические средства.

Программные средства:

– DLP-системы - комплексные системы, предотвращающие утечку данных;

– SIEM-системы - комплексные системы управления событиями и информационной безопасностью, отслеживающие в режиме реального времени событий безопасности (тревог) (MaxPatrol SIEM от Positive Technologies, КОМРАД от «НПО «Эшелон», RUSIEM).

DLP (Data Loss Prevention) — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

Предотвращение потери данных является фундаментальным принципом безопасности в компании любого масштаба.

DLP-система включает в себя набор методов и инструментов для борьбы с утечками данных, исходящими от лиц, которые могут разглашать важную для бизнеса информацию по небрежности или злому умыслу с использованием своих или украденных учетных данных.

Программное обеспечение и инструменты защиты от потери данных осуществляют мониторинг и контроль действий пользователей на конечных точках; при помощи специальных алгоритмов фильтруют потоки информации и коммуникации в корпоративных сетях, контролируют перемещение данных. В случае выявления несанкционированной передачи данных DLP-система блокирует операцию либо оповещает об этом офицера информационной безопасности, а также может использовать определенные защитные действия (например, блокирование и изменение сообщений).

Решения класса Data Leak Prevention (DLP) можно сравнить с «водопроводной системой» для потоков конфиденциальных данных. Они обнаруживают и предотвращают несанкционированное использование (Data-in-use), передачу (Data-in-motion) и хранение (Data-at-rest) конфиденциальных данных (рис. 2).

Data-in-use – это данные, к которым пользователи активно обращаются, обрабатывают и обновляют их. DLP предотвращает утечку данных благодаря функции мониторинга действий на рабочих станциях (например, съемные USB-носители, буфер обмена, приложения) и анализа поведения пользователей.

Data-in-motion – это информация, которая перемещается из одной точки в другую. DLP предотвращает утечку данных через сетевые коммуникации (например, электронная почта, инструменты совместной работы, программы мгновенного обмена сообщениями и практически любой публичный канал связи). При этом типе мониторинга делается акцент на идентификации данных, их источнике и назначении, и последующем контроле потока информации в соответствии с политикой безопасности.

Data-at-rest – это данные, которые не перемещаются между устройствами или сетями. DLP обнаруживает конфиденциальный контент в данных, хранящихся на корпоративных ИТ-ресурсах (например, сетевые файловые ресурсы, файловые системы конечных устройств, базы данных, хранилища документов и облачные хранилища), и устраняет нарушения политики хранения данных.

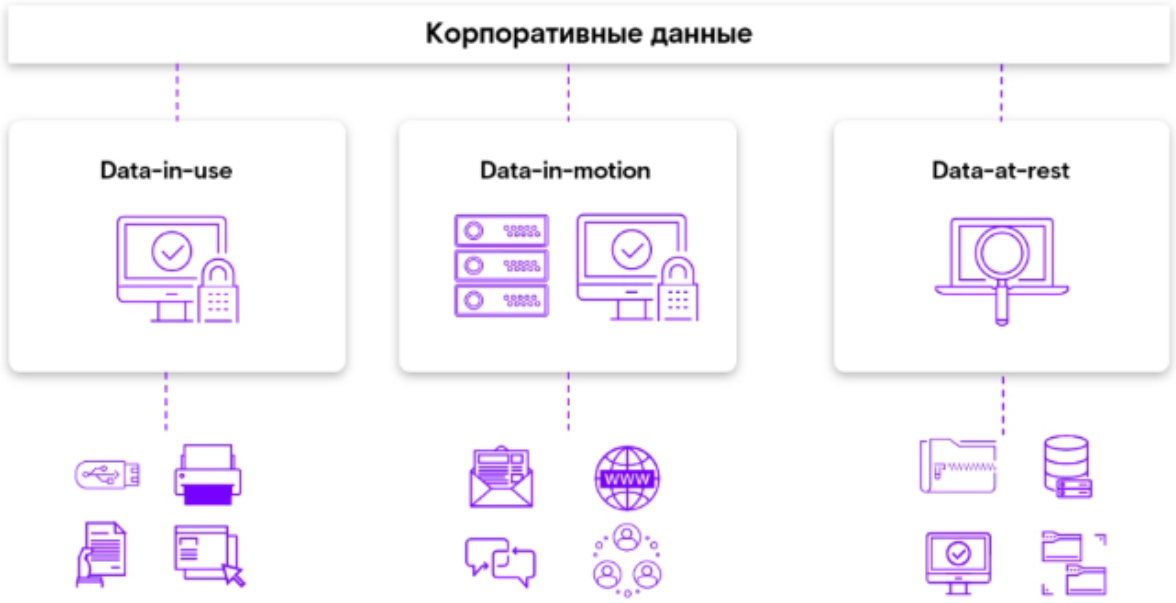

Рисунок 2 − Виды корпоративных данных

После того как данные перехвачены, они отправляются на полнотекстовый поиск, контентный (анализ содержимого) и контекстный (основанный на контексте операции – например, отправитель, получатель, используемый канал) анализ для обеспечения соблюдения политик использования и обработки данных, принятых в организации. При обнаружении подозрительного действия система принимает решение о блокировке или оповещении сотрудников службы безопасности о нарушении политики безопасности. Полученные сведения могут быть использованы для проведения расследований со стороны служб информационной, внутренней и экономической безопасности.

Технологии, которые могут быть использованы для обеспечения оперативного перехвата конфиденциальной информации, профилактики инцидентов безопасности и контроля конфиденциальных данных:

Контроль идентификаторов (IDID, ID identification) – технология позволяет распознавать в тексте сообщений специальные идентификаторы в виде последовательности цифр или букв, однозначно определяющей данные, интересные с точки зрения информационной безопасности, в частности контроля утечек информации и работы с персональными данными, и осуществляет:

1. Выявление финансовых данных: банковских реквизитов, ИНН налогоплательщика, номеров пластиковых карт и т. д.

2. Выявление персональных данных: паспортных данных, СНИЛС.

3. Выявление документов, создаваемых по шаблону: договоров, регламентов и т. д.

4. Выявление слов и фраз определенной тематики.

Цифровые отпечатки (DiFi, digital fingerprints) – технология позволяет сравнивать текстовые, графические и табличные данные с эталонными документами, что дает возможность находить как полностью, так и частично скопированные документы, и выявляет:

1. Текстовые документы (планы, уставы, приказы, типовые договоры, тендерные документы и т. д.).

2. Табличные данные (базы клиентов, персональные данные и т. д.).

3. Графические документы (сканы, фотографии, чертежи и т. д.).

4. Шаблонные элементы ГОСТ и документов внутреннего стандарта.

5. Печать-гриф («конфиденциально», «копия», «ДСП», и т. д.).

Графические шаблоны – технология позволяет распознавать конфиденциальные сведения в графических форматах с учетом их деформации (растяжение, поворот, наложение на другие объекты), а также при полном отсутствии текста и выявляет:

- печати организации;
- изображения паспортов с персональными данными;
- платежные карты.

Поведенческий анализ – передовая технология, основанная на машинном обучении, благодаря чему стало возможно получать сведения о зарождающихся угрозах через анализ собранной информации о поведенческой динамике пользователей, их связях и выявленных аномалиях. Детальный анализ показателей поведения может выявить негативные тенденции, что позволяет офицеру безопасности работать с рисками утечек конфиденциальных данных превентивно, вовремя принимая соответствующие меры.

Файловый краулер – технология, благодаря которой становится возможно проводить проверку узлов корпоративной сети и составлять ее наглядную карту, после чего контролировать ресурсы сети. Это позволяет находить конфиденциальную информацию в корпоративных и облачных хранилищах, электронной почте и других ресурсах.

Задачи информационной безопасности, которые решает DLP-система, включают защиту конфиденциальных данных организации от утечек, контроль использования, передачи и хранения информации. Кроме того, DLP-система позволяет проводить расследования инцидентов, связанных с

утечками конфиденциальной информации, путем мониторинга и анализа активности пользователей. Система позволяет определить какие действия выполнялись с данными. Это помогает выявить причины нарушения и принять меры по предотвращению подобных инцидентов в будущем.

DLP-система также способствует обеспечению экономической безопасности, предотвращая финансовое мошенничество, утечки коммерческой и бухгалтерской информации. DLP-система может использоваться для мониторинга коммуникаций и обнаружения любых подозрительных действий, таких как попытки передачи конфиденциальной информации третьим лицам или изменение условий сделок без соответствующего разрешения.

В борьбе с коррупцией DLP-система помогает обнаруживать и предотвращать несанкционированные действия с конфиденциальными данными, связанные с получением взяток, конфликтом интересов, вымогательством, неправомерным использованием ресурсов организации и другими видами коррупции.

Внутренний контроль также является важной задачей DLP-системы. Она позволяет контролировать исполнение управленческих решений, определять сокрытие нарушений и факты саботажа, а также проводить анализ реакций на различные распоряжения.

Наконец, DLP-система способствует обеспечению внутренней безопасности организации, выявляя компрометирующие связи, признаки шпионажа и разведки, предотвращая мошенничество и нарушения законодательства.

Криптографические методы защиты.

Пересылаемую информацию между пользователями в социальных сетях зачастую шифруют программой PGP. Он шифрует сообщения с помощью открытого (публичного, public) ключа и расшифровывает их с помощью закрытого (секретного, private) ключа (рис. 3).

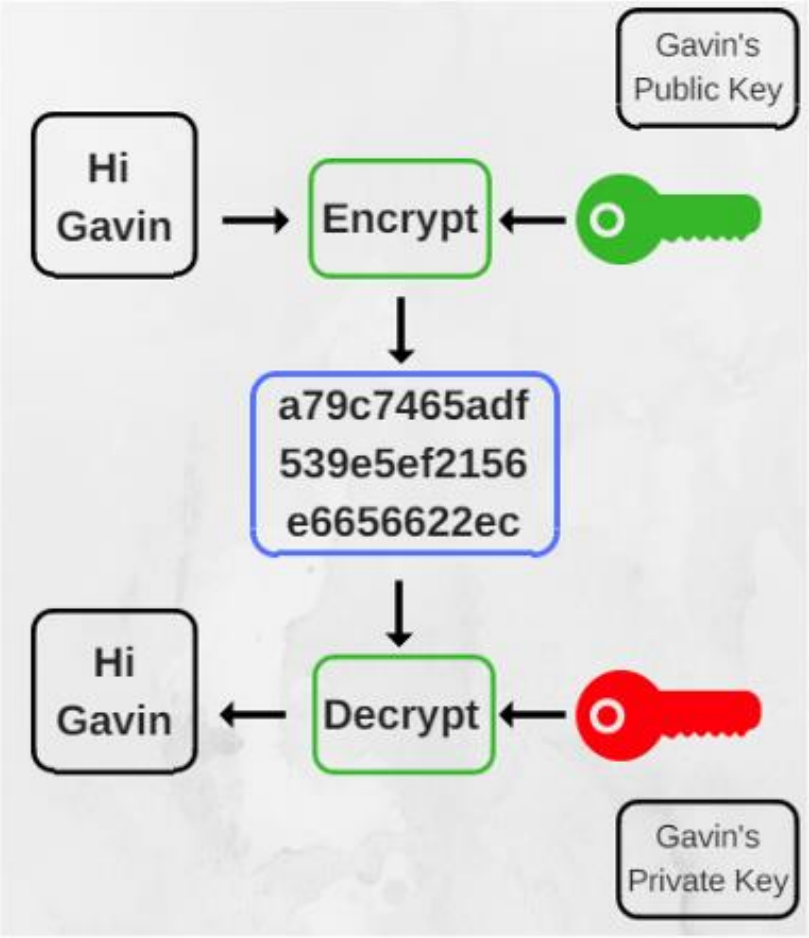

Рисунок 3 – Схема использования, открытого и закрытого ключей [3]

Шифрование PGP включает в себя такие этапы:

1. Хеширование.
2. Сжатие данных.
3. Шифрование с симметричным ключом.
4. Шифрование с открытым ключом.

Сеансовый ключ получается с помощью криптографически стойкого генератора псевдослучайных чисел, затем он шифруется открытым ключом получателя. Открытые ключи соответствуют адресу электронной почты или имени пользователя. При генерации ключей задаются их владелец, тип ключа, длина ключа и срок его действия.

PGP также позволяет использовать цифровые подписи. Подписанное закрытым ключом зашифрованное сообщение получатель может проверить открытым ключом. Если сообщение до расшифровки было изменено, то

подпись будет признана недействительной. В таблице 4 показаны преимущества и недостатки технологии PGP.

Таблица 4 – Преимущества и недостатки технологии PGP

Преимущества	Недостатки
Безопасная асимметричная криптография	Большая длина открытых ключей
Скорость симметричного шифрования	Сложность для освоения пользователем
Цифровые подписи, обеспечивающие целостность данных и подлинность отправителя	Отсутствие прямой секретности

Протокол Signal – криптографический протокол, обеспечивающий сквозное шифрование голосовых вызовов, видеозвонков и мгновенных сообщений [4]. Этот протокол реализовывали такие популярные мессенджеры, как WhatsApp, Viber. Signal позволяет создавать сквозные зашифрованные групповые чаты, обеспечивает конфиденциальность, целостность, аутентификацию, прямую секретность, проверку назначения, согласованность участников, отказ от сообщений, отказ от участия, асинхронность. Он не обеспечивает сохранение анонимности и требует наличие серверов для ретрансляции сообщений и хранения информации об открытом ключе [5].

Рекомендации для дополнительной безопасности.

Пользователи самостоятельно оставляют много персональных данных в социальных сетях. Это объясняется самой сутью социальных сетей – обмениваться информацией с другими пользователями. Эта информация в руках злоумышленников может повлечь негативные последствия. Для безопасного пользования социальными сетями существуют специальные правила, которые представлены в таблице 5.

Таблица 5 – Способы защиты своей информации в социальных сетях

Угроза	Способ защиты
Взлом пароля средством программ с словарями с паролями	Пароль должен содержать цифры, буквы разного регистра и специальные знаки, быть длиннее 8 символов
Кража cookies, подмена cookies	Не пользоваться незащищенными сетями
Фишинг	Отправлять письма от неизвестных пользователей в спам. Сравнивать ссылки

	на сайты в письме с ссылками на официальные сайты.
Фарминг	Став жертвой атаки, очистить DNS-кэш, запустить антивирусную программу, связаться с интернет-провайдером

Дополнительные меры:

– не используйте для регистрации на общедоступных ресурсах почту, которая связана с важными процессами (например, рабочими и финансовыми сервисами);

– устанавливайте свой пароль для каждого ресурса, избегайте классических комбинаций типа «12345»;

– для восстановления или подтверждения пароля используйте мобильный телефон, а не электронную почту;

– делитесь личной информацией в соцсетях осторожно - продумывайте, какие последствия может повлечь за собой размещение тех или иных сведений в общем доступе;

– не добавляйте в друзья незнакомых людей и не переходите по всем ссылкам подряд;

– не публикуйте в соцсетях фотографии важных документов, не пересылайте такие документы через личные сообщения;

– не скачивайте предлагаемые вам через соцсети приложения, если не уверены в том, что это официальный продукт известной вам компании.

В случае с защитой информации образовательной организации, необходимо принятие следующих рекомендаций и направлений по обеспечению информационной безопасности в социальных сетях и мессенджерах [5]:

– с целью технического обеспечения информационной безопасности необходимо использование комплексных средств мониторинга, анализа и фильтрации входящего и исходящего трафика на уровне шлюзов, а также средств анализа поведения приложений и сетевых коммуникаций;

− в рамках управления доступом к социальным сетям необходимо использование диверсифицированной внутрикорпоративной политики «белых списков» и фильтрации контента для различных групп пользователей;

− необходимо проводить адекватную разъяснительную и просветительскую работу среди сотрудников и обучающихся образовательной организации.

2.3. Расчет экономической эффективности рекомендаций по обеспечению информационной безопаности при использовании социальных сетей и мессенджеров на базе ГБПОУ «Челябинский профессиональный колледж»

Исходной посылкой экономической эффективности является очевидное предположение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, с другой - обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и потерь от ее нарушения.

Очевидно, что оптимальным решением было бы выделение на защиту информации средств, минимизирующих общую стоимость работ по защите информации.

Также очевидно, что экономическая эффективность мероприятий по защите информации может быть определена, через объем предотвращенного ущерба или величину снижения риска для информационных активов образовательной организации.

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. В качестве одной из методик определения уровня затрат возможно использование следующей эмпирической зависимости ожидаемых потерь (рисков) от i-й угрозы информации [37]:

$$Ri = 10^{Si+Vi-4} \quad (1)$$

где S_i - коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;

V_i - коэффициент, характеризующий значение возможного ущерба при ее возникновении.

S_i и V_i приведены в таблице 6.

Таблица 6 – Значения коэффициентов S_i и V_i

Ожидаемая (возможная)частота появления угрозы	**Предполагаемое значение S_i**
Почти никогда	0
1 раз в 1 000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7
Значение возможного ущерба при проявлении угрозы, руб	**Предполагаемое значение V_i**
30	0
300	1
3 000	2
30 000	3

Продолжение таблицы 6

300 000	4
3 000 000	5
30 000 000	6
300 000 000	7

Суммарная стоимость потерь определяется формулой:

$$R = \sum_{i=1}^{N} Ri \quad (2)$$

где N – количество угроз информационным активам, определенных в п.2.1.

При расчете суммарного показателя рекомендуется принять, что угрозы конфиденциальности, целостности и доступности реализуются нарушителем независимо. То есть, если в результате действий нарушителя была нарушена целостность информации, предполагается, что её содержание по-прежнему

остается ему неизвестным (конфиденциальность не нарушена), а авторизованные пользователи по-прежнему имеют доступ к активам, пусть и искаженным (см. таблицу 7).

Таблица 7 − Величины потерь (рисков) для критичных информационных ресурсов до внедрения/модернизации защиты информации

Актив	Угроза	Величина потерь (тыс.руб.)
Документация образовательной организации	конфиденциальности	100
Документация образовательной организации	целостности	50
Документация образовательной организации	доступности	20
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	конфиденциальности	500
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	целостности	100
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	доступности	20
Личные данные обучающихся	конфиденциальности	300
Личные данные обучающихся	целостности	20
Личные данные обучающихся	доступности	20
Личные сведения о сотрудниках	конфиденциальности	100

Продолжение таблицы 7

Личные сведения о сотрудниках	целостности	10
Личные сведения о сотрудниках	доступности	10
Системное программное обеспечение	конфиденциальности	0
Системное программное обеспечение	целостности	100
Системное программное обеспечение	доступности	100
Прикладное программное обеспечение (в т.ч. АСУ «ProCollege», Региональная АИС «Сетевой город. Образования», Сферум, СКЗИ)	конфиденциальности	0
Прикладное программное обеспечение (в т.ч. АСУ «ProCollege», Региональная АИС «Сетевой город. Образования», Сферум, СКЗИ)	целостности	100
Прикладное программное обеспечение (в т.ч. АСУ «ProCollege», Региональная АИС «Сетевой город. Образования», Сферум, СКЗИ)	доступности	100
Суммарная величина потерь		1650

После произведения расчетов и построения таблицы 7 мы определились с риском финансовых потерь для образовательной организации, которая может составить приблизительно 1 650 000 рублей. Из этого можно сделать вывод, что для колледжа это будет очень существенной потерей. Для понимания насколько эффективны предложенные мероприятия для обеспечения информационной безопасности при использовании социальных сетей и мессенджеров в образовательном процессе необходимо произвести расчет показателей экономической эффективности рекомендаций.

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы.

Ресурс может быть определен в виде количества людей, привлекаемых к защите информации, в виде инженерных конструкций и технических средств, применяемых для защиты, денежных сумм для оплаты труда людей, строительства, разработки и покупки технических средств, их эксплуатации и других расходов. Наиболее общей формой представления ресурса является денежная мера. Ресурс, выделяемый на защиту информации, может иметь разовый и постоянный характер.

Разовый ресурс расходуется на закупку, установку и наладку дорогостоящей техники.

Постоянный ресурс - на заработную плату сотрудникам службы безопасности и поддержание определенного уровня безопасности, прежде всего, путем эксплуатации технических средств и контроля эффективности защиты.

Затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Совокупная стоимость владения для системы ИБ в общем случае складывается из стоимости: проектных работ; закупки и настройки

программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и ААА (средства аутентификации, авторизации и администрирования); затрат на обеспечение физической безопасности; обучения персонала; управления и поддержки системы (администрирование безопасности); аудита ИБ; периодической модернизации системы ИБ [8].

Суммарно ежегодные затраты на информационную безопасность складываются из трех показателей: затраты на организационные мероприятия; затраты на мероприятия инженерно-технической защиты; затраты на ликвидацию последствий.

Таким образом, для определения экономической эффективности защиты информации образовательной организации необходимы следующие данные (показатели): расходы (выделенные ресурсы) на создание/модернизацию данной и поддержание её в работоспособном состоянии; величины потерь (рисков), обусловленных угрозами информационным активам после внедрения/модернизации защиты информации.

Данные о содержании и объеме разового ресурса, выделяемого на защиту информации, представлены в таблице 8 [37].

Таблица 8 − Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п/п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час.)	Стоимость, всего (тыс.руб.)
1	Разработка методик и приказов	250	5	1250
2	Доведение информации до сотрудников, обучение, тренинги.	250	2	500
Стоимость проведения организационных мероприятий, всего				1750
Мероприятия инженерно-технической защиты				
	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб.)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
	Приобретение лицензии на	2	50	100

	антивирусную систему (комплексное решение в комплекте с антиспам, фаервол, защита эл. почты и т.д.)			
	Лицензии на ОС Windows10	9,2	50	460
	Установка и обновление программного обеспечения чел./час.	0,4	40	16
	Установка СКЗИ программного комплекса ViPNet Client 4 (1 канал на 1 рабочее место)	8	1	8
Стоимость проведения мероприятий инженерно-технической защиты				584

Содержание и объем постоянного ресурса, выделяемого на защиту информации, представлены в таблице 9.

Таблица 9 − Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п/п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час.)	Стоимость, всего (тыс.руб.)
1	Проведение тренингов, инструктажей.	0,4	40	4
Стоимость проведения организационных мероприятий, всего				4
Мероприятия инженерно-технической защиты				
	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб.)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
2	Обновление ПО	15	1	15
3	Создание защищенной виртуальной частной сети, которая соответствует заявленным требованиям	8	1	8
4	Протокол signal			бесплатно
5	DLP-системы	20	1	20
6	КОМРАД от «НПО «Эшелон»	40	1	40
Стоимость проведения мероприятий инженерно-технической защиты				83 000

Таким образом, для разработки информационной безопасности требуется 585 750 руб., а для ежегодной поддержки - 87 000 руб. Для проведения расчета необходимо получить прогнозируемые данные о величине потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации защиты информации. Результаты формируются по результатам экспертного опроса (см. таблицу 10).

Таблица 10 − Величины потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации защиты информации

Актив	Угроза	Величина потерь (тыс.руб.)
Документация образовательной организации	конфиденциальности	10
Документация образовательной организации	целостности	50
Документация образовательной организации	доступности	2

Продолжение таблицы 10

Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	конфиденциальности	50
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	целостности	10
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	доступности	20
Личные данные обучающихся	конфиденциальности	30
Личные данные обучающихся	целостности	2
Личные данные обучающихся	доступности	2
Личные сведения о сотрудниках	конфиденциальности	10
Личные сведения о сотрудниках	целостности	1
Личные сведения о сотрудниках	доступности	1
Системное программное обеспечение	конфиденциальности	0
Системное программное обеспечение	целостности	10
Системное программное обеспечение	доступности	10
Прикладное программное обеспечение (в т.ч. АСУ «ProCollege», Региональная АИС «Сетевой город. Образования», Сферум, СКЗИ)	конфиденциальности	0
Прикладное программное обеспечение (в т.ч. АСУ «ProCollege», Региональная АИС «Сетевой город. Образования», Сферум, СКЗИ)	целостности	10
Прикладное программное обеспечение (в т.ч. АСУ «ProCollege», Региональная АИС «Сетевой город. Образования», Сферум, СКЗИ)	доступности	10
Суммарная величина потерь		228 000

Оценка динамики величин потерь за период 2года (см. таблицу 11).

Таблица 11 − Оценка динамики величин потерь

	1 кв.	2 кв.	3 кв.	1 год	1 кв.	2 кв.	3 кв.	2 год
До внедрения СЗИ	412,5	825	1237,5	1650	2062,5	2475	2887,5	3300
После внедрения СЗИ	57	114	171	228	285	342	399	456
Снижение потерь	355,5	711	1066,5	1422	1777,5	2133	2488,5	2844

После принятия обязательных допущений о неизменности частоты появления угроз, а также о неизменном уровне надежности созданной защиты

информации, возможно определить срок окупаемости ($Т_{ок}$). Это выполняется аналитическим способом, с использованием приведенной ниже формулы:

$$T_{ок} = \frac{R_{\Sigma}}{(R_{ср} - R_{прогн})} \quad (3)$$

и графическим, как это представлено на рисунке 4.

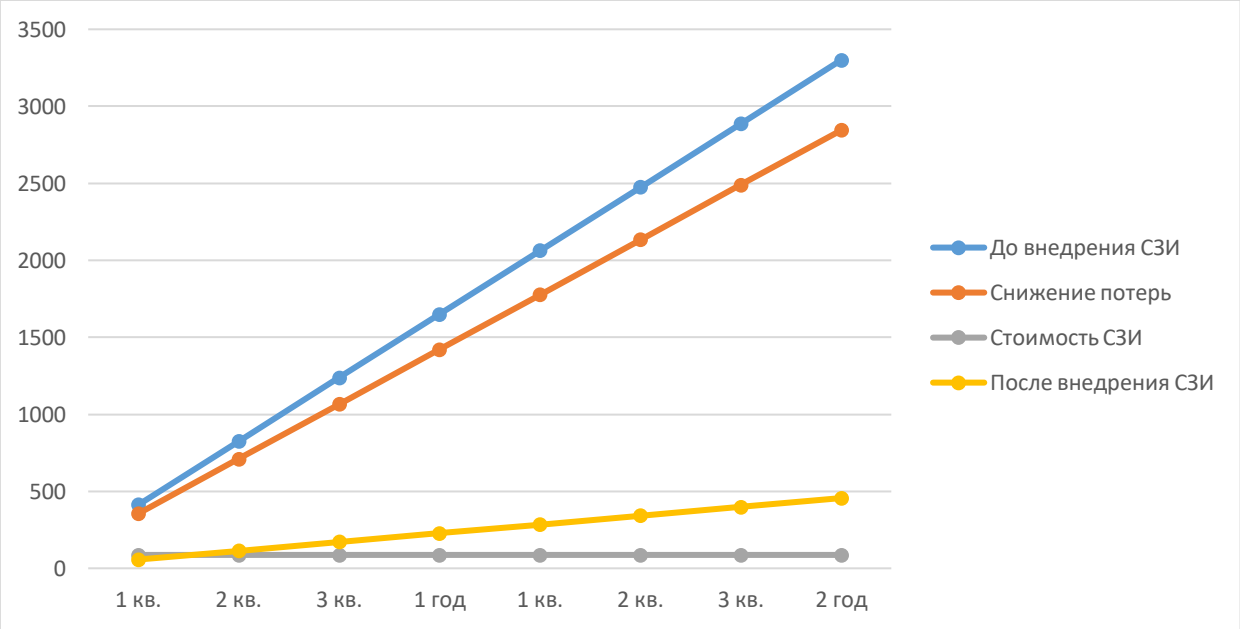

Рисунок 4 - Графическое определение срока окупаемости

Таким образом экономические расчеты показывают эффективность внедрения комплекса информационной защиты по обеспечению информационной безопасности в социальных сетях и мессенджерах. Согласно проведённым расчётам, окупаемость информационной безопасности произойдёт ещё в первом квартале её использования. Что для колледжа является очень минимальной финансовой нагрузкой.

Выводы по второй главе

Во второй главе описано текущее состояние политики информационной безопаности при использовании социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж» (актуальные уязвимости и риски), разработаны рекомендации по использованию социальных сетей и мессенджеров в образовательном

процессе в условиях информационной безопасности, проведен расчет экономической эффективности разработанных рекомендаций по обеспечению информационной безопаности при использовании социальных сетей и мессенджеров в образовательной организации.

Политика информационной безопасности колледжа (ГБПОУ «Челябинский профессиональный колледж») представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов колледжа от угроз информационной безопасности. Объектом защиты являются автоматизированные системы (как собственной, так и сторонней разработки), входящие в состав информационной системы колледжа.

В колледже введены в эксплуатацию следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства): ИСПДн «Обучающиеся и абитуриенты» ГБПОУ «ЧелПК» (далее - ИСПДн «Обучающиеся и абитуриенты»); ИСПДн «Сотрудники» ГБПОУ «ЧелПК» (далее - ИСПДн «Сотрудники»); ИСПДн «Библиотека» ГБПОУ «ЧелПК» (далее - ИСПДн «Библиотека»); АСУ «ProCollege»; региональная АИС «Сетевой город. Образования»; информационно-коммуникационная образовательная платформа Сферум» (VK Мессенджер); социальные сети и мессенджеры: электронная почта, WhatsApp, Telegram, «ВКонтакте», Яндекс.

Проанализировав популярные на сегодняшний день технологии защиты информации в социальных сетях и мессенджерах, анализ рисков и уязвимостей системы защиты персональных данных, мы разработали рекомендации по использованию социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж» при соблюдении политики информационной безопасности.

Основными задачами рекомендаций являются: улучшение организационного и технического уровня защиты информации; повышение эффективности, непрерывности, контролируемости мероприятий по

обеспечению противодействия вредоносной информации в социальных сетях и мессенджерах; организация периодической проверки соблюдения информационной безопасности сотрудниками.

Для предотвращения ошибок и взломов системы предпринимаются меры программно-технической безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит, экранирование, криптография. Для обеспечения защиты личных данных мы остановились на программных и криптографических средствах, таких как DLP-системы и SIEM-системы, протокол Signal.

В параграфе 2.3 произведены расчеты, из них мы можем увидеть, что прогнозируемый ущерб является достаточно весомым для образовательной организации, а едино разовые затраты на реализацию политики информационной безопасности меньше, чем предполагаемые финансовый ущерб. Это говорит о том, что реализация политики информационной безопасности поможет защитить данные, и это будет эффективная защита, которая поможет предотвратить финансовые потери для колледжа от возможных угроз в целом, а также при использовании мессенджеров и социальных сетей, в частности. И через 2 года политика информационной безопасности, реализованная в образовательной организации (ГБПОУ «ЧелПК»), поможет защитить порядка одного миллиона рублей.

Соответственно можно сделать вывод, что разработанные рекомендации по использованию мессенджеров и социальных сетей, направленные на предотвращение утечки персональных данных и защиты информации в социальных сетях и мессенджерах в рамках политики информационной безопасности образовательной организации являются эффективными.

ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности в мессенджерах и социальных сетях - актуальная проблематика не только для корпоративных структур, коммерческая информация и интеллектуальный капитал которых находится в поле поиска злоумышленников, но и для образования.

Информационная безопасность является важным аспектом в использовании популярных мессенджеров и социальных сетей. В связи с ростом цифровой коммуникации и обменом информацией, защита данных и личной информации становится все более актуальной задачей.

Исходя из этого, важно определить то, какие инструменты и механизмы необходимо применять, чтобы формировать информационную безопасность виртуального пространства социальных сетей, сохраняя интересы всех его участников.

Мессенджеры и социальные сети стали новым явлением в информатизации образования и представляют собой новые дидактические средства. Они позволяют преподавателям и студентам общаться в режиме реального времени, проводить онлайн-конференции, вебинары и другие образовательные мероприятия. Также позволяют создавать групповые чаты, что упрощает коммуникацию в рамках учебных проектов и обсуждение учебных материалов. Кроме того, социальные сети могут быть использованы для публикации новостей, объявлений и другой актуальной информации, для создания электронных портфолио, публикации проектов и презентаций.

Однако, необходимо учитывать ограничения и риски, связанные с их использованием, и обеспечивать правильную организацию и контроль их использования в учебном процессе.

Вопросы обеспечения информационной безопасности в мессенджерах и социальных сетях является важной задачей, которая требует особого внимания и подхода. Для управления защитой персональных и личных данных физического пользователя или целой организации необходимо принятие

различных рекомендаций, методов и инструментов по обеспечению информационной безопасности в рамках пользования социальными сетями и мессенджерами. К основным аспектам данной задачи относится конфиденциальность данных, защита от вредоносных программ, контроль доступа, защита от фишинга, обучение пользователей правилам безопасности.

В рамках второй главы описано текущее состояние политики информационной безопаности при использовании социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж» (актуальные уязвимости и риски), разработаны рекомендации по использованию социальных сетей и мессенджеров в образовательном процессе в условиях информационной безопасности, проведен расчет экономической эффективности разработанных рекомендаций по обеспечению информационной безопаности при использовании социальных сетей и мессенджеров в образовательной организации.

Проанализировав популярные на сегодняшний день технологии защиты информации в социальных сетях и мессенджерах, анализ рисков и уязвимостей системы защиты персональных данных, мы разработали рекомендации по использованию социальных сетей и мессенджеров в образовательном процессе ГБПОУ «Челябинский профессиональный колледж» при соблюдении политики информационной безопасности.

Основными задачами рекомендаций являются: улучшение организационного и технического уровня защиты информации; повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению противодействия вредоносной информации в социальных сетях и мессенджерах; организация периодической проверки соблюдения информационной безопасности сотрудниками.

Для предотвращения ошибок и взломов системы предпринимаются меры программно-технической безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит, экранирование, криптография. Для обеспечения защиты личных данных мы

остановились на программных и криптографических средствах, таких как DLP-системы и SIEM-системы, протокол Signal.

Произведен расчет экономической эффективности рекомендаций по обеспечению информационной безопаностью при использовании социальных сетей и мессенджеров на базе ГБПОУ «Челябинский профессиональный колледж». В результате расчетов разовые затраты на реализацию политики информационной безопасности меньше, чем предполагаемые финансовый ущерб. Это говорит о том, что реализация политики информационной безопасности поможет защитить данные, и это будет эффективная защита, которая поможет предотвратить финансовые потери для колледжа от возможных угроз в целом, а также при использовании мессенджеров и социальных сетей, в частности.

Оценка эффективности предложенных мероприятий показала их целесообразность внедрения в образовательную организацию. Дано экономическое обоснование эффективности и окупаемости защиты информации, в результате которой было установлено, что окупаемость защиты происходит за несколько лет, причём время окупаемости прямо пропорционально количеству отраженных атак, а эффективность будет расти с каждым годом.

Соответственно можно сделать вывод, что разработанные рекомендации по использованию мессенджеров и социальных сетей, направленные на предотвращение утечки персональных данных и защиты информации в социальных сетях и мессенджерах в рамках политики информационной безопасности образовательной организации являются эффективными.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального образования с целью повышения эффективности защиты информации при использовании социальных сетей и мессенджеров в образовательном процессе.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Андреев К. Метод оценки экономической эффективности подразделения по защите информации / К. Андреев. – URL: https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения: 24.11.2023).

2. Апанина А. М. Использование социальных сетей и мобильных мессенджеров как форм интерактивной работы с родителями / А.М. Апанина. − URL: https://www.prodlenka.org/metodicheskie-razrabotki/516968-ispolzovanie-socialnyh-setej-i-mobilnyh-messe (дата обращения: 15.12.2023).

3. Аснович Н. Г. Использование социальных сетей в образовательном процессе / Н. Г. Аснович // Информационные технологии в образовании, науке и производстве : IV Международная научно-техническая интернет-конференция, 18-19 ноября 2019 г. Секция Современные информационные технологии в преподавании технических и гуманитарных дисциплин. 2019.

4. Башлыков М. Социальные сети как угроза корпоративной информационной безопасности / М. Башлыков. – URL: http://lib.itsec.ru/articles2/Inf_security/social-networks (дата обращения: 24.11.2023).

5. Белова Е. С. Интернет-технологии и социальные сети как средство учебной коммуникации / Е. С. Белова. − URL: https://urok.1sept.ru/articles/697742 (дата обращения: 11.11.2023).

6. Бондаренко Е. Социальные сети как инструмент развития: виды и возможности / Е. Бондаренко. – URL: http://www.trainings.ru/library/articles/?id=10067 (дата обращения 20.10.2023).

7. Букаева А.А. Использование социальных сетей в образовательном процессе / А.А. Букаева, А. Т. Магзумова // Инновации в науке. 2015. №2 (39). − URL: https://cyberleninka.ru/article/n/ispolzovanie-sotsialnyh-setey-v-obrazovatelnom-protsesse (дата обращения: 21.12.2023).

8. Буянов Д.С. Информационная безопасность в социальных сетях / Д. С. Буянов // Молодой ученый. – 2018. – №39. – С. 14-16.

9. Гель А.В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ / А.В. Гель, А. О. Путилов // Скиф. – 2020. – №5-1 (45). – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sotsialnyh-setyah (дата обращения: 10.10.2023).

10. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

11. Диких Э.Р. Об использовании социальных сетей в образовании / Э. Р. Диких // Личность, семья и общество: вопросы педагогики и психологии: сб. ст. по матер. XVI междунар. науч.-практ. конф. Часть I. Новосибирск: СибАК. 2022.

12. Информационная безопасность. – URL: https://pirit.biz/reshenija/informacionnaja-bezopasnost (дата обращения: 10.10.2023).

13. Клименко О. А. Социальные сети как средство обучения и взаимодействия участников образовательного процесса / О. А. Клименко // Теория и практика образования в современном мире: материалы Междунар. науч. конф. (г. Санкт-Петербург, февраль 2012 г.). СПб.: Реноме. 2012. С. 405-407. – URL: https://moluch.ru/conf/ped/archive/21/1799 (дата обращения: 14.10.2023).

14. Козырева А.А. Социальные сети в России: развивается ли новый политический институт? / А. А. Козырева // Электронный научный журнал «ГосРег». − 2014. № 1. – URL: https://elibrary.ru/item.asp?id=239206962 (дата обращения: 14.10.2023).

15. Кривоухов А.А. Оценка информационной безопасности интернет-среды пользователями социальных сетей / А. А. Кривоухов // Коммуникология. – 2018. – №1.

16. Куликов Н. В. Разработка политики информационной безопасности предприятия (на примере ООО Саунбилд) / Н. В. Куликов. – URL:

https://dspace.tltsu.ru/bitstream/123456789/4133/1/%D0%9A%D1%83%D0%BB%D0%B8%D0%BA%D0%BE%D0%B2%20%D0%9D.%D0%92._%D0%9F%D0%98%D0%B1%D0%B4-1202%D0%B0.pdf

17. Ласукова Н. А., Рабкина Н. В. Обзор публикаций о роли социальных сетей и мессенджеров в обучении иностранному языку / Н. А. Ласукова, Н. В. Рабкина // Виртуальная коммуникация и социальные сети. – 2022. – №1. – URL: https://cyberleninka.ru/article/n/obzor-publikatsiy-o-roli-sotsialnyh-setey-i-messendzherov-v-obuchenii-inostrannomu-yazyku (дата обращения: 15.12.2023).

18. Левитин Р.В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ СОЦИАЛЬНЫХ СЕТЕЙ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ / Р. В. Левитин // «Актуальные вопросы развития современного образования» «Актуальные вопросы развития современного образования»: Материалы международной научно-практической конференции «СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ-2023», 15 марта 2023 года. Костанай: Костанайский региональный университет имени А.Байтурсынова, 2023. – С. 222-225.

19. Левитин Р.В. Обеспечение информационной безопасности в популярных мессенджерах и социальных сетей / Р. В. Левитин // Фундаментальные научно-практические исследования: актуальные тенденции и инновации. Сборник научных трудов по материалам XLVIII Международной научно-практической конференции (г.-к. Анапа, 29 декабря 2023 г.). – Анапа: Изд-во «НИЦ ЭСП» в ЮФО, 2023. – С. 37-41.

20. Малова А.В. Опыт использования социальной сети «ВКонтакте» в образовательном процессе. – URL: http://проф-обр.рф/blog/2017-01-23-968 (дата обращения: 14.10.2023).

21. Манапова О.Н. СОВРЕМЕННЫЕ МЕССЕНДЖЕРЫ В УЧЕБНОМ ПРОЦЕССЕ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ: СИЛЬНЫЕ И СЛАБЫЕ СТОРОНЫ / О. Н. Манапова, М. С.

Подин // Инновационное развитие профессионального образования. – 2021. – №3 (31). – URL: https://cyberleninka.ru/article/n/sovremennye-messendzhery-v-uchebnom-protsesse-professionalnoy-obrazovatelnoy-organizatsii-silnye-i-slabye-storony (дата обращения: 14.10.2023).

22. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 16 мая 2019 г.). – URL: https://pravo.edusite.ru/Guidelines-16-05-2019.pdf дата обращения: 24.10.2023).

23. Мирсанова О.А. К ВОПРОСУ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАТРАТ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ / О. А. Мирсанова // Интеллект. Инновации. Инвестиции. 2015. − №3. − URL: https://cyberleninka.ru/article/n/k-voprosu-ob-otsenke-effektivnosti-zatrat-na-informatsionnuyu-bezopasnost (дата обращения: 15.12.2023).

24. Муромцева А.В. Проблемы информационной безопасности в социальных сообществах в сети Интернет / А. В. Муромцева, В. В. Муромцев // Вестник РГГУ. Серия «Экономика. Управление. Право». – 2016. №3 (5).

25. Набатов А. В. Защита информации в социальных сетях и мессенджерах / А. В. Набатов, А. В. Григорьев // Программная инженерия: методы и технологии разработки информационно-вычислительных систем (ПИИВС-2020): сборник научных трудов III Международной научно-практической конференции (студенческая секция), Донецк, 25–26 ноября 2020 года. Том 2. – Донецк: Донецкий национальный технический университет, 2020. – С. 28-31.

26. Ненашев С.М. Информационно-технологическая и информационно психологическая безопасность пользователей социальных сетей / С. М. Ненашев С. М. // Вопросы кибербезопасности. 2020. № 5 (18).

27. Николаева Е. А. Использование социальных сетей и мессенджеров в образовании / Е. А. Николаева // Аграрное образование в условиях модернизации и инновационного развития АПК России : материалы всероссийской (национальной) научно-методической конференции, Улан-Удэ, 24 апреля 2020 года / ФГБОУ ВО «Бурятская государственная сельскохозяйственная академия имени В. Р. Филиппова». – Улан-Удэ: Бурятская государственная сельскохозяйственная академия имени В.Р. Филиппова, 2020. – С. 230-232.

28. Новые цифры: Facebook признал утечку данных 87 млн пользователей. – URL: https://delo.ua/business/novye-cifry-facebook-priznal-utechku-dannyh-87-mln-chelovek-341074/ (дата обращения: 24.12.2022).

29. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. − Режим доступа: www.consultant.ru (дата обращения: 10.09. 2023.

30. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. – Режим доступа: www.consultant.ru (дата обращения: 10.09. 2023).

31. Об утверждении состава содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [Приказ ФСТЭК России от 18 февраля 2013 г. № 21, в ред. от 14.05.2020 г. № 68]. – Режим доступа: https://fstec.ru/. (дата обращения: 20.09.2023).

32. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

[Электронный ресурс]: [постановление правительства РФ от 01.11.2012 г. №1119**]. –** Режим доступа: www.consultant.ru (дата обращения: 10.09. 2023).

33. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: [Приказ ФСТЭК России от 11.02.2013 г. № 17, в ред. от 29.05.2019 г.] – Режим доступа: www.consultant.ru (дата обращения: 20.09.2023).

34. Павлова О.В. Социальные сети как инструмент информального образования / О. В. Павлова // Социальное взаимодействие в различных сферах жизнедеятельности: Материалы II Международной научно-практической конференции. – СПб.: Экспресс, 2012. – С. 122-129.

35. Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

36. Программно-аппаратная защита информации // searchinform [Электронный ресурс]. – URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/programmno-apparatnaya/ (дата обращения: 15.10.2023).

37. Разработка нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности [Электронный ресурс]: [методический документ ФСБ России: от 31.05.2015 г. № 149/7/2/6-432]. − Режим доступа: https://docs.cntd.ru. (дата обращения: 20.11.2023).

38. Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005).

39. Родионова Н. В. Потенциальные возможности использования социальных сетей в качестве образовательного ресурса / Н. В. Родионова, М.Н. Яранская // «Научное сообщество студентов: проблемы художественного и

музыкального образования»: сб. мат-лов Всерос. студ-й науч.-практ. конф. – Чебоксары: Чуваш. гос. пед. ун-т им. И. Я. Яковлева, 2017. – С. 66-69.

40. Рудинский И.Д. Социальные сети образовательного назначения как объект защиты при подготовке специалистов по информационной безопасности / И. Д. Рудинский, Д. Я. Околот // Открытое образование. – 2019; 23(1). – С. 46-56. – URL: https://openedu.rea.ru/jour/article/view/586?locale=ru_RU (дата обращения: 14.10.2023).

41. Рузина Т. А. Педагогическая составляющая социальных сетей в открытой образовательной среде / Т. А. Рузина // Стратегия и тактика подготовки современного педагога в условиях диалогового пространства образования: сборник научных статей, Брянск, 20–21 апреля 2023 года. – Брянск: РИСО БГУ; ООО «Аверс», 2023. – С. 205-210.

42. Сабанова М.М. РОЛЬ СОЦИАЛЬНЫХ СЕТЕЙ В ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ / М. М. Сабанова, А. Х. Виндижева, Т. Х. Виндижев // Научные междисциплинарные исследования. – 2020. – №6. – URL: https://cyberleninka.ru/article/n/rol-sotsialnyh-setey-v-informatizatsii-obrazovaniya-1 (дата обращения: 24.09.2023).

43. Социальная сеть. Википедия [Электронный ресурс]. − URL: http: //ru.wikipedia. org/wiki/Социальная_сеть_(Интернет) (дата обращения: 11.11.2023).

44. Технологии защиты информации. – URL: https://studfile.net/preview/5663206/ дата обращения: 24.09.2023).

45. Тумбинская М.В. Обеспечение защиты от нежелательной информации в социальных сетях / М. В. Тубинская // Вестник МГУ. – 2017. – №2.

46. Шестакова Я. Безопасность персональных данных в социальных сетях / Я. Шестакова // Гуманитарные научные исследования. – 2015. – № 11.

47. Barnes J. A. Class and Comittees in Norwegian Island Parish // Human Relations. Hafner Press. – NY., 1975. – P. 39-58.

48. Boyd D. M. Social Network Sites: Definition, History, and Scolarship / D. M. Boyd, N. B. Elison // Journal of Computer-Mediated Communication. – 2007. – Vol. 13 (1). – P. 210-230.

49. Gilpin D. R. Working the Twittersphere: Microblogging as professional identity construction [Electronic resource] // A networked self: Identity, community, and cultureon social network sites. – NY, 2011. – Chapter 11. – P. 232-250. – Mode of access: https://www.academia.edu/197814/Working_the_Twittersphere_Microblogging_as_professional_identity_construction (date of access: 15.04.2023).

50. Handley A., Chapman A. Content Rules // How to Create Killer Blogs, Podcasts, Videos, Ebooks, Webi-nars (and More) That Engage Customers and Ignite Your Business. – Hoboken, N.J.: Wiley, 2011.