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

Формирование компетентности сотрудников в области информационной безопасности в процессе информатизации образовательной организации

Магистерская диссертация по направлению:
44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения заочная

Проверка на объем заимствований:
80,49% авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Фаляхитдинов Эрик Рашитович

Научный руководитель:
к.п.н., доцент
Диденко Галина Александровна

Челябинск
2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Индустрия безопасности является малоизученной областью; ее разнообразные, дублирующие друг друга функции и иногда нестандартная терминология затрудняют точное определение границ. Однако готовность к риску и устойчивость отдельных лиц, организаций и целых экономик зависят от действующих систем безопасности и инфраструктуры. Для их осуществления требуется квалифицированная и информированная рабочая сила [59].

Пробелы в кадрах в области безопасности привели работодателей и преподавателей к тому, что необходимо пересмотреть использование моделей компетенций в качестве инструментов для определения и оценки квалификации и навыков работников.

Компетентность определяется как знания, навыки и способности, которые влияют на основную функцию работы, указывают на успешное выполнение работы, измеряются в соответствии со стандартами и подлежат улучшению с помощью обучения и опыта.

Педагогическая наука пытается найти пути решения выше обозначенных вызовов, проводя исследования по направлению информационной безопасности личности в условиях информационного общества. Актуальность поставленных проблем отражена и в майском указе 2015 года Президента РФ, в котором утверждена Стратегия национальной безопасности РФ до 2030 года [11].

Принципиальная особенность Стратегии состоит в том, что обеспечение безопасности России рассматривается в тесной связи с решением проблем социально-экономического и культурного развития страны. Это ставит перед педагогическим образованием следующую цель: повышение цифровой грамотности педагогов. Педагог должен формировать у подрастающего поколения навыки информационной безопасности и медиаграмотности, которые позволили бы обучающемуся самостоятельно оценивать опасность

тех или иных ресурсов, противостоять возникающим в глобальной сети Интернет новым угрозам и рискам, компьютерной и интернет-зависимости, самостоятельно организовывать учебную деятельность в условиях функционирования информационной среды дистанционного и электронного обучения.

Педагоги должны понимать, что современная молодежь живет в новом информационном обществе глобальной коммуникации, в котором существуют как новые возможности, так и новые угрозы, и риски, и чтобы обучающиеся выросли конкурентоспособными гражданами, они должен знать эти возможности. Если при этом он столкнется с угрозами и рисками, у него будет определенный «иммунитет». В связи с этим, педагог должен в обучении студента подвести его к пониманию возможного манипулирования его поведением и сознанием при помощи информации, распространяемой СМИ, социальными сервисами в Интернете и др. Кроме этого, в современном обществе для безопасной социализации обучающемуся и педагогу необходимо противостоять информационным угрозам и сетевым атакам.

Необходимая квалификация педагога, способного влиять на обучающихся, формировать их устойчивость к информационным угрозам, может быть достигнуто путем введения в соответствующие стандарты образования соответствующих компетенций, направленных на формирование информационной культуры специалиста с обязательной составляющей – компетентностью в области информационной безопасности.

Система повышения квалификации педагога и сотрудников, характеризуясь компетентностной направленностью, требует переориентации на сформированность устойчивой профессиональной компетентности в области информационной безопасности, которая формируется в неразрывном единстве и системе с ключевыми и общепрофессиональными компетентностями и требует постоянного обновления и актуализации в связи с появляющимися новыми уязвимостями и рисками в контексте перманентной информатизации.

При этом в силу специфики информатизации объектов информатизации – образовательных организаций, повышение квалификации сотрудников должно происходить на базе образовательной организации, где педагог постоянно работает.

Степень разработанности проблемы. Отечественные и зарубежные исследования, связанные с проблематикой информационной безопасности (далее ИБ), широко раскрывают следующие вопросы:

– общие научные и методологические вопросы информационной безопасности поднимаются в трудах Е.Б. Белов [21]; В.П. Шерстюк [72], W. Stallings [76];

– аспекты нормативно-правового обеспечения информационной безопасности (С.Л. Зефиров [41], Ю.М. Батурин [20]; О.А. Городов, Р.И. Дремлюга, Ю.А. Журавлев, Г.О. Крылов, Т.А. Полякова, D.B. Thaw [77]);

– аспекты ИБ как педагогической проблемы (Р.В. Амелин, А.А. Журин, П.Н. Корнюшин, А.А. Марков, В.А. Семененко, В.Н. Ясенев и др.);

– проблемы подготовки кадров и формирования компетентности в области ИБ (А.П. Коваленко [47], Е.Б. Белов [47]; А.С. Доронин, Э. В. Танова, E. Albrechtsen и др.).

Однако в научной литературе также отмечается, что в настоящее время вопросам целенаправленного формирования компетентности в области информационной безопасности в педагогических исследованиях уделяется недостаточно внимания.

Таким образом, существует *противоречие* между необходимостью повышения квалификации сотрудников образовательной организации в области информационной безопасности по месту трудовой деятельности и отсутствием практической и методической разработанности названного направления в системе повышения квалификации педагогических работников и сотрудников.

Компетентность как интегральная характеристика личности формируется в образовательном процессе через определенный набор

компетенций. На сегодняшний день созданы предпосылки для формирования компетентности в области информационной безопасности сотрудников и педагогов, которая предстает в неразрывном единстве и системе с ключевыми и общепрофессиональными компетенциями посредством приобретения ряда дополнительных специальных компетенций.

Необходимость разрешения противоречий, актуальность и недостаточная теоретическая и практическая разработанность проблемы определили выбор *темы исследования*: «Формирование компетентности сотрудников в области информационной безопасности в процессе информатизации образовательной организации».

Выбор темы исследования определен актуальностью проблемы, ее социальной значимостью, недостаточной теоретической разработанностью в педагогической литературе, а также потребностями в практических рекомендациях по повышению квалификации сотрудников образовательной организации в области информационной безопасности.

Цель исследования: выявление, теоретическое обоснование и экспериментальная проверка формирования компетентности сотрудников в области информационной безопасности у сотрудников образовательной организации.

Объект исследования: процесс формирования компетентности в области информационной безопасности у сотрудников образовательной организации.

Предмет исследования: разработка курса повышения квалификации «Информационная безопасность и защита персональных данных» для сотрудников образовательной организации.

Гипотеза исследования состоит в предположении о том, что формирование компетентности в области информационной безопасности у сотрудников образовательной организаций будет происходить эффективней, если разработать курс повышения квалификации в области информационной безопасности, реализованный по месту трудовой деятельности сотрудников,

учитывающий специфику образовательной организации как объекта информатизации.

В соответствии с объектом, предметом и целью исследования были поставлены следующие *задачи:*

– изучить законодательные акты и нормативно-правовые документы, разработки в области комплексной информатизации образовательных организаций;

– рассмотреть понятийный аппарат, выявить закономерности и принципы процесса информатизации в образовательной организации;

– проанализировать профессиональные компетенции педагога среднего профессионального образования;

– раскрыть сущность и содержание компетентности сотрудников образовательной организации в области информационной безопасности;

– разработать курс повышения квалификации «Информационная безопасность и защита персональных данных»;

– провести опытно-экспериментальную работу по формированию компетентности в области информационной безопасности у сотрудников образовательной организации.

Методологической основой исследования являются фундаментальные работы в области:

– педагогики и психологии (Ю.К. Бабанский, В.П. Беспалько, Л.С. Выготский, П.Я. Гальперин, И.Я. Лернер, В.А. Сластенин и др.);

– профессиональной подготовки педагога в системе непрерывного педагогического образования (С.И. Архангельский, Н.В. Кузьмина, А.К. Маркова, Л.М. Митина, В.А. Сластенин, А.И. Щербаков и др.);

– психологического и педагогического консультирования и педагогического сопровождения (Е.А. Александрова, В.Г. Воронцова, Н.Н. Михайлова, К. Роджерс, С.Н. Чистякова и др.)

– информатизации образования (С.А. Бешенков, А.А. Кузнецов, М.П. Лапчик, Л.П. Мартиросян, А.Н. Привалов, И.В. Роберт и др.);

– компетентностного подхода к организации образовательного процесса (В.И. Байденко, А.С. Белкин, Э.Ф. Зеер, И.А. Зимняя, А.К. Маркова, А.В. Хуторской, Н.Ф. Ефремова);

– системного подхода (В.И. Андреев, Ю.К. Бабанский, А.П. Беляев, В.П. Беспалько, С.М. Маркова, В.А. Сластенин, Н.Ф. Талызина);

– разработки и использования автоматизированных обучающих систем в образовании (С.Г. Данилюк, А.Д. Дараган, В.Л. Латышев, А.А. Павлов, Ю.А. Романенко, В.И. Сердюков и др.);

– исследования проблем информационной, информационно-психологической безопасности (Ю.Д. Бабаева, Л.Н. Бабанин, С.В. Бондаренко, И.В. Бурлаков, В.А. Голубев, Л.О. Пережогин, Т.Л. Тропина, К. Янг и др.);

– аспекты нормативно-правового обеспечения информационной безопасности (В.М. Алексеев, Ю.М. Батурин, Р.И. Дремлюга, Г.О. Крылов, Т.А. Полякова, D.B. Thaw и др.);

– аспекты информационной безопасности как педагогической проблемы (Р.В. Амелин, О.В. Казарин, А.А. Марков, В.Н. Ясенев и др.);

– проблемы подготовки кадров и формирования компетентности в области информационной безопасности (Е.Б. Белов, И.Н. Доронина, Э.В. Танова, E. Albrechtsen и др.);

– теория профессионального образования (С.И. Архангельский, Е.Ф. Зеер, Р.А. Литвак, Н.А. Шайденко, А.Н. Сергеев, В.А. Сластенин и др.);

– исследования, которые раскрывают содержание, структуру педагогической деятельности, закономерности и особенности формирования личности педагога в системе высшего педагогического образования (Т.В. Лисовский, А.А. Деркач, Ф.Н. Гоноболина, Н.А. Шайденко и др.);

– теории развития личности (Л.С. Выготский, А.Н. Леонтьев, В.А. Маслоу, Г. Оппорт, К. Роджерс и др.).

Научная новизна исследования заключается в следующем:

1. В постановке проблемы о необходимости формирования компетентности в области информационной безопасности у педагогов образовательной организации и разработке понятийного аппарата в области изучения информационной безопасности.

2. Определены критерии и уровни сформированности компетентности в области информационной безопасности у сотрудников образовательной организации.

3. Разработан курс повышения квалификации, способствующий эффективному повышению уровня сформированности компетентности в области информационной безопасности у сотрудников образовательной организации.

Теоретическая значимость исследования заключается в следующем: с учетом аспектов информационной безопасности разработан и актуализирован понятийный аппарат, характеризующий информационную подготовку в рамках курса повышения квалификации педагогов в области информационной безопасности; определены место и роль проблематики информационной безопасности в организации обучения студентов колледжа.

Практическая значимость исследования заключается в том, что его результаты:

а) могут выступать основой для создания методических разработок с целью оптимизации процесса формирования компетентности в области информационной безопасности сотрудников образовательных организаций;

б) содействуют научно-обоснованному подходу к отбору содержания учебного материала, методов и форм обучения, обусловливающих эффективность формирования компетентности в области информационной безопасности.

Разработанный курс повышения квалификации в области информационной безопасности может быть адаптирован и применен в других образовательных организациях.

В ходе работы применялись следующие *методы исследования:* изучение и анализ теоретической и методической литературы по проблеме исследования, нормативной документации, педагогический эксперимент.

Апробация исследования: результаты исследования были опубликованы на Международной научно-практической конференции «Молодой исследователь: вызовы и перспективы», 2021; Международной научно-практической конференции «Стимулирование научно-технического потенциала общества в стратегическом периоде», 2022.

База исследования: ГБПОУ «Южно-Уральский государственный технический колледж».

Структура магистерской диссертации состоит из введения, трех глав, заключения, списка использованных источников, состоящего из 77 наименований, приложения.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФОРМИРОВАНИЯ КОМПЕТЕНТНОСТИ СОТРУДНИКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Профессиональные компетенции педагога среднего профессионального образования

На сегодняшний день одной из проблем в образовательных организациях среднего профессионального образования является проблема непрерывного развития профессиональной компетентности педагогических работников, поскольку «обеспечение глобальной конкурентоспособности российского образования, вхождение РФ в число десяти ведущих стран мира по качеству образования» [59], возможно только при наличии высокопрофессионального педагогического сообщества.

Эффективность модернизации системы среднего профессионального образования зависит от способности преподавателей оперативно провести ревизию своих компетенций, выявить слабые места, нарастить актуальные и востребованные навыки и умения. Большую помощь в процессе самоанализа и пересмотра педагогами своих компетенций сыграло изучение Профессионального стандарта педагога профессионального образования, который был утвержден приказом Министерства труда и социальной защиты Российской Федерации от 08 сентября 2015 г. № 608н [10]. В профстандарте были сформулированы актуальные требования к знаниям и умениям педагогов СПО, призванных обеспечить экономику страны высококвалифицированными кадрами. Ведь работодатель желает получить активного, инициативного работника, быстро адаптирующегося к постоянно изменяющимся условиям труда, способного творчески и ответственно применять свои знания, умения и навыки на практике.

В настоящее время этот приказ признан утратившим силу (приказом Министерства труда и социальной защиты РФ № 832-н от 26.12.2019, рег. № 58533 от 01.06.2020). Готовятся существенные поправки, но, по утверждению

разработчиков, они большей частью будут касаться требований к квалификации преподавателей вузов [52], поэтому для целей нашего исследования мы используем прежний текст профстандарта, поскольку в анализируемый период (2019 – 2021 гг.) педагоги СПО работали согласно стандарту образца 2015 года.

Существенные перемены в образовании невозможны без кардинальных изменений профессионального сознания педагога. Появилось множество новых знаний, понятий, которые необходимы современному педагогу. Одно из таких понятий компетентность.

В структуру профессиональной компетентности современного преподавателя СПО входят следующие компетенции: педагогическая; предметная; методическая; научно-исследовательская; проектная; информационно-коммуникационная; рефлексивная [66].

Вступление России в Болонский процесс послужило прологом к внедрению компетентностного подхода в обучение как альтернативы существующему процессу формирования у обучающихся «знаний-умений-навыков», недостаточно учитывающих сущность компетентности специалиста в условиях рыночных отношений. Компетентностная модель образования является важнейшим условием модернизации и приведения его результатов в соответствие с международными стандартами.

Компетентностный подход – это подход, акцентирующий внимание на результате обучения, причем в качестве результата рассматривается не сумма усвоенной информации, а способность человека на ее основе адекватно действовать в различных ситуациях (в том числе и в ситуации неопределенности).

Идея компетентностного подхода – это, прежде всего, идея открытого заказа на содержание образования. В качестве результата рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях. Равновесие между образованием и жизнью

видится в смещении конечной цели образования со знаний на интеллектуальные деятельностно-практические умения – компетентность.

Компетентность определяется, как «готовность специалиста включиться в определенную деятельность». Сегодня на рынке труда востребованы не сами по себе знания, а именно способность выполнять определенные функции.

Понятия компетентность и компетенция (по А.В. Хуторскому) [69]:

Компетенция – включает совокупность взаимосвязанных качеств личности (знаний, умений, навыков, способов деятельности), задаваемых по отношению к определенному кругу предметов и процессов, и необходимых для качественной продуктивной деятельности по отношению к ним.

Компетентность – владение, обладание человеком соответствующей компетенцией, включающей его личностное отношение к ней и предмету деятельности.

Компетентность – сформированная характеристика личности, которая определяет варианты поведения или мышления обучаемого в различных ситуациях при выполнении определенной деятельности.

Компетентность – это профессионально-личностная, социально-значимую качественная характеристика специалиста, умеющего использовать знания, умения, навыки не только для профессиональной деятельности, но и для понимания социальной значимости и нравственного сознания своей деятельности (Л.М. Устич).

Структура компетентности (по В.Д. Шадрикову) [71].

В соответствии с функциональными блоками психологической системы деятельности:

–личностно-мотивационная составляющая;

–составляющая в части целеобразования;

–составляющая в части разработки и реализации программы деятельности;

–составляющие в части информационной основы деятельности;

–составляющие в части принятия решений;

–составляющие в части контроля и коррекции результатов деятельности.

Когнитивный компонент компетентности – это совокупность, система знаний, на основе которой строится целостная картина действительности и осуществляется процесс собственно деятельности.

Поведенческий компонент компетентности – это система универсальных способов познания, соответствующих алгоритмов поведения и способов коммуникации, ориентированных на реализуемую деятельность, развитие у человека разнообразных способов деятельности, необходимых для самореализации в профессиональной деятельности. Это реальная деятельность, осуществляемая в конкретных условиях, компонент практический, активный, определяющий, какими способами, методами, приемами и в каких формах осуществляется деятельность в различных ситуациях.

Ценностный компонент компетентности – это понимание смысла и значения реализуемой деятельности, субъективное нравственно-эстетическое, рефлексивное отношение к осваиваемым ценностям и способам их освоения, смелость в отстаивании своего мнения и своих взглядов, независимость в суждениях, чувство ответственности за предлагаемые инновационные решения.

Профессиональный стандарт – документ, включающий перечень профессиональных и личностных требований к работнику, действующий на всей территории Российской Федерации.

Во исполнение указа Президента Российской Федерации от 7 мая 2012 г. № 597 «О мероприятиях по реализации государственной социальной политики» Федеральным законом от 3 декабря 2012г. № 236-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации и статью 1 Федерального закона «О техническом регулировании» были внесены изменения и дополнения в Трудовой кодекс РФ, закрепившие в статье 195.1 новые понятия – «квалификация» и «профессиональный стандарт» [12].

Во исполнение статьи 195.1 Трудового кодекса РФ и постановления Правительства РФ от 22 января 2013 г. № 23 «О Правилах разработки, утверждения и применения профессиональных стандартов» Министерством труда и социальной защиты РФ были разработаны следующие ведомственные нормативные правовые акты:

– приказ Минтруда России от 12 апреля 2013 г. № 147н «Об утверждении Макета профессионального стандарта» (зарегистрирован в Минюсте России 24 мая 2013 г. № 28489);

– приказ Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов» (зарегистрирован в Минюсте России 27 мая 2013 г. № 28534);

– приказ Минтруда России от 29 апреля 2013г. №170н «Об утверждении методических рекомендаций по разработке профессионального стандарта», который по заключению Минюста России от 23 июля 2013 г. № 01/66036-ЮЛ не нуждается в государственной регистрации [12].

Письмо Минобрнауки России от 02.11.2015 № АК-3192/06 «О пилотном введении профессиональных стандартов».

Минтрудом России были утверждены профессиональные стандарты в сфере образования:

– «Педагог дополнительного образования детей и взрослых» (утвержден Приказом Минтруда России от 08.09.2015 № 613н);

– «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования» (утвержден Приказом Минтруда России от 08.09.2015 № 608н) [10];

– Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель) (утвержден Приказом Минтруда России от 18.10.2013 № 544н).

Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности) представлено в таблице 1 [10].

Таблица 1 – Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности) [55]

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалифи-кации	наименование	код	уровень (подуровень) квалификации
А	Преподавание по программам профессионального обучения, среднего профессионального образования (СПО) и дополнительным профессиональным программам (ДПП), ориентированным на соответствующий уровень квалификации	6	Организация учебной деятельности обучающихся по освоению учебных предметов, курсов, дисциплин (модулей) программ профессионального обучения, СПО и (или) ДПП	А/01.6	6.1
			Педагогический контроль и оценка освоения образовательной программы профессионального обучения, СПО и (или) ДПП в процессе промежуточной и итоговой аттестации	А/02.6	6.1
			Разработка программно-методического обеспечения учебных предметов, курсов, дисциплин (модулей) программ профессионального обучения, СПО и (или) ДПП	А/03.6	6.2

Продолжение таблицы 1

B	Организация и проведение учебно-производственного процесса при реализации образовательных программ различного уровня и направленности	6	Организация учебно-производственной деятельности обучающихся по освоению программ профессионального обучения и (или) программ подготовки квалифицированных рабочих, служащих	B/01.6	6.1
			Педагогический контроль и оценка освоения квалификации рабочего, служащего в процессе учебно-производственной деятельности обучающихся	B/02.6	6.1
			Разработка программно-методического обеспечения учебно-производственного процесса	B/03.6	6.2
C	Организационно-педагогическое сопровождение группы (курса) обучающихся по программам СПО	6	Создание педагогических условий для развития группы (курса) обучающихся по программам СПО	C/01.6	6.1
			Социально-педагогическая поддержка обучающихся по программам СПО в образовательной деятельности и профессионально-личностном развитии	C/02.6	6.1

Продолжение таблицы 1

D	Организационно-педагогическое сопровождение группы (курса) обучающихся по программам ВО	6	Создание педагогических условий для развития группы (курса) обучающихся по программам высшего образования (ВО)	D/01.6	6.1
			Социально-педагогическая поддержка обучающихся по программам ВО в образовательной деятельности и профессионально-личностном развитии	D/02.6	6.1
E	Проведение профориентационных мероприятий со школьниками и их родителями (законными представителями)	6	Информирование и консультирование школьников и их родителей (законных представителей) по вопросам профессионального самоопределения и профессионального выбора	E/01.6	6.1
			Проведение практикоориентированных профориентационных мероприятий со школьниками и их родителями (законными представителями)	E/02.6	6.1
F	Организационно-методическое обеспечение реализации программ профессионального обучения, СПО и ДПП, ориентированных на соответствующий уровень квалификации	6	Организация и проведение изучения требований рынка труда и обучающихся к качеству СПО и (или) дополнительного профессионального образования (ДПО) и (или) профессионального обучения	F/01.6	6.3

Продолжение таблицы 1

			Организационно-педагогическое сопровождение методической деятельности преподавателей и мастеров производственного обучения	F/02.6	6.3
			Мониторинг и оценка качества реализации преподавателями и мастерами производственного обучения программ учебных предметов, курсов, дисциплин (модулей), практик	F/03.6	6.3
G	Научно-методическое и учебно-методическое обеспечение реализации программ профессионального обучения, СПО и ДПП	7	Разработка научно-методических и учебно-методических материалов, обеспечивающих реализацию программ профессионального обучения, СПО и (или) ДПП	G/01.7	7.3
			Рецензирование и экспертиза научно-методических и учебно-методических материалов, обеспечивающих реализацию программ профессионального обучения, СПО и (или) ДПП	G/02.7	7.3

Продолжение таблицы 1

H	Преподавание по программам бакалавриата и ДПП, ориентированным на соответствующий уровень квалификации	7	Преподавание учебных курсов, дисциплин (модулей) или проведение отдельных видов учебных занятий по программам бакалавриата и (или) ДПП	H/01.6	6.2
			Организация научно-исследовательской, проектной, учебно-профессиональной и иной деятельности обучающихся по программам бакалавриата и (или) ДПП под руководством специалиста более высокой квалификации	H/02.6	6.2
			Профессиональная поддержка ассистентов и преподавателей, контроль качества проводимых ими учебных занятий	H/03.7	7.1
			Разработка под руководством специалиста более высокой квалификации учебно-методического обеспечения реализации учебных курсов, дисциплин (модулей) или отдельных видов учебных занятий программ бакалавриата и (или) ДПП	H/04.7	7.1

Продолжение таблицы 1

I	Преподавание по программам бакалавриата, специалитета, магистратуры и ДПП, ориентированным на соответствующий уровень квалификации	8	Преподавание учебных курсов, дисциплин (модулей) по программам бакалавриата, специалитета, магистратуры и (или) ДПП	I/01.7	7.2
			Профессиональная поддержка специалистов, участвующих в реализации курируемых учебных курсов, дисциплин (модулей), организации учебно-профессиональной, исследовательской, проектной и иной деятельности обучающихся по программам ВО и (или) ДПП	I/02.7	7.3
			Руководство научно-исследовательской, проектной, учебно-профессиональной и иной деятельностью обучающихся по программам бакалавриата, специалитета, магистратуры и (или) ДПП	I/03.7	7.2
			Разработка научно-методического обеспечения реализации курируемых учебных курсов, дисциплин (модулей) программ бакалавриата, специалитета, магистратуры и (или) ДПП	I/04.8	8.1

Продолжение таблицы 1

J	Преподавание по программам аспирантуры (адъюнктуры), ординатуры, ассистентуры-стажировки и ДПП, ориентированным на соответствующий уровень квалификации	8	Преподавание учебных курсов, дисциплин (модулей) по программам подготовки кадров высшей квалификации и (или) ДПП	J/01.7	7.3
			Руководство группой специалистов, участвующих в реализации образовательных программ ВО и (или) ДПП	J/02.8	8.2
			Руководство подготовкой аспирантов (адъюнктов) по индивидуальному учебному плану	J/03.8	8.2
			Руководство клинической (лечебно-диагностической) подготовкой ординаторов	J/04.8	8.2
			Руководство подготовкой ассистентов-стажеров по индивидуальному учебному плану	J/05.8	8.2
			Разработка научно-методического обеспечения реализации программ подготовки кадров высшей квалификации и (или) ДПП	J/06.8	8.3

Профессиональные стандарты применяются:

– работодателями при формировании кадровой политики и в управлении персоналом, при организации обучения и аттестации работников, разработке должностных инструкций, тарификации работ, присвоении тарифных разрядов работникам и установлении систем оплаты труда с учетом особенностей организации производства, труда и управления;

– образовательными организациями при разработке основных профессиональных образовательных программ и дополнительных профессиональных программ;

– при разработке в установленном порядке федеральных государственных образовательных стандартов профессионального образования.

Под профессиональной компетентностью применительно к педагогической деятельности понимается интегральная характеристика личности и профессионализма педагога, определяющая его способность результативно решать профессиональные задачи, возникающие в педагогической деятельности в конкретных реальных ситуациях. При этом педагогу приходится использовать свои знания, умения, опыт, жизненные ценности и нравственные ориентиры, свои интересы и наклонности.

Профессиональный стандарт педагогической деятельности включает 6 компетенций:

1. Компетентность в области личностных качеств.

2. Компетентность в постановке целей и задач педагогической деятельности.

3. Компетентность в мотивировании обучающихся (воспитанников) на осуществление учебной (воспитательной) деятельности.

4. Компетентность в разработке программы деятельности и принятии педагогических решений.

5. Компетентность в обеспечении информационной основы педагогической деятельности.

6. Компетентность в организации педагогической деятельности [55].

Рассмотрим алгоритм работы с компетенциями и компетентностями в процессе формирования профессиональных компетенций специалиста:

1) выявить весь набор компетенций в соответствии с профессиональным стандартом и (или) ФГОС ВО (СПО);

2) объединить компетенции в матрицу (паспорт, компетентностную модель);

3) описать признаки проявления общих и специальных профессиональных кластеров компетенций в будущей профессиональной деятельности;

4) выявить потенциал дисциплин или курсов для формирования кластера или отдельной компетенции;

5) разработать компетентностно-ориентированные задания для каждого кластера или компетенции;

6) определить логику и последовательность заданий для формирования компетенций;

7) подобрать педагогическую технологию, адекватную логике заданий для формирования компетенций и отслеживания результатов.

Для решения профессиональных задач специалист должен обладать соответствующими конкретным профессиональным задачам компетенциями, основными компонентами которых являются знания, умения, навыки и личностные качества специалиста. Совокупность же профессиональных компетенций, позволяющая выполнять весь перечень профессиональных задач в конкретной области, составляет компетентность специалиста в этой области.

Развитие профессиональной компетентности — это динамичный процесс усвоения и модернизации профессионального опыта, ведущий к развитию индивидуальных профессиональных качеств, накоплению профессионального опыта, предполагающий непрерывное развитие и самосовершенствование.

Таким образом, общим результатом обучения в системе образования является сформированная компетентность специалиста в определенной области, которая проявляется путем реализации соответствующих компетенций при решении профессиональных задач. Следовательно, при компетентностном подходе основное внимание в учебном процессе должно

уделяться формированию у обучающихся профессиональных компетенций по всему спектру профессиональных задач, выполняемых специалистом в его профессиональной деятельности.

1.2 Требования информационной безопасности для образовательной организации

Вопрос организации защиты информации в образовательной организации является в достаточной степени актуальным и диктует свои требования к защите ресурсов образовательных организаций и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации в рамках образовательной организации.

Информационная безопасность образовательных организаций отличается от информационной безопасности других предприятий и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью образовательных организаций, которые вынуждены делать доступ к информационным ресурсам легким с целью удобства для граждан.

Информационная безопасность в образовательных организациях должна учитывать следующие специфические факторы:

– конфиденциальность информации (несанкционированное получение информации, в т.ч. персональных данных сотрудников и обучающихся, служебной информации о самой образовательной организации);

– технические сбои и неполадки вычислительной техники и аппаратуры передачи данных, нарушения энергообеспеченности техники, физическое уничтожение или порча техники и др.;

– вредоносное и нежелательное программное обеспечение, хакерские атаки и спам;

– несанкционированное использование нелицензионного программного обеспечения сотрудниками образовательной организации;

– недисциплинированность и бесконтрольность педагогов, учебно-вспомогательного персонала и обучающихся в вопросах защиты информации;

– непонимание и незнание проблем информационной безопасности;

– нарушение авторских прав и прав интеллектуальной собственности.

В образовательной организации для обеспечения информационной безопасности необходимо:

– во-первых, целесообразно обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т.д.). Решение данной проблемы возможно только при условии, исключающем вывод локальных сетей образовательной организации на Интернет, либо размещение своего сайта у удаленного провайдера;

– во-вторых, необходимо иметь как минимум два сервера. Наличие хороших серверов позволит протоколировать любые действия работников образовательной организации в локальной сети;

– в-третьих, необходимо установить строгий контроль за электронной почтой, обеспечив постоянный контроль за входящей и исходящей корреспонденцией;

– в-четвертых, установка соответствующих паролей на персональные ЭВМ, а также определение работы с информацией на съемных носителях ЭВМ (флэшки, диски). И самое главное, класс информатики не должен быть подключен к локальным сетям образовательной организации.

В свою очередь, ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации» определяет порядок защиты информации [6]. В соответствии с данной статьей защита информации представляет собой принятие правовых, организационных и технических мер. Меры должны быть направлены на обеспечение защиты информации от неправомерного доступа, уничтожения,

модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации [6].

Образовательный процесс касается наименее защищенных от пропаганды членов общества –подростков. Поэтому система информационной безопасности образовательной организации должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены образовательной организации любой пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание обучающихся.

Разнообразные информационные системы достаточно давно и эффективно используются в образовательном процессе, активизируя познавательную активность обучающихся, влияя на их творческие способности, на вовлеченность в образовательный процесс. Однако это только одна из граней внедрения и введения информационных систем в образовательную организацию. Другой особенностью является использование систем не только в качестве обучающих средств, но и в поддержке организации данного процесса, и в управлении образовательной организации.

В качестве основных направлений обеспечения информационной безопасности подростков можно выделить следующие:

1) правовая защита, заключающаяся в создании нормативно-правовой базы регулирования общественных отношений в этой области;

2) технологическая защита, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления родительского контроля за временем пребывания обучающегося в сети и качественный анализ сайтов и интернет-сообществ, посещаемых ими;

3) психолого-педагогические методы, направленные на работу с обучающимся по формированию его медиа и компьютерной грамотности, стратегий поведения при встрече с нежелательным контентом и опасными

знакомыми в сети Интернет, формирование критического мышления по отношению к информации, получаемой в сети и др.

Наиболее эффективными признаны методы психолого-педагогического воздействия, без отрицания значения первых двух.

Однако в России программы, направленные на повышение грамотности педагогов в области обеспечения информационной безопасности обучающихся, в настоящее время пока только разрабатываются. В связи с этим встает вопрос о содержании и границах компетентности педагогов, специалистов по работе с подростками и семьей. Что они должны знать, какой опыт иметь в этой области, чтобы противостоять «информационным» угрозам, научить и помочь справиться с возникающими проблемами подросткам и их родителям.

В России базовым законодательным проектом в области регуляции вопросов информационной безопасности детей стал Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Данный закон определил два основных вида информации, причиняющей вред здоровью и (или) развитию детей: запрещенной для распространения среди детей и информации, распространение которой среди детей определенных возрастных категорий ограничено [14]. В Законе также рассматриваются требования к обороту информационной продукции, предназначенной для детей, и градации её в зависимости от возраста. Для введения в оборот информационной продукции данный закон обязывает проводить экспертизу информационной продукции. Проведение экспертизы требует подготовки соответствующих специалистов-экспертов в этой области.

Закон определяет государственный надзор и общественный контроль за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, а также ответственность за его нарушения, предусмотренные положениями Кодекса

Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ (КоАП РФ) (с изменениями и дополнениями).

Принятые в недавнем прошлом новые документы в области информационных технологий и информационной безопасности, такие как Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [13] и Стратегия развития информационного общества на 2017 – 2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. N 203) [11], только декларируют основные направления развития информационного общества и вопросы кибербезопасности в России, но не дают конкретных разъяснений алгоритмов осуществления информационной безопасности личности, общества и государства. Правовому (юридическому) сообществу придется повернуться лицом к новым информационным технологиям, чтобы держать руку на пульсе регулирования правовых норм в этой области.

Другой очень важный юридический вопрос, связанный с обеспечением информационной безопасности подростков - защита персональных данных [5]. Педагоги, по роду деятельности, постоянно имеют дело с персональными данными. Цифровизация, в том числе воспитательного и образовательного процесса, приводит к появлению различных информационных ресурсов, содержащих персональные данные, личную информацию обучающихся. Однако уровень компетентности специалистов, работающих с обучающимися, в области обращения с персональными данными, часто оставляет желать лучшего. Специальное обучение в этой области для педагогов отсутствует. С одной стороны, цифровые технологии упрощают возможности анализа и обобщения информации, помогают в управлении и планировании, с этим трудно поспорить. Но тогда нужно учить рядового пользователя (в нашем случае педагога) вопросам защиты информации, в первую очередь, персональных данных обучающихся. Вместе с тем тенденция к расширению подобных информационных ресурсов предъявляет новые требования к

повышению компетентности всех специалистов и руководителей системы образования в области защиты информации.

Для развития данных положений в РФ 27.07.2006 принят Федеральный закон № 152-ФЗ «О персональных данных», который вступил в силу с 1 января 2008 г. Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в т.ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайны [5].

Статья 3 данного закона определяет: «Персональные данные – любая информация, относящаяся к определенному или неопределенному на основании такой информации лицу (субъекту персональных данных), в т.ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация» [5].

Вопрос обеспечения правового поля защиты персональных данных в образовательной организации в настоящее время особенно актуален, так как, во-первых, такие данные должны храниться в электронном виде, а во-вторых, оператор, обрабатывающий такие данные, в соответствии с ч. 1 ст. 19 закона № 152-ФЗ должен предпринимать все необходимые организационно-технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, от иных неправомерных действий. Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 утверждено Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [5].

На основании положений ст. 1 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных», законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не

входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Основные нормативные правовые акты в сфере персональных данных:

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных».

3. Федеральный закон от 21.07.2014 г. №242 «..«о запрете хранения ПДн россиян заграницей» (вступил в силу 01.09.2015г).

4. Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Постановление Правительства РФ от 15.09.2008 г. №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Постановление Правительства РФ от 21.03.2012 г №211. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

7. Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям

законодательства Российской Федерации в области персональных данных (Приказ Роскомнадзора от 11.11.2011 №312).

8. Приказ Роскомнадзора от 19.08.2011г. №706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

9. Приказ Минкомсвязи от 28.08.2015 №315 «О внесении изменений в Административный регламент Роскомнадзора…» «…О месте нахождения базы данных информации, содержащей персональные данные».

10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК РФ от 15.02.2008).

11. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (Приказ ФСТЭК РФ от 14.02.2008 г.).

12. Приказ Федеральной службы по техническому и экспортному контролю 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.

13. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17 «Требования о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах».

14. Методический документ**.** Меры защиты информации в государственных информационных системах. (Утверждено ФСТЭК России 11.02.2014г.).

15. Банк данных угроз безопасности информации. (Утверждено ФСТЭК России 06.03.2015 №240/22/879).

16. Приказ Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их

обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (Приказ ФСБ РФ от 10.07.2014 г. №378).

Нормативные правовые акты, регламентирующие размещение персональных данных на сайте образовательной организации [56]:

- ФЗ от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- ПП от 10.07.2013 №582 «Об утверждении Правил размещения на официальном сайте образовательной организации в сети «Интернет» и обновления информации об образовательной организации»;

- Приказ Минобрнауки от 29.05.2014 №785 «Об утверждении требований к структуре официального сайта образовательной организации в сети «Интернет» и формату представления на нем информации»;

- Письмо Рособрнадзора от 25.03.2015 №07-675 с «Методическими рекомендациями представления информации об образовательной организации в открытых источниках с учетом соблюдения требований законодательства в сфере образования»;

- Приказ Роскомнадзора от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- Методические рекомендации Роскомнадзора от 14.12.2012 «Разъяснение вопросов, касающиеся обработки персональных данных работников, соискателей и лиц, находящихся в кадровом резерве».

Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Оценивая законодательную базу, следует обратить внимание, что к объектам информационной безопасности в Минобрнауки России,

региональных министерствах (департаментах) образования, муниципальных органах управления образованием и в образовательных организациях относят:

- сведения, составляющие государственную тайну, в соответствии с выписками из перечня сведений, подлежащих засекречиванию в министерствах, ведомствах и организациях;
- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в т.ч. и персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

Содержание компетенций в области информационной безопасности далеко не исчерпывается перечисленными выше и постоянно расширяется, так же быстро, как и влияние Интернета и информационных технологий на нашу жизнь.

Несмотря на признание проблемы информационной безопасности российскими общественными и правовыми институтами, данный вопрос требует тщательной проработки и развития во всех описанных выше направлениях: организационно-правовом, техническом и социально-психолого-педагогическом уровнях.

Одним из пусковых механизмов формирования комплексной системы информационной безопасности может быть создание обучающих программ в этой области для педагогов и сотрудников, работающих с детьми и их родителями.

Такие шаги предпринимаются, например, на сайте www.единыйурок.рф, который предлагает повысить квалификацию по программам: 1) «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях

обучения и воспитания обучающихся в образовательной организации»; 2) «Основы обеспечения информационной безопасности детей»; 3)«Организация защиты детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях» [32].

Особое внимание хочется уделить третьему направлению повышения квалификации (компетентности) педагогов, которая касается непосредственно их сферы деятельности: это психолого-педагогические методы обеспечения информационной безопасности.

В России существует потребность в создании программ и проектов, связанных с образованием в области психологической безопасности в работе с информационными технологиями для трех категорий: детей, родителей и лиц, которые занимаются с детьми профессионально: руководителей образования, педагогов, психологов.

Таким образом, можно сделать вывод, что информационная безопасность является одним из составных элементов комплексной безопасности образовательной организации. Также следует отметить, что поскольку вопросы информационной безопасности с внедрением информационных технологий в повседневную жизнь стали достаточно актуальными, необходимо на уровне государственной политики и на уровне всех институтов социализации уделять внимание вопросам обучения педагогов и сотрудников в области информационной безопасности. Меры противостояния информационным угрозам лежат в разных плоскостях: юридическая область, организационно-техническое и психолого-педагогическое направление.

Для достижения этого необходимы специальные обучающие программы и педагоги, обладающие знаниями в области информационной безопасности.

1.3 Сущность и содержание системы подготовки в области информационной безопасности сотрудников образовательной организации

Глубокое понимание проблематики информационной безопасности может быть достигнуто образовательной деятельностью по нескольким взаимодополняющим направлениям:

– получением базового образования в области информационной безопасности в рамках существующих специальностей;

– получением второго высшего образования (объем вновь изучаемого материала по проблематике информационной безопасности - несколько тысяч часов);

– прохождением профессиональной переподготовки или получением дополнительной квалификации (объем вновь изучаемого дополнительного материала - в рамках тысячи часов и более);

– формированием специализации по информационной безопасности в рамках специальности высшего образования (объем вновь изучаемого материала также составляет несколько сот часов, но не дополнительно, а взамен);

– внедрением во все специальности, не относящиеся к группе специальностей «Информационная безопасность» отдельной одноименной дисциплины;

– совершенствованием информационной подготовки специалистов в области информационной безопасности за счет введения в соответствующие Федеральные государственные образовательные стандарты высшего образования дидактических единиц, объективно отражающих значимость и научный уровень решения этой проблемы, создания и укрепления внутри дисциплинарных связей дисциплин информационного цикла и междисциплинарных связей с дисциплинами других разделов в рамках единой методической системы, обеспечивающей формирование профессиональных умений в области информационной безопасности.

По мнению ряда ученых и педагогов (Е.Б. Белова, Ю.С. Васильева, П.Д. Зегжды, Е.Б. Маховенко) подготовка специалистов в области информационной безопасности связана с целым рядом проблем [21].

Прежде всего, качество обучения во многом определяется глубиной соответствующих научных исследований в предметной области. Исследования в области информационной безопасности до недавних пор проводились только в закрытых и военных вузах, а информация о достижениях в развитии этой научной области и педагогический опыт не имели широкого распространения. Да и в настоящее время динамизм развития сферы информационной безопасности несопоставим с темпами подготовки соответствующих специалистов, т.е. система обучения в области информационной безопасности обладает существенной инертностью.

Некоторые исследователи считают, что подготовка в области информационной безопасности и защиты информации должна быть детерминирована по всем уровням образования: среднего, высшего, послевузовского, дополнительного и ориентирована на различные направления и профили подготовки [16].

Характеристики существующей системы подготовки в области информационной безопасности и защиты информации.

В самом общем плане категории специалистов, которым необходима подготовка по информационной безопасности в системе профессионального образования, могут быть сведены в несколько основных групп:

– специалисты в области информационной безопасности и защиты информации: аналитики по компьютерной безопасности, разработчики средств и систем безопасности, сотрудники организаций и подразделений, занимающихся информационной безопасностью и защитой информации, в том числе в системах критических приложений (опасных производств);

– специалисты в области информационных технологий (ИТ-специалисты), обеспечивающие создание и эксплуатацию информационных систем, а также отвечающие за их администрирование и безопасность;

– специалисты, обеспечивающие эксплуатацию сложных иерархических человеко-машинных систем управления специального назначения (эргатических систем);

– все остальные специалисты, имеющие доступ к информационным системам, использующие информационные и коммуникационные технологии как в профессиональной деятельности, так и в интересах самосовершенствования и развития [27].

При этом каждая из групп может быть дифференцирована в зависимости от условий социального заказа на подготовку специалистов определенного профиля.

Для подготовки первой из перечисленных категорий специалистов, чья профессиональная деятельность напрямую связана с обеспечением информационной безопасности и защиты информации, основополагающим является наличие соответствующих Федеральных государственных образовательных стандартов (ФГОС) и разработанных на их базе основных профессиональных образовательных программ в области информационной безопасности по специальностям, выделенным в группу 10.00.00 в перечне направлений и специальностей (табл. 2).

Таблица 2 – Перечень специальностей среднего профессионального образования в области информационной безопасности

Коды укрупненных групп специальностей. Коды специальностей	Наименования укрупненных групп специальностей. Наименования специальностей	Квалификация(и) специалиста среднего звена
10.00.00	**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**	
10.02.01	Организация и технология защиты информации	Техник по защите информации Старший техник по защите информации
10.02.02	Информационная безопасность телекоммуникационных систем	Техник по защите информации Старший техник по защите информации
10.02.03	Информационная безопасность автоматизированных систем	Техник по защите информации Старший техник по защите информации

Продолжение таблицы 2

10.02.04	Обеспечение информационной безопасности телекоммуникационных систем	Техник по защите информации
10.02.05	Обеспечение информационной безопасности автоматизированных систем	Техник по защите информации

Подготовка таких специалистов предусматривает изучение общепрофессиональных и специальных дисциплин, охватывающих широкий круг вопросов по обеспечению информационной безопасности и защиты информации.

В таблице 3 представлена дифференциация подготовки по информационной безопасности специалистов в системе среднего профессионального образования.

Таблица 3 – Дифференциация подготовки по информационной безопасности специалистов в системе среднего профессионального образования

№ п/п	Категории выпускников СПО	Качественная характеристика потребности
1.	Специалисты в области информационной безопасности и защиты информации: аналитики по компьютерной безопасности, разработчики средств и систем безопасности, сотрудники органов, организаций и подразделений, занимающихся информационной безопасностью и защитой информации, в том числе в системах критических приложений.	Незначительная
2.	Специалисты, обеспечивающие эксплуатацию сложных иерархических человеко-машинных систем управления специального назначения (эргатических систем).	Незначительная
3.	Специалисты в области информационных технологий (ИТ-специалисты), обеспечивающие создание и эксплуатацию информационных систем, в том числе отвечающие за их администрирование и безопасность.	Существенная
4.	Специалисты, имеющие доступ к информационным системам, использующие информационные и коммуникационные технологии как в профессиональной деятельности, так и в интересах самосовершенствования и развития.	Наиболее значимая

Для подготовки первой категории специалистов, чья профессиональная деятельность напрямую связана с обеспечением информационной безопасности и защиты информации, создана система, основы которой были заложены Решением Межведомственной комиссии Совета безопасности Российской Федерации по информационной безопасности от 28.09.95 г. №8.3, приказом Госкомвуза России от 22.12.95 г. №1687, решением Комитета по образованию и науке Государственной Думы Российской Федерации «О состоянии и перспективах подготовки кадров в области информационной безопасности» от 24.10.96 г. в 90-х годах века минувшего.

Система подготовки специалистов в области информационной безопасности и защиты информации, сформированная на базе Учебно-методического объединения (УМО) вузов России по образованию в области информационной безопасности в системе высшей школы носит узкопрофессиональный, специализированный характер, и отличается закрытостью. Для целого ряда других министерств и ведомств (в первую очередь силовых) сформированы ведомственные подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Министерстве образования и науки Российской Федерации.

Следует отметить, что в системе Федеральной службы безопасности (ФСБ) России, Министерства обороны, Федеральной службы охраны (ФСО), Министерства внутренних дел (МВД), Федеральной службы по техническому и экспортному контролю (ФСТЭК – ранее Гостехкомиссия при Президенте РФ), Министерство путей сообщения (МПС), других министерств и ведомств России сформировались ведомственные подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Министерстве образования и науки России. В рамках данных министерств и ведомств имеются образовательные учреждения различного вида, реализующие образовательные программы среднего, высшего, дополнительного и послевузовского профессионального образования в области информационной безопасности. Подобные подсистемы направлены

на целевую подготовку кадров в интересах ведомств и по своей организации, содержанию и развитию имеют определенную специфику.

В целях координации работы по подготовке кадров в области информационной безопасности работают Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности (см. Указ Президента Российской Федерации от 29 декабря 2012 г. №1711 «О составе по должностям»), Межведомственная комиссия по защите государственной тайны (см. Указ Президента Российской Федерации от 6 октября 2004 г. №1286), Координационный совет Минобразования России по проблемам подготовки специалистов в области защиты государственной тайны и информационной безопасности.

Подготовка кадров в области информационной безопасности имеет существенные особенности, поскольку выступает не только как реакция на спрос рынка в отношении таких специалистов, но и как важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере. Этими особенностями определяются и содержание подготовки указанных специалистов, и особые требования, предъявляемые к образовательным учреждениям при организации такой подготовки [30].

Специалисты с такой подготовкой в настоящее время полноценно могут готовиться только вне сферы гуманитарного, педагогического, экономического образования, однако уже сегодня нуждается в научной проработке вопрос о введении в существующие экономические специальности специализации по безопасности информационных систем в экономике, направленной на подготовку специалистов с экономическим образованием и высоким уровнем подготовки в области информационной безопасности, ориентированных по предназначению на работу в службах финансового мониторинга, аналитического обеспечения экономической безопасности, решение задач форестики (финансовой разведки).

Для целого ряда других министерств и ведомств сформированы ведомственные подсистемы подготовки кадров, по своей структуре

аналогичные общей системе подготовки специалистов в Министерстве образования и науки РФ. Эти подсистемы направлены на целевую подготовку кадров в интересах ведомств и по своей организации, содержанию и развитию имеют определенную специфику. Взаимодействие подсистем осуществляется в рамках Координационного совета министерства по проблемам подготовки кадров в области защиты государственной тайны и информационной безопасности, созданного приказом министра образования РФ от 25.02.2003 г. [27].

Вопросы информационной безопасности с той или иной степенью полноты и детализации нашли отражение в учебных планах и программах подготовки специалистов прикладной информатики (по областям) и других категорий ИТ-специалистов. Помимо изучения проблематики информационной безопасности и защиты информации в рамках дисциплин информационного цикла их знания в этой области развиваются и систематизируются в рамках общепрофессиональных и специальных дисциплин соответствующей направленности.

Для самой широкой категории специалистов, являющихся конечными пользователями современных ИКТ весь спектр вопросов по информационной безопасности в настоящее время сконцентрирован в курсе информатики и информационных технологий в профессиональной деятельности, что существенно сужает рассмотрение проблемы и нуждается в корректировке.

Как отмечается в [20; 21; 27; 30] важнейшей задачей является усиление подготовки специалистов по информационной безопасности гуманитарного профиля.

Особую остроту приобретает гуманистическая составляющая проблемы ИБ, предполагающая наличие адекватного гражданского воспитания и основанная в т.ч. на информационном праве, высокой информационной культуре.

Для создания системы подготовки по информационной безопасности последняя должна быть определена как педагогическая категория. Под

категорией в философии, например, понимается наиболее общее и существенное понятие, выражающее одну из основных форм или одно из основных отношений бытия (материя, время, пространство и т.п.); категории общепсихологические представляют собой предельно широкие психологические понятия (сознание, личность, деятельность и т.п.); в педагогике это должны быть понятия, отображающие существенные ее стороны как науки о сущности развития и формирования человеческой личности. В этом ключе педагогическая категория «подготовка по информационной безопасности» может трактоваться как обязательный компонент информационной подготовки, обеспечивающий секьюритологический аспект информационной культуры, характеризующий состояние защищенности инфосферы индивидуума в процессе информационного взаимодействия от различного рода информационных опасностей и угроз, а также регламентирующий работу индивидуума с информационными ресурсами с соблюдением морально-этических и правовых норм.

Для решения задачи обучения основам информационной безопасности и защиты информации как инвариантной составляющей информационной подготовки, направленной на формирование информационной культуры личности на этапе перехода к постиндустриальному обществу, требуется системный подход, реализующий методологические, организационные, содержательные, дидактические и технологические аспекты.

Одним из основополагающих принципов такого подхода является преемственность между уровнями образования. Система подготовки в области информационной безопасности и защиты информации должна быть детерминирована по всем уровням образовательной деятельности как общего (пропедевтика, т.е. вводный курс, а также базовый и профильный курсы информатики), так и профессионального образования – среднего, высшего, послевузовского и дополнительного.

В процессе информационной подготовки на этапе общего образования закладываются основы компьютерной грамотности и компьютерной компетентности как фундамент информационной культуры личности. В стандарте основного общего образования по информатике и информационным технологиям отмечается, что «изучение информатики и информационных технологий в основной школе должно быть направлено на воспитание ответственного отношения к информации с учетом правовых и этических аспектов ее распространения; избирательного отношения к полученной информации». А в обязательный минимум основных образовательных программ включены дидактические единицы, рассматривающие информационные процессы в обществе («информационные ресурсы общества, образовательные информационные ресурсы; личная информация, информационная безопасность, информационные этика и право»). В требованиях к уровню подготовки выпускников школы учтены их умения по применению мер антивирусной безопасности, использованию приобретенных знаний и умений на практике.

Актуальными остаются задачи повышения правовой грамотности в вопросах использования средств информационных и коммуникационных технологий, применения типовых методов защиты информации при работе на персональном компьютере, в локальных и глобальных сетях. Поэтому подготовка в области информационной безопасности и защиты информации нуждается в существенном совершенствовании и развитии на последующих этапах образования.

Модель системы подготовки будущих специалистов гуманитарного профиля средствами информационных технологий раскрывает теоретическую сущность целостного образовательного процесса, построенного на идее формирования информационной культуры и информационной безопасности.

Система подготовки должна характеризоваться комплексностью, непрерывностью, технологичностью (см. рис. 1). Содержание обучения основам информационной безопасности и защиты информации может быть

построено на основе системного анализа основных объектов предметной области будущей профессиональной деятельности. Результатом такого анализа должно стать выявление базовых объектов изучения, их взаимосвязей (процессов взаимодействия), методов и технологии их изучения. При проектировании системы подготовки специалистов гуманитарного профиля средствами информационных технологий с учетом информационной безопасности должны быть использованы основополагающие принципы архитектоники – научность; преемственность; последовательность; систематичность; доступность; связь теории с практикой; адаптивность и динамичность; полифункциональность [30].

Рисунок 1 – Модель системы обучения основам информационной безопасности

Целями обучения в такой системе является подготовка к профессиональной деятельности в соответствии с требованиями ФГОС, а также формирование высокого уровня информационной культуры и подготовки в области информационной безопасности.

Проблематика информационной безопасности должна стать органической частью информационной подготовки специалистов гуманитарного профиля, необходимым компонентом формирования информационной культуры личности в условиях постиндустриального общества.

И если вопрос формирования профессиональной компетентности в области обеспечения информационной безопасности для студентов педагогических специальностей должен быть реализован в процессе обучения, то для работающих педагогов и сотрудников образовательной организации вопрос формирования профессиональной компетентности в области обеспечения информационной безопасности может быть решен путем организации соответствующих курсов повышения квалификации.

Учитывая вышеизложенное, сформулируем противоречие между существующим содержанием подготовки будущих педагогов в рамках федеральных государственных образовательных стандартов, недостаточно учитывающим современные угрозы информационного характера, и необходимостью подготовки компетентных выпускников системы педагогического образования, имеющих профессиональные компетенции в области информационной безопасности.

Детализация содержания информационно-педагогической деятельности будущего педагога в условиях современного информационного общества требует от выпускников *знаний* о формах и методах информационного воздействия и информационного подавления; *способности* ориентироваться в потоках разнообразной информации, умений выявлять возможные угрозы, связанные с отбором, оценкой и защитой информации, запрещенной для распространения среди детей; *готовности* использовать эффективный

комплекс мер информационной безопасности с учетом правовых основ, разработанных программно-технических средств защиты информации и экономической целесообразности; *владения* знаниями и методами защиты от криминальной и террористической информации в многообразном информационном потоке; *владения* приемами обеспечения информационной безопасности образовательного учреждения и отдельного индивида.

Компетентность педагогов в области организационно-технической защиты информации должна касаться таких вопросов как:

1) условия обработки информации ограниченного доступа (персональные данные, медицинская информация и другая);

2) элементарные знания в области защиты информации в компьютере;

3) обеспечение безопасности информации при работе с интернетом;

4) осведомленность о программах «родительский контроль» и их функциях;

5) элементарные знания о возможностях «пожаловаться» или заблокировать нежелательный контент в социальных сетях, правилах безопасности в социальных сетях.

Особенностью формирования компетентности в области информационной безопасности является и то, что наряду с изучением организационных и технических средств защиты информации, необходимо прививать нравственную составляющую и ответственность за использование информации, которая, потенциально, может причинить ущерб от неумелого с ней обращения не только личности обучающегося, но и остальным субъектам образовательного процесса, а также, что немаловажно, репутации образовательного учреждения [29].

Таким образом, процесс формирования компетентности сотрудников образовательной организации в области информационной безопасности в учебном процессе должен носить комплексный характер и учитывать, как существующие стандарты образования, так и требования, и реалии современного информационного общества массовой коммуникации. При этом

необходимо учесть все существенные угрозы и возможные негативные последствия информатизации.

Выводы по главе I

Во первой главе магистерской диссертации описана необходимость совершенствования профессиональной компетентности педагога образовательной организации, в частности:

1) определено понятие «компетентность», «компетенция», «профессиональная компетентность»;

2) проанализирован профессиональный стандарт «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования (утвержден Приказом Минтруда России от 08.09.2015 № 608н)»;

3) выделены компетенции в области информационной безопасности сотрудника образовательной организации.

Особенностью формирования компетентности в области информационной безопасности является и то, что наряду с изучением организационных и технических средств защиты информации, необходимо прививать нравственную составляющую и ответственность за использование информации, которая, потенциально, может причинить ущерб от неумелого с ней обращения не только личности обучающегося, но и остальным субъектам образовательного процесса, а также, что немаловажно, репутации образовательной организации.

В связи с чем, совершенствования профессиональной подготовки в области информационной безопасности сотрудников образовательной организации, определяет успешность обозначенной потенциальной педагогической деятельности и эффективность педагогического образования. Поскольку требования к обеспечению информационной безопасности постоянно обновляются, педагогам необходимо повышать свою квалификацию в этом направлении.

ГЛАВА 2 ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ КУРСА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ» НА БАЗЕ ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

3.1 Описание базы исследования

ГБПОУ «Южно-Уральский государственный колледж» - крупнейшее учебное заведение среднего профессионального образования в г. Челябинске. В Южно-Уральском государственном техническом колледже сегодня учится более 4000 студентов.

Директор колледжа Тубер Игорь Иосифович – заслуженный учитель РФ, кандидат педагогических наук, почетный строитель России. В колледже 300 преподавателей, среди которых кандидаты педагогических наук, заслуженные учителя РФ, почетные работники среднего профессионального образования, лауреаты Всероссийских конкурсов и премий, лауреаты премии губернатора, лауреаты премии Законодательного собрания Челябинской области в сфере образования, преподаватели высшей и первой квалификационных категорий. Студенты ЮУрГТК учатся по 19 образовательным программам базового и повышенного уровней среднего профессионального образования на бюджетной основе и коммерческой основе [56].

В основу успехов колледжа на современном этапе заложена сертифицированная в соответствии со стандартом ГОСТ Р ИСО 9001-2001 система менеджмента качества. Она стимулирует педагогический коллектив к постоянному совершенствованию, внедрению инновационных технологий, нацеливает на успех. Высокий уровень подготовки специалистов в колледже подтверждается победами на олимпиадах, конкурсах и выставках регионального и российского значения.

Сегодня в своей деятельности Южно-Уральский государственный технический колледж опирается на современные образовательные технологии

– их внедрению уделяется большое внимание, а также на требования работодателей – заказчиков кадров квалифицированных специалистов.

Информатизация колледжа вышла на новый уровень, когда появилась компьютерная сеть, информационный портал, единое информационное пространство, электронная библиотека, система библиотечного обслуживания Ирбис, система электронного обучения Moodle, новые лицензионные программные продукты.

Благодаря рациональной политике использования лицензионного и свободного программного обеспечения, доступности компьютеров для студентов, как в учебное, так и в не урочное время, возможности работать в сети Интернет и сети электронной библиотеки федерального уровня с доступом к полнотекстовому содержимому, можно считать, что информационно-коммуникационная база колледжа отвечает современным требованиям.

Подготовка специалистов осуществляется на базовом уровне. Максимальный объём учебной нагрузки (включая все виды аудиторной и внеаудиторной учебной работы) и объём обязательных учебных занятий соответствует установленным нормативам.

Современные тенденции информатизации образования предполагают активное создание и использование электронных образовательных ресурсов (далее - ЭОР) в образовательных организациях.

Согласно ГОСТ Р 53620 - 2009 «Информационно-коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения» [56] электронный образовательный ресурс - это образовательный ресурс, представленный в электронной цифровой форме и включающий в себя структуру, предметное содержание и метаданные о них.

На сегодняшний день имеется большой выбор электронных образовательных ресурсов, позволяющих повысить эффективность образовательного процесса.

С использованием электронных образовательных ресурсов (ЭОР) возникают проблемы закупки современной техники, структурирования информации, защиты авторского права, защиты от несанкционированного доступа (НСД), а также проблема подготовки кадров [33], способных использовать электронные образовательные ресурсы как полноценное дидактическое средство. Традиционный подход к обеспечению безопасности ЭОР в образовательных организациях сводится к тому, чтобы обеспечить целостность и доступность ЭОР на каком-либо общем информационном портале в составе информационно-образовательной среды (далее – ИОС). В ЮУрГТК большая часть ЭОР сконцентрирована в системе дистанционного обучения – Moodle.

В компьютерных классах колледжа осуществляется обучение студентов работе с прикладными программными продуктами, системами автоматизации и проектирования, разрешен доступ к электронному библиотечному каталогу, а также внешним образовательным базам данных. В часы самоподготовки к занятиям, а также во время самостоятельной работы можно воспользоваться перечисленными сервисами для лучшего понимания пройденного материала и выполнения домашних заданий.

Программное обеспечение, используемое в колледже: Windows 7, Linux, AdobePhotoshop CC, MicrosoftVisualStudio 2015, MS SQL, MicrosoftVisio 2007, BPWin 4/1, ERWin 7.0, Opera, AdobeDreamweaver CS3, MicrosoftOffice 2016, AdobeFlash CC, CorelDraw, 3D Studio MAX, 1C 8.0, MathCAD, Компас [56].

Применение электронных образовательных ресурсов в образовательном процессе, актуальных в условиях реализации информационной безопасности с развитием технического прогресса, все существующие средства и методы неизбежно будут устаревать прежде, чем осуществится их внедрение в жизнедеятельность образовательных организаций. Это выдвигает на повестку дня осознание важности опережающего противодействия угрозам информационных атак на учебные заведения. Решить же проблему можно только в случае поддержки современных образовательных систем

необходимыми финансовыми, нормативными, научно-методическими средствами и компетентными кадрами, способными обеспечить защиту этих систем от вредоносных технических, негативных интеллектуальных и разрушающих духовно-нравственных воздействий [56].

В «ЮУрГТК» на момент проведения нашего исследования имелись следующие локальные правовые акты, так или иначе затрагивающие аспекты информационной безопасности: «Положение об официальном сайте ГБПОУ «ЮУрГТК», «Положение об обработке и защите персональных данных в ГБПОУ «ЮУрГТК», «Политика в отношении обработки персональных данных в ГБПОУ «ЮУрГТК», «Положение об организации работы по охране труда, обеспечению безопасности образовательного процесса в ГБПОУ «ЮУрГТК»,«Правила пользования библиотекой». Все документы размещены на сайте колледжа - http://sustec.ru [56].

Нормативной составляющей в колледже на электронные образовательные ресурсы существуют правила работы персонала и обучающихся колледжа в компьютерных сетях и правила работы с ресурсами сети Интернет, входящие в Концепцию информационной безопасности колледжа, которые соответствуют требованиям обеспечения безопасности.

Проанализировав структуру колледжа, выявили подразделение, отвечающее за информационную безопасность в данном колледже. Таким подразделением является Информатизационный центр.

Информатизационный центр (ИЦ) – структурное подразделение, отвечающее за состояние единой информационной среды колледжа. В его сферу деятельности входят:

– все рабочие станции в сети;

– все сервисы доступны с любого компьютера в соответствии с политикой безопасности;

– корпоративная сеть на основе оптоволокна;

– 7 современных физических серверов;

– 28 виртуальных серверов;

– два канала доступа к сети Интернет;

– собственный web-хостинг;

– лицензионное программное обеспечение;

– организация ИТ-службы по международному стандарту ITIL;

– собственное вычислительное облако [56].

Согласно положению информатизационного центра главной целью деятельности ИЦ является организация и предоставление доступа к электронным сетевым сервисам для повышения эффективности работы подразделений колледжа.

В своей деятельности данный центр руководствуется: Конституцией РФ; Законом Российской Федерации от 29 декабря 2012 г. № 273-1 «Об образовании в Российской Федерации»; Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»; Уставом колледжа; документацией внутриколледжной системы менеджмента качества; документацией внутриколледжной системы менеджмента охраны труда и техники безопасности; законодательными и нормативными актами по охране труда, пожарной безопасности и обеспечения защиты персональных данных.

Информатизационный центр осуществляет свою деятельность как структурное подразделение колледжа. Структура ИЦ состоит из лабораторий, специализирующихся по направлениям: лаборатория технического обеспечения; лаборатория информационных технологий.

Руководство лабораторией осуществляет заведующий лабораторией, который подчиняется непосредственно руководителю ИЦ. Руководство ИЦ осуществляет руководитель ИЦ, который подчиняется непосредственно заместителю директора по информационным технологиям.

Руководитель ИЦ и заведующие лабораториями, назначаются на должность и освобождаются от нее приказом директора колледжа. Структуру и штатную численность ИЦ утверждает директор колледжа. Сотрудники ИЦ являются штатными сотрудниками колледжа.

Сотрудники:

- Руководитель центра.

Монтажный комплекс:

- Заведующий ЛТО.

- Администратор сети.

- Инженер АСУ.

- Инженер ИЦ.

- Техники ИЦ Техник ИЦ (2-ой корпус).

Машиностроительный комплекс:

- Инженер ИЦ.

- Оператор ЭВМ ИЦ.

Политехнический комплекс:

- Инженер ИЦ.

- Техник ИЦ [56].

Информатизационный центр решает следующие задачи:

1. Разработка и осуществление единой технической политики и практического использования современных достижений информационных технологий в бизнес-процессах колледжа.

2. Выполнение работ по созданию и развитию единой информационной сети колледжа.

3. Выполнение работ, ориентированных на создание новых информационных технологий в целях информационного обеспечения учебного процесса и управления в колледже.

За обеспечение информационной безопасности в колледже отвечает лаборатория информационных технологий.

В ее функции входит: создание, обслуживание и развитие защищенного центрального серверного центра колледжа; проектирование и развитие компьютерной сети с использованием современных достижений в данной области; установка, настройка и сопровождение сетевых программных продуктов; создание надежных условий для доступа всех пользователей к компьютерной сети колледжа; предоставление сетевых сервисов в целях

обеспечения учебных и управленческих работ; организация централизованной антивирусной защиты информационных ресурсов; предоставление сетевых ресурсов для автоматизации управленческой деятельности подразделений; проектирование, разработка, размещение и поддержка внешних и внутренних Web-серверов; подбор, адаптация, разработка нового и внедрение программного обеспечения с целью создания, и развития автоматизированной системы управления колледжем; адаптация и внедрение программного обеспечения для организации процесса дистанционного образования и независимой проверки знаний; организация работ по обеспечению защиты информационных систем персональных данных.

Администратор сети в данном центре несет ответственность по обеспечению информационной безопасности и защиты от вирусов, а также безопасности информационных систем персональных данных [56].

Таким образом, можно сделать вывод, что информатизационный центр является подразделением службы информационной безопасности в ГБПОУ «Южно-Уральский государственный технический колледж» и обеспечивает в колледже комплексную защиту информации.

3.2 Разработка курса повышения квалификации «Информационная безопасность и защита персональных данных»

Для формирования компетентности в области информационной безопасности и изучения проблематики информационной безопасности для сотрудников колледжа был разработан и внедрен курс повышения квалификации «Информационная безопасность и защита персональных данных».

Целевая аудитория: руководители, педагогические работники, психологи и социальные работники колледжа.

Основная *цель изучения курса* обучение сотрудников образовательной организации принципам и средствам обеспечения информационной

безопасности личности, конкретных образовательных объектов и учреждений, общества и государства.

В курсе объясняется важность освоения системных комплексных методов защиты персональной информации от различных видов объективных и субъективных угроз в процессе ее обработки, использования и хранения в образовательной и профессиональной деятельности.

Задачи изучения курса «Информационная безопасность и защита персональных данных»:

– овладение теоретическими знаниями в области информационной безопасности;

– формирование умений выбора методов для защиты персональной информации;

– получение практического опыта деятельности по вопросам обеспечения информационной безопасности личности, семьи, дома, образовательного учреждения.

Курс повышения квалификации знакомит с современной концепцией информационной безопасности, организационно-правовыми аспектами безопасности информации, задачами защиты персональной учебной информации и информационными ресурсами, а также основными тенденциями и направлениями формирования и функционирования систем защиты информации.

Курс включает в себя лекции в компьютерной учебной аудитории с видеопроектором и с электронным учебно-методическим материалом по шести основным темам, таким как:

1. Информационная безопасность как составляющая национальной безопасности.

2. Правовые основы информационной безопасности и защита интеллектуальной собственности.

3. Виды и особенности угроз информации.

4. Программные средства защиты персональной информации.

5. Технические средства защиты и комплексное обеспечение безопасности.

6. Безопасность в сети Интернет.

7. Работа в системе электронного обучения Moodle.

В результате освоения курса слушатель будет:

знать:

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

– основные нормативные правовые акты в области информационной безопасности и защиты информации;

– правовые основы организации защиты персональной информации, коммерческой, служебной и профессиональной тайны;

– принципы и методы противодействия негативному информационному воздействию на личность ребенка и манипуляции его сознанием;

– методы фильтрации контента и родительского контроля в интернете;

уметь:

– анализировать и оценивать угрозы информационной воздействия на личность подростка;

– использовать и соблюдать федеральное законодательство в области обеспечения информационной безопасности и защиты персональных данных;

– формулировать и проектировать политику информационной безопасности образовательных организаций, знать и осуществлять организационные меры по защите персональных данных;

– анализировать и оценивать угрозы и факторы рисков негативного воздействия на личность в интернете и локальных вычислительных сетях;

– разрабатывать и соблюдать основные требования информационной безопасности, в том числе политики информационной безопасности образовательной организации;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;

владеть:

– навыками работы с нормативными правовыми актами в области обеспечения информационной безопасности;

– методами и средствами выявления угроз негативного воздействия информации на личность;

– навыками защиты авторских прав и прав на интеллектуальную собственность;

– навыками организации и обеспечения режима защиты персональных данных;

– навыками безопасного использования технических и программных средств защиты информации в учебно-воспитательном процессе образовательной организации.

Сфера применения слушателями полученных профессиональных компетенций, умений и знаний: учебная, воспитательная, административная и управленческая деятельность.

Учебная нагрузка разработанного курса – 72 академических часа.

Тематический план и содержание курса представлен в таблице 4.

Таблица 4 - Тематический план и содержание курса

Наименование разделов и тем	**Содержание учебного материала, практические занятия, самостоятельная работа слушателей**		**Объем часов**
1	**2**		**3**
Тема 1. Основные понятия информационной безопасности	Содержание учебного материала		*4*
	1	Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. Понятие «национальная безопасность». Доктрина безопасности Российской Федерации	4

Продолжение таблицы 4

	2	Понятия информации. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Перечень сведений, доступ к которым не может быть ограничен. Понятие конфиденциальной информации, ее виды.	2
	3	Концепция информационной безопасности. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры по защите информации.	2
	Выполнение учебного проекта «Принципы комплексного подхода к обеспечению информационной безопасности»		*2*
	Самостоятельная работа. Ответы на вопросы		*2*
Тема 2. Правовые основы информационной безопасности и защита интеллектуальной собственности	Содержание учебного материала		*20*
	1	Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание.	
	2	История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность.	
	3	Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права. Произведения, пользующиеся охраной. Правовые нормы и стандарты по лицензированию и сертификации	
	Лекция в компьютерной учебной аудитории с видеопроектором и с учебно-методическим материалом в электронном виде		*2*
	Практические работы: 1. Правовые аспекты деятельности в глобальной сети Интернет 2. Безопасность и конфиденциальность в Интернете		*4*
	Выполнение учебного проекта		*8*
	Самостоятельная работа. Выполнение заданий		*4*

Продолжение таблицы 4

Тема 3. Виды информационных угроз	Содержание учебного материала		*14*
	1	Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак. Информационные войны. Информационное оружие. Анализ и оценивание угроз информационной безопасности личности в современном информационном обществе	
	2	Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступа.	
	3	Угрозы информационно-психологической безопасности личности и их основные источники. Сущность и современное состояние манипуляции сознанием и поведением людей. Информационная среда иллюзии и реальности	

Итоговый контроль по курсу осуществляется в форме защиты индивидуального проекта.

Тематика индивидуальных заданий включает следующие темы.

1. Информация, относящаяся к государственной тайне.

2. Понятие персональных данных.

3. Информация, составляющая коммерческую тайну.

4. Объекты информационной безопасности.

5. Случайные и целенаправленные угрозы нарушения сохранности информации.

6. Понятие «противоправный контент».

7. Риски информационной безопасности обучающихся.

8. Понятие информационного оружия. Информационные войны

9. Критерии безопасности.

10. Аудит информационной безопасности.

11. История хакерства. Хакерство в России.

12. Правовые механизмы защиты информации на разных уровнях.

13.Задачи и способ функционирования межсетевого экрана.

14. Политика безопасности администратора сети и брандмауэра.

15. Инфобезопасная среда в образовательной организации.

Требования к проекту представлены в таблице 5.

Таблица 5 – Требования к проекту

Количественная оценка проекта							
Выполненные работы							
Оцениваемые составляющие проекта	Электронный текст	Электронные таблицы	Презентация, Буклет	Сетевые технологии	Содержание	Дизайн проекта	Итого
Баллы	1	2	3	4	5	5	20
Название проекта							
Автор							

Требования к электронному тексту:

1. Текст состоит из трех частей, объеденных одной темой (10-20 страниц): текст, набранный с клавиатуры; текст, найденный в Интернете; сканированный текст.

2. Параметры страницы: Верхнее поле - 2, Нижнее поле - 2, Левое - 3, Правое - 1.

3. Параметры абзаца: Первая строка - 1,25, Интервал - 1,5; Выравнивание по ширине.

4. Параметры шрифта: Обычный, Times New Roman; размер 14

5. Текст должен содержать заголовки.

6. Текст содержит: 5-7 рисунков с различным расположением в тексте; формулы; таблицу; список.

7. Автоматически создано оглавление, расставлены номера страниц вверху по центру, оформлен титульный лист.

8. Создан список используемой литературы, оформленный по правилам с указанием адресов сайтов; на каждый источник в тексте должна иметься ссылка, оформленная в виде числа в квадратных скобках, соответствующему номеру в списке.

9. Текст может содержать сноски и колонтитулы.

Требования к презентациям:

1. Презентация содержит 8-15 слайдов.
2. Использованы различные виды разметки слайдов.
3. Текст на слайдах должен содержать не больше 250 символов, размер шрифта не менее 26 пунктов, сплошной текст выровнен по ширине. Текст на слайдах не должен содержать орфографических и синтаксических ошибок.
4. Слайды содержат рисунки, подходящие по смыслу теме презентации и тексту слайда.
5. На слайдах расположены управляющие кнопки.
6. К объектам на слайдах применены эффекты анимации.
7. На отдельном слайде создан список используемой литературы, оформленный по правилам с указанием адресов сайтов.

В результате успешного освоения курса «Информационная безопасность и защита персональных данных» слушатели должны иметь высокий уровень компетентности в области информационной безопасности, а, следовательно,

Знать:

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

– основные нормативные правовые акты в области информационной безопасности и защиты информации;

– правовые основы организации защиты государственной тайны, персональной информации;

– принципы и методы организационной защиты информации;

– принципы и методы противодействия несанкционированному информационному воздействию на личность и системы передачи информации;

– методы фильтрации контента и родительского контроля в Интернете.

Уметь:

– анализировать и оценивать угрозы информационной безопасности личности;

– использовать нормативные документы по защите информации;

– формулировать и проектировать политику информационной безопасности образовательной организации;

– анализировать и оценивать степень риска проявления факторов опасности личности и информации в Интернете и локальных вычислительных сетях;

– соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Владеть:

– работы с нормативными правовыми актами в области обеспечения информационной безопасности;

– методами и средствами выявления угроз личности и информации;

– навыками защиты прав на интеллектуальную собственность;

– навыками организации и обеспечения режима защиты персональных данных;

– навыками выявления и уничтожения компьютерных вирусов;

– навыками безопасного использования технических и программных средств защиты информации в профессиональной деятельности.

3.3 Опытно-экспериментальная работа по формированию компетентности в области информационной безопасности у педагогов ГБПОУ «Южно-Уральский государственный колледж»

Курсы повышения квалификации педагогов — это неотъемлемая важная часть всего образовательного процесса. Курсы повышения должны

преследовать цель повышения профессионального мастерства, как самого педагога, так и всего коллектива образовательной организации. Как показывает практика, разрозненное прохождение курсов не позволяет достичь положительного эффекта в пополнении багажа знаний в усовершенствовании педагогической деятельности [3, с. 302].

Система повышения квалификации должна создавать условия для самореализации педагога, развития его ключевых компетенций, возрастающих требований в качественном образовании.

В 2021 году по рассматриваемой программе обучения прошли курсы повышения квалификации 20 сотрудников колледжа.

Эффективность разработанного курса повышения квалификации проявляется в комплексе характеристик, показателей и критериев для оценки уровня сформированности компетентности сотрудников в области информационной безопасности.

Важным компонентом формирования компетентности в области информационной безопасности сотрудников является разработка интегральной системы оценивания (оценочного инструментария) с целью объективного представления результатов деятельности слушателей в терминах компетенций с учетом показателей их интегральной квалиметрической оценки, как количественной, так и качественной.

В настоящем исследовании под сформированностью компетентности в области информационной безопасности будем понимать единство овладения следующими компонентами сотрудников в рамках курсов повышения квалификации:

– высокая степень освоения понятийного аппарата, владение знанием содержания компетентности (*когнитивный компонент*);

– практическое применение знаний к конкретным ситуациям, готовность к проявлению компетентности, высокая степень результативности при обеспечении информационной безопасности, выбор приоритетных направлений решения проблемы с точки зрения педагогической

целесообразности, функционирование понятийного аппарата в режиме активного, осознанного и творческого применения (*мотивационно-деятельностный компонент*).

Компонентный состав данного качества представлен на рисунке 2. Такое рассмотрение компетентности педагогов в области информационной безопасности позволило дифференцировать критерии сформированности выше обозначенных компетенций и обеспечить надежность диагностики.

Использование данных компонентов в качестве критериев сформированности компетентности сотрудников в области информационной безопасности способствует практической реализации компетентностного подхода.

При проектировании критериально-оценочного аппарата в настоящем исследовании будем исходить из постулата компетентностного подхода, утверждающего, что компетентность, как интегральная характеристика личности, формируется в образовательном процессе через определенный набор компетенций.

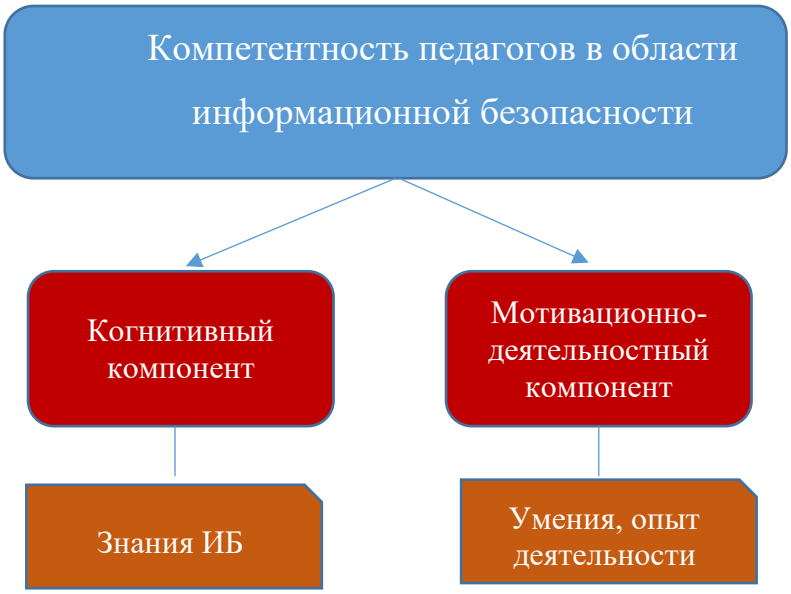


Рисунок 2 – Компонентный состав компетентности педагогов в области информационной безопасности

В данном исследовании адаптированы и применены следующие оценочные средства для анализа сформированности у сотрудников компетентности в области информационной безопасности:

1) личностные опросники как наборы стандартизованных анкет с вопросами открытого и закрытого типов;

2) тестирование;

3) ситуационный метод - анализ проблемных ситуаций на основе фактов из реальной жизни;

4) компетентностно-ориентированные задания;

5) беседы, обсуждения и дискуссии;

6) междисциплинарные комплексные контрольные вопросы и задания;

7) индивидуальные проекты;

8) практические задания;

9) интерактивные лекции, лекции-визуализации и др.

Теоретический анализ компетентностного подхода показал, что в процессе выполнения одного вида деятельности могут проявляться различные виды компетенций. На основании этого можно утверждать, что каждый вид деятельности, учебной или профессиональной, требует интегральной оценки. Вычисление коэффициента уровня сформированности компетентности должно основываться на показателях результативности различной учебной деятельности слушателей. студентов. В свою очередь, результативность оценивается через критерии, которые являются признаком сформированности компетенций (см. табл. 6).

Таблица 6 – Структура интегральной оценки подготовки сотрудников к обеспечению информационной безопасности

Критерий	Характеристика	Задача
Когнитивный	знания, умения, владение опытом применения аппаратно-программных средств защиты в решении задач формирования инфобезопасной среды образовательной организации, а также базовые профессиональные знания, определяемые ФГОС, обеспечивающие возможностью свободно ориентироваться в информационном пространстве и использовать возможности средств ИКТ при решении прикладных задач.	формирование у сотрудников колледжа знаний по информационной безопасности
Мотивационно-деятельностный	готовность, интерес, стремление, потребность действовать в целях защиты информации, выполнение профессиональных задач с учетом правовых основ, разработанных аппаратно-программных средств защиты информации и экономической целесообразности для организации инфобезопасной среды образовательной организации, установка на совершенствование профессионального опыта.	формирование у сотрудников колледжа устойчивой мотивации к решению задач обеспечения информационной безопасности

Проблема критериев для определения уровней сформированности рассматриваемых компетенций сотрудников является актуальной для проведения педагогического эксперимента и анализа его результатов.

Необходимо отметить, что критерии определения уровней сформированности компетентности в области информационной безопасности должны соотноситься с конечной целью обучения и отображать характеристики, на развитие которых в первую очередь направлено обучение. Критерии для оценки уровня сформированности компетентности состоят из следующих показателей:

– знание сотрудниками колледжа правовых норм и законов Российской Федерации об информационной безопасности, защите

персональных данных, об авторском праве и смежных правах, недопустимость навязывания информации обучающемуся;

– умение проектировать психологически безопасную и комфортную инфобезопасную образовательную среду, проводить профилактику различных форм зависимостей, насилия и агрессии в студенческом коллективе и в едином информационном образовательном пространстве;

– опыт деятельности по подготовке сознания обучающихся к противодействию негативным информационным воздействиям, формирование навыков критического мышления, развитие способностей к самоблокированию противоправной информации;

– навыки защиты профессионально значимой информации и противостояния угрозам информационной безопасности в профессиональной деятельности.

Оценочно-результативный компонент курса повышения квалификации непосредственно связан с выделением и раскрытием уровня сформированности компетентности в области информационной безопасности сотрудников колледжа. Уровневый подход позволяет рассматривать любой процесс развития личности как переход от одного уровня к другому, более сложному и качественно отличному.

Нами на основе способов оценки компетенций Н.Ф. Ефремовой [36] выделены следующие уровни сформированности компетентности в области информационной безопасности: начальный, базовый и углубленный.

Теоретический анализ, детальная разработка критериев и показателей (уровней) сформированности компетентности в области информационной безопасности позволили установить их взаимозависимость, что представлено в таблице 7.

Таблица 7 – Критерии и уровневые показатели сформированности компетентности в области информационной безопасности

Высокий уровень	Средний уровень	Низкий уровень
1	2	4
Когнитивный компонент		
Критерий: 2) когнитивная готовность к профессиональной деятельности в области ИБ. **Показатели:** знания, умения, владение опытом применения аппаратно-программных средств защиты, об источниках угроз, о методах оценки и защиты информации, а также базовые профессиональные знания, обеспечивающие будущего специалиста возможностью свободно ориентироваться в информационном пространстве и использовать возможности средств ИКТ при решении прикладных задач.		
Уровневые показатели		
Имеются, неполные, отрывочные, без системного знания по информационной безопасности, частично знаком с методами защиты информации, не соотносит полученные знания с будущей профессиональной деятельностью	обладает знаниями и умениями, необходимыми и достаточными для применения эффективных алгоритмических методов и моделей при решении типовых задач защиты информации	способен ориентироваться в информационных потоках, может выявлять возможные угрозы, связанные с отбором, оценкой и защитой информации, действия целенаправленны и результативны
Мотивационно-деятельностный компонент		
Критерий: 3) операционально-техническая и технологическая готовность к профессиональной деятельности в области информационной безопасности. **Показатели:** профессиональные умения (умение применять методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ; умение применять стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; умение применять на практике программно-аппаратные средства ОИБ).		
Уровневые показатели		
понимает актуальность постановки проблемы информационной безопасности и ее практического решения, неосознанность выполняемых действий, шаблонный характер деятельности, отсутствует вариативность используемых средств и методов	деятельность носит полушаблонный характер, целенаправленность действий неустойчива, не способен моделировать ситуации, решать нестандартные ситуации, давать обоснованную оценку уровню и качеству собственной деятельности	действия имеют творческий и инновационный характером, осознает значимость деятельности, умеет адекватно и самостоятельно корректировать пробелы и недочеты, сознательно стремится к самосовершенствованию в области информационной безопасности

Следующая задача критериально-оценочного аппарата – перевод выделенных критериев и показателей в количественные эквиваленты, которые позволят использовать математический аппарат для статистического анализа

получаемой педагогической информации о сформированности компетентности в области информационной безопасности. Для осуществления данной операции необходимо эмпирические индикаторы (показатели) каждого критерия преобразовать в количественные эквиваленты с помощью числовых систем по заранее обусловленным оценкам, т.е. разработать специальную шкалу оценки выделенного комплекса критериев и показателей эффективности формирования компетентности в области информационной безопасности.

Оценка (параметр) степени овладения компетенциями в области информационной безопасности Y представляет собой безразмерную величину, равную отношению числа рейтинговых баллов студента R к максимально возможному числу баллов R_{max}:

$$Y = \frac{R}{R_{max}} \qquad (1)$$

При определении значения степени овладения компетенциями необходимо исходить из положений экспериментальной педагогики о том, что если значение коэффициента менее 0,7, то рассматриваемая деятельность не может считаться положительной и эффективной.

Согласно принятым критериям сформированности компетентности значения параметра Y были соотнесены со следующими уровнями:

низкий - $Y \leq 0.69$

средний - $0.70 \leq Y \leq 0.89$

высокий - $Y \geq 0.90$

Для оценки курса повышения квалификации для формирования знаний, умений, навыков и компетенций, а также накопления статистических данных, был использован метод анализа иерархий Саати [63], связанный с уровневой оценкой усвоения модулей содержательной линии ИБ. Основным оценочным критерием был принят коэффициент усвоения курса (К).

$$K = \frac{N}{M} \qquad (2)$$

где N - общее число баллов, набранных слушателями за выполнение заданий на определенном уровне усвоения; M - максимальное количество баллов, которое мог бы набрать слушатель за правильное выполнение заданий на данном уровне.

Для общей оценки выполнения всех заданий по изучаемому курсу вычисляется обобщенный коэффициент усвоения (Q) на основе экспертных оценок. При этом учитывается, что сложность оценочных средств на всех уровнях различна, в связи с чем вводится коэффициент значимости (весовой коэффициент) уровня.

$$Q = K_1 \cdot r_1 + K_2 \cdot r_2 + \cdots + K_i \cdot r_i + K_n \cdot r_n \quad (3)$$

где Q - обобщенный коэффициент усвоения, K_i - коэффициент усвоения на *i*-уровне, r_i - коэффициент сложности соответствующего уровня.

Предложенные оценочные средства, требующие воспроизведения знаний на всех трех уровнях сформированности компетентности, разрабатывались с учетом коэффициентов значимости, которые рассчитывались на основе предположения, что сложность (значимость) уровней подчиняется соотношению 2:3:5, а их значения: r_1=0,2; r_2=0,3; r_3=0,5 $\sum r_i$ =1.

Начальный уровень (r_1=0,2) - контроль с помощью опросника.

Базовый уровень (r_2=0,3) - выполнение практических работ и ответы на практико-ориентированные задания.

Углубленный уровень (r_3=0,5) - выполнение индивидуальных заданий по решению ситуационных задач, проверка с помощью итогового теста.

В результате формула (3) принимает следующий вид:

$$Q = K_1 \cdot 0{,}2 + K_2 \cdot 0{,}3 + K_3 \cdot 0{,}5 \quad (4)$$

Таким образом, коэффициент усвоения может быть использован для сравнения результатов обучения в различных группах слушателей. Он может быть также соотнесен с обычной пятибалльной шкалой балльно-рейтинговой системой оценки успеваемости (табл. 8).

Таблица 8 – Корреляция между коэффициентами усвоения и оценками

Обобщённый коэффициент усвоения	Оценка	
	пятибалльная	Балльно-рейтинговая
0,91≤Q≤1	5	91-100
0,75≤Q≤0,9	4	75-90
0,74≤Q≤0,6	3	60-74
Q≤0,6	2	≤60

Используя формулы 1-4, можно с помощью весовых коэффициентов учитывать влияние различных оценочных средств на процесс формирования компетенций информационной безопасности, а также на оценку уровней сформированности компетентности в области ИБ.

Разработанный критериально-оценочный аппарат позволяет вести автоматизированную обработку результатов для оценки уровня освоения каждой темы курса при формировании рассматриваемой компетентности.

В целях изучения отношения педагогов к проблеме информационной безопасности было проведено анкетирование (см. приложение 1), в котором приняли участие 33 респондента, среди которых были сотрудники колледжа (12%) и педагоги (88%).

По результатам анкетирования было выявлено, что 58% из числа опрошенных используют компьютер более 5 часов ежедневно, при этом более 40% от общего числа респондентов проводят в глобальной сети Интернет более трех часов каждый день. На вопрос «Оцениваете ли Вы степень угрозы от использования Интернета, как серьезную», лишь 27% ответили утвердительно.

На вопрос анкеты: «Имеет ли вы опыт защиты личной или профессионально значимой информации в компьютере?» ответы респондентов распределились: не имеют опыта – 47%, имеют небольшой опыт – 27%, имеют достаточный опыт – 25%, что свидетельствует о том, что большинство педагогов и студентов имеют или незначительный опыт, или вообще не имеют навыков защиты информации. Следующий вопрос анкеты вытекал из предыдущего: «Как вы оцениваете свой уровень подготовки в

области информационной безопасности и защиты информации». Ответы распределились следующим образом: нулевой – 1 чел. (4%), низкий – 16 чел. (50%), средний – 14 чел. (44%), высокий – 2 чел. (2%) (рисунок 3).

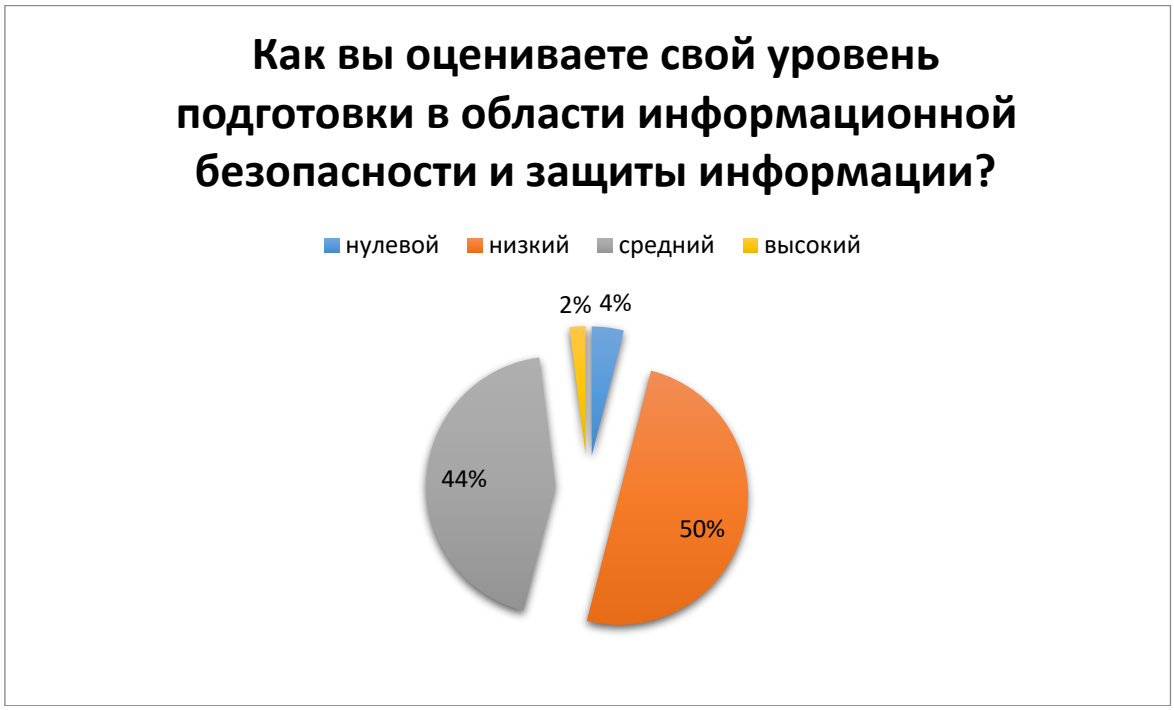


Рисунок 3 – Самооценка уровня подготовки респондентов в области информационной безопасности

На последний вопрос анкеты: «Ощущаете ли Вы потребность в повышении уровня умений в области информационной безопасности, а также в получении практического опыта противостояния информационным угрозам» большинство респондентов (79%) ответили положительно, что говорит о высокий мотивации сотрудников колледжа к саморазвитию в области информационной безопасности.

Формирование компетентности в области информационной безопасности было выстроено в соответствии с выделенными в её структуре компонентами и представляло собой разнообразные методы и приёмы, направленные на изучение теоретического материала для формирования когнитивного компонента; решение практико-ориентированных и индивидуальных заданий, групповые дискуссии, психологические тренинги, обеспечивающих развитие мотивационно-деятельностного компонента.

После изучения курса полученные результаты оформлялись в виде аналитических таблиц, гистограмм с целью получения сравнительных количественных данных, позволяющих проследить динамику качественных изменений, происшедших в результате целенаправленного воздействия по повышению квалификации сотрудников колледжа в области информационной безопасности, оценивалась эффективность влияния разработанного электронного учебно-методического обеспечения, были сформулированы общие выводы результатов исследования на основе анализа эмпирических материалов об оценки эффективности внедряемых средств, так же на данном этапе давалась оценка степени реализации положений гипотезы и теоретических основ формирования компетентности в области информационной безопасности у сотрудников образовательной организации.

Гистограмма (рис. 4) позволяет наглядно оценить, какие компоненты компетенций в области информационной безопасности развиты у сотрудников колледжа, после прохождения курса повышения квалификации достаточно хорошо, а какие требуют совершенствования.

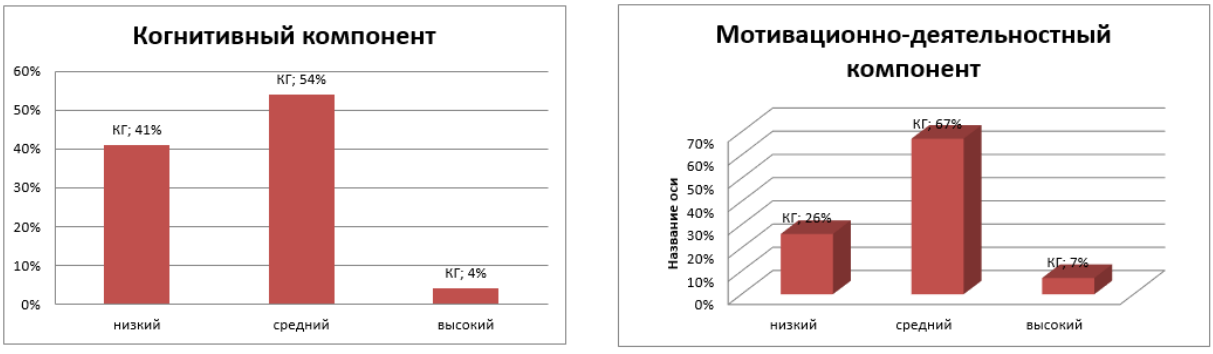


Рисунок 4

Цифры свидетельствуют о том, что у большего количества слушателей проявились компоненты высокого уровня компетенции в области ИБ (14%, 9% и 3% от общего числа слушателей), что позволяет зафиксировать положительную динамику перехода слушателей с низкого на высокий уровень профессиональной подготовки, оцениваемой по выделенным критериям, показателям и параметрам.

В целом анализ результатов исследования эксперимента показывает, что на фоне роста показателей сформированности всех двух компонентов компетенций в области ИБ по мотивационно-деятельностному компоненту динамика более высокая.

Опрос слушателей по окончанию занятий показал, что большинство респондентов на вопрос «Что должен делать колледж для обеспечения информационной безопасности?» определили основной задачей колледжа – формирование у обучающихся культуры информационной безопасности, информирование о полезных веб-сайтах, а также обучение безопасному использованию технологий и сервисов интернета (рис. 5).

По результатам итогового опроса и анкетирования был сделан вывод о том, что педагогические работники в полной мере осознают степень угроз информационного воздействия на обучающихся, владеют средствами и приемами решения проблем информационной безопасности, проектирования безопасной информационно-образовательной среды образовательной организации.

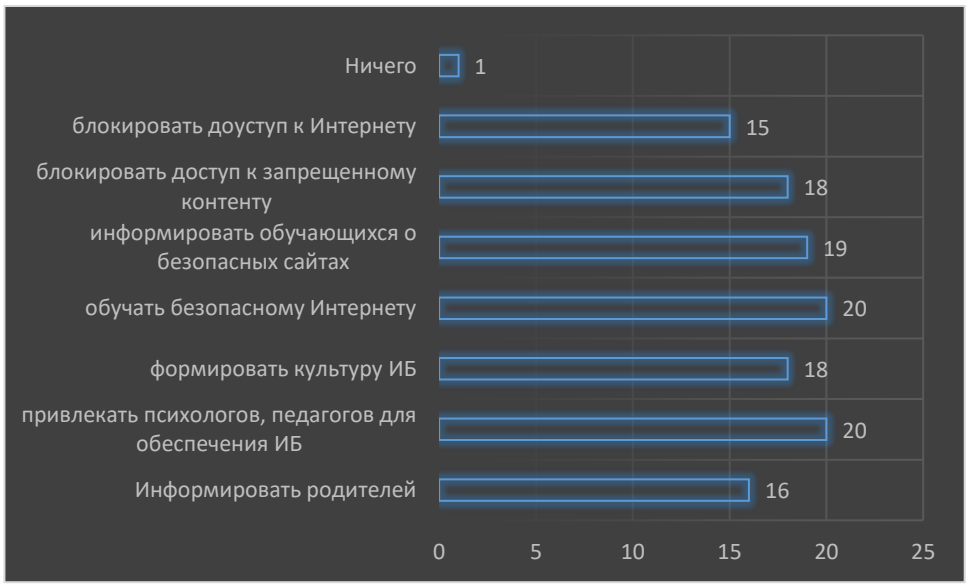


Рисунок 5 – Ответы слушателей на вопрос «Что должен делать колледж для обеспечения безопасной информационно-образовательной среды?»

В результате освоения курса сотрудники колледжа приобрели теоретические знания об основных существующих нормативно-правовых

актах в области информационной безопасности и защиты информации, методах фильтрации информационного контента и родительского контроля в глобальной сети интернет, принципах организационной защиты информационных потоков, а также мерах противодействия несанкционированному информационному воздействию на личность.

Практические навыки обучаемых после освоения курса включают в себя: владение методами и средствами выявления угроз личности и информации, выявление и уничтожение компьютерных вирусов, безопасное использование технических средств в профессиональной педагогической деятельности, проектирование политики информационной безопасности образовательного учреждения.

В связи со всем вышеизложенным, считаем, что курс повышения квалификации «Информационная безопасность образовательной организации» видится как разумное средство формирования у сотрудников колледжа компетентности в области информационной безопасности.

Таким образом, решение проблемы информационной безопасности образовательной организации видится нам в подготовке компетентных специалистов, повышении квалификации работающих педагогов и организации безопасной информационно-образовательной среды колледжа.

В то же время данный перечень мер и направлений не является исчерпывающим, так как современные вызовы и угрозы общества массовой коммуникации и глобализации не позволяют полностью решить проблему информационной безопасности образовательной организации, а только снизить ее последствия.

Выводы по третьей главе

В третьей главе диссертационного исследования были рассмотрены следующие вопросы:

1) Для углубленного изучения вопросов, связанных с обеспечением информационной безопасности в образовательной деятельности и для формирования компетентности в области информационной безопасности для сотрудников колледжа, был разработан и внедрен курс повышения квалификации «Информационная безопасность и защита персональных данных». Основная цель изучения курса обучение сотрудников колледжа принципам и средствам обеспечения информационной безопасности личности, конкретных образовательных объектов и учреждений, общества и государства.

2) В целях повышения эффективности и применения технологий электронного обучения был разработан электронный образовательный ресурс «Информационная безопасность и защита персональных данных».

3) Разработаны критерии и уровневые показатели сформированности компетентности в области информационной безопасности.

4) Результаты, полученные в ходе опытно-экспериментальной работы, направленной на проверку эффективности курса повышения квалификации педагогов, подтвердили предположение о том, что проведения курсов способствует формированию компетентности в области информационной безопасности педагогов и сотрудников колледжа, способствует формированию ценностного отношения к рассматриваемым проблемам, компетенций информационной безопасности в процессе профессионально–педагогической деятельности.

ЗАКЛЮЧЕНИЕ

Магистерское диссертационное исследование решает проблему разработки теоретических и методологических основ профессиональной подготовки сотрудников образовательной организации, обладающих профессиональными умениями в области информационной безопасности в условиях информатизации общества и образования. Результаты проведенного исследования позволили сделать следующие общие выводы:

1) Проанализированы профессиональные компетенции педагога профессионального образования.

Профессиональный стандарт – документ, включающий перечень профессиональных и личностных требований к работнику, действующий на всей территории Российской Федерации.

Для решения профессиональных задач специалист должен обладать соответствующими конкретным профессиональным задачам компетенциями, основными компонентами которых являются знания, умения, навыки и личностные качества специалиста. Совокупность же профессиональных компетенций, позволяющая выполнять весь перечень профессиональных задач в конкретной области, составляет компетентность специалиста в этой области.

Профессиональный стандарт педагогической деятельности включает 6 компетенций:

1. Компетентность в области личностных качеств.

2. Компетентность в постановке целей и задач педагогической деятельности.

3. Компетентность в мотивировании обучающихся (воспитанников) на осуществление учебной (воспитательной) деятельности.

4. Компетентность в разработке программы деятельности и принятии педагогических решений.

5. Компетентность в обеспечении информационной основы педагогической деятельности.

6. Компетентность в организации педагогической деятельности.

Таким образом, общим результатом обучения в системе образования является сформированная компетентность специалиста в определенной области, которая проявляется путем реализации соответствующих компетенций при решении профессиональных задач. Следовательно, при компетентностном подходе основное внимание в учебном процессе должно уделяться формированию у обучающихся профессиональных компетенций по всему спектру профессиональных задач, выполняемых специалистом в его профессиональной деятельности.

2) Раскрыты требования информационной безопасности для образовательной организации.

Информационная безопасность является одним из составных элементов комплексной безопасности образовательной организации. Также следует отметить, что поскольку вопросы информационной безопасности с внедрением информационных технологий в повседневную жизнь стали достаточно актуальными, необходимо на уровне государственной политики и на уровне всех институтов социализации уделять внимание вопросам обучения детей в области информационной безопасности. Меры противостояния информационным угрозам лежат в разных плоскостях: юридическая область, организационно-техническое и психолого-педагогическое направление.

3) Разработан курс повышения квалификации «Информационная безопасность и защита персональных данных».

Для формирования компетентности в области информационной безопасности и изучения проблематики информационной безопасности для сотрудников колледжа был разработан и внедрен курс повышения квалификации «Информационная безопасность и защита персональных данных».

Целевая аудитория: руководители, педагогические работники, психологи и социальные работники образовательных учреждений.

Основная *цель изучения курса* обучение сотрудников колледжа принципам и средствам обеспечения информационной безопасности личности, конкретных образовательных объектов и учреждений, общества и государства.

В курсе объясняется важность освоения системных комплексных методов защиты персональной информации от различных видов объективных и субъективных угроз в процессе ее обработки, использования и хранения в образовательной и профессиональной деятельности.

Задачи изучения курса «Информационная безопасность и защита персональных данных»:

– овладение теоретическими знаниями в области информационной безопасности;

– формирование умений выбора методов для защиты персональной информации;

– получение практического опыта деятельности по вопросам обеспечения информационной безопасности личности, семьи, дома, образовательного учреждения.

Курс повышения квалификации знакомит с современной концепцией информационной безопасности, организационно-правовыми аспектами безопасности информации, задачами защиты персональной учебной информации и информационными ресурсами, а также основными тенденциями и направлениями формирования и функционирования систем защиты информации.

4) Описана опытно-экспериментальная работа по формированию компетентности в области информационной безопасности у сотрудников образовательной организации, на примере ГБПОУ «ЮУрГТК».

Формирование компетентности в области информационной безопасности было выстроено в соответствии с выделенными в её структуре

компонентами и представляло собой разнообразные методы и приёмы, направленные на изучение теоретического материала для формирования когнитивного компонента; решение практико-ориентированных и индивидуальных заданий, групповые дискуссии, психологические тренинги, обеспечивающих развитие мотивационно-деятельностного компонента.

Результаты, полученные в ходе опытно-экспериментальной работы, направленной на проверку эффективности курса повышения квалификации сотрудников колледжа, подтвердили предположение о том, что проведения курсов способствует формированию компетентности в области информационной безопасности педагогов и сотрудников колледжа, способствует формированию ценностного отношения к рассматриваемым проблемам, компетенций информационной безопасности в процессе профессионально–педагогической деятельности.

Таким образом, задачи исследования решены, цель достигнута, гипотеза нашла свое подтверждение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно – правовые акты

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности. Основные термины и определения. – URL: http://www.opengost.ru/iso/35_gosty_iso/35020_gost_iso/11522-gost-r-53114-2008-zaschita-informacii.-obespechenie-informacionnoy-bezopasnosti.-osnovnye-terminy-i-opredeleniya.html (дата обращения: 16.12.2021).

4. Конституция Российской Федерации: офиц. текст. – М.: Право, 2002. – 39 с.

5. О персональных данных: ФЗ от 27 июля 2006 № 152 - ФЗ // Бюллетень нормативных актов министерств и ведомств. – № 7. – 2006. – С.15.

6. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149 - ФЗ // СЗ РФ. – 2006. – №31

7. Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации от 30.04.02. № 290: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. – 2002. – № 8. – С.102.

8. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 17 ноября 2007 г. № 781. – URL: https://base.garant.ru/192223/ (дата обращения: 21.12.2021).

9. Приказ Министерства образования и науки Челябинской области от 28.07.2016 г. № 01/2445 «О вводе в эксплуатацию автоматизированной системы «Образование Челябинской области»».

10. Профессиональный стандарт «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования» (утв. приказом Министерства труда и социальной защиты РФ от 8 сентября 2015 г. N 608н). – URL: http://anichkov.ru/official/gzrdo/profstadart_prof.pdf (дата обращения: 16.12.2021).

11. Стратегия развития информационного общества на 2017 – 2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. N 203) [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_216363/e91cc5f89aaced60e19c6c6554f c03432f4ee971// (дата обращения: 11.01.2022).

12. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 N 197-ФЗ (ред. от 25.05.2020). – URL: https://clck.ru/B8yGj (дата обращения: 14.12.2021).

13. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 05.01.2022).

14. Федеральный закон от 29.12.2010 №436-ФЗ (ред. от 18.12.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 11.01.2022).

15. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 30.12.2021) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2022). – URL: https://legalacts.ru/doc/273_FZ-ob-obrazovanii/ (дата обращения: 11.01.2022).

Литература

16. Алтуфьева, А.А. Методические основы обучения информационной безопасности на базе телекоммуникационных ресурсов сети Интернет.

автореф. дисс. … канд. пед. наук: 13.00.02. / Алтуфьева Александра Андреевна. - Санкт-Петербург, 2008. – 19 с.

17. Бабанский, Ю.К. Избранные педагогические труды / Ю.К. Бабанский. – М.: Педагогика, 1989. – 560 с.

18. Бабанский, Ю.К. Оптимизация педагогического процесса / Ю.К. Бабанский, М.М. Поташник. – Киев: Радянська школа, 1984. – 286 с.

19. Баданов, А.Г. Информационная безопасность образовательного учреждения. Использование компьютерных технологий и работа в сети Интернет. – URL: http://dostizenie.ucoz.ru/document/badanov-2010-old_variant.pdf (дата обращения: 08.01.2022).

20. Батурин, Ю.М. Структура и содержание магистерской программы «Информационное право и противодействие компьютерным угрозам» в МГУ им. МВ Ломоносова / Ю.М. Батурин, А.А. Морозов // Информационное право. – 2015. – №. 2. – С. 29-32.

21. Белов, Е.Б. Образование в области информационной безопасности: принципы совершенствования подготовки кадров / Е.Б. Белов, В.П. Лось // Информация и связь. - 2002. - №2. - С. 94-96.

22. Беспалько, В.П. Слагаемые педагогической технологии / В.П. Беспалько. - М.: Педагогика, 1989. - 192 с.

23. Беспалько, В.П. Теория создания и применения школьных технологий / В. П. Беспалько. – М., 2006. – 542 с.

24. Бешенков, С.А. Школьное образование: информатика и информационные технологии / С.А. Бешенков // Информатика и образование. – 2000. – №7. С 17 - 24.

25. Богатырева, Ю. И. Безопасный Интернет для школьников, родителей и учителей / Ю.И. Богатырева, А.Н. Привалов, Л.В. Пятницкая // Преподавание информационных технологий в Российской Федерации: материалы Одиннадцатой открытой Всероссийской конференции (17-17 мая 2013 г.). – Воронеж: Воронежский государственный университет, 2013. – 332 с. – С. 319-320.

26. Богатырева, Ю.И. Анализ проблем информационной безопасности личности обучающихся / Новые информационные технологии в образовании: материалы VI междунар. научно-практической конференции, Екатеринбург, 12-15 марта 2013 г. //ФГАОУ ВПО «Рос. гос. проф.-пед. ун-т», Екатеринбург, 2013. – 390 с. – с. 313-316.

27. Богатырева, Ю.И. Компетентность педагогов в области информационной безопасности: проблема и пути решения / Ю.И. Богатырева, А.Н. Привалов // Известия Российской академии образования – 2013, № 2 (26) – 148 с. - С. 96-106.

28. Богатырева, Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения / Ю.И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. Вып. 3. Ч. 2. Тула: изд-во ТулГУ, 2013. – 343 с. – С. 14-25.

29. Богатырева, Ю.И. Подходы к разработке методической системы формирования компетентности в области информационной безопасности учителей информатики / Ю.И. Богатырева, А.Н. Привалов // Информатика и образование. 2012. Выпуск 10. – С. 77- 80.

30. Богатырева, Ю.И. Формирование компетенций в области ИКТ в рамках ФГОС третьего поколения по направлению подготовки «Педагогическое образование» / Ю.И. Богатырева, Р.Р. Яфаева // Педагогическая информатика. 2010. – №3. – С. 56-65.

31. Будыкин, С.В. Информационная безопасность детей и подростков в понимании родителей и учителей (Часть 2. Результаты эмпирического исследования) / С.В. Будыкин, Н.В. Дворянчиков, И.Б. Бовина // Психология и право. 2016. Том 6. № 1. – С. 25–38.

32. Будыкин, С.В. Информационная безопасность детей и подростков в современном мире: психологические аспекты проблемы / С.В. Будыкин // Психология и право. – 2017. Том 7. № 1. – С. 13–24.

33. Введенский, В.Н. Моделирование профессиональной компетентности педагога / В.Н. Введенский // Педагогика. – 2003. – №10. – С. 51-55.

34. Викторова, Л.Г. О педагогических системах / Л.Г. Викторова. – Красноярск: Изд-во Красноярского университета, 1989. – 101 с.

35. Владимирова, Л.П. Сетевые профессиональные сообщества учителей / Л.П. Владимирова. – URL: http://distant.ioso.ru/for%20teacher/25-11-04/sps.htm. (дата обращения: 24.01.2022).

36. Выготский, Л.С. Методика рефлексологического и психологического исследования: Проблемы современной психологии / Л.С. Выготский. – Л.: ГИЗ, 1926. – С. 41–52.

37. Елистратова, Н.Н. Современные проблемы высшего образования. – URL: http://vestnik.rsu.edu.ru/pdf/2_(29).pdf (дата обращения: 18.01.2022).

38. Жук, О.Л. Компетентностный подход к педагогической подготовке студентов в классическом университете / О.Л. Жук // Качество высшего педагогического образования: проблемы и пути повышения: Материалы междунар. научн.-практ. конф. Минск, 15 апр. 2004 г. / Редкол.: Н. А. Березовин (отв. ред.) и др. – Минск: БГУ, 2004. – 371 с.

39. Загвязинский, В.И. Педагогическое творчество учителя / В.И. Загвязинский. – М: Педагогика, 1987. – 59 с.

40. Зеер, Э.Ф. Практика формирования компетенций: методологический аспект / Э.Ф. Зеер, Д.П. Заводчиков // Формирование компетенций в практике преподавания общих и специальных дисциплин в учреждениях среднего профессионального образования. – Екатеринбург, 2011. – С. 5-10.

41. Зефиров С. Л., Алексеев В. М. Способы оценки информационной безопасности организации //Труды Международного симпозиума «Надежность и качество». – 2011. – Т. 2.

42. Зимняя, И. А. Компетентность и проблемы ее формирования в системе непрерывного образования (школа – вуз – послевузовское образование) / науч. ред. проф. И.А. Зимняя: мат-лы XVI науч.-метод. конф.

Актуальные проблемы качества образования и пути их решения. – М.: Исследовательский центр проблем качества подготовки специалистов, 2006.

43. Зубаиров, А.Ф. Создание единой информационной среды для оказания муниципальных услуг в сфере образования в электронном виде / А.Ф. Зубаиров // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2017 №1(2). – С. 105-109.

44. Иванова, Н.Н., Филимонюк Л.А. Развитие профессиональных компетенций педагогов системы среднего профессионального образования в современном образовательном пространстве / Л.А. Филимонюк, Н.Н. Иванова // Мир науки, культуры, образования. – 2019. – № 1 (74) – С. 280-281.

45. Ильин, А.С. Анализ состояния защищенности персональных данных при их обработке в учреждениях системы образования Челябинской области в 2016 году / А.С. Ильин, Д.С. Ильина // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2017 №1(2). С. 89-94.

46. Ильин, А.С. Обеспечение безопасности информации в образовательной организации в современных условиях / А.С. Ильин, Д.С. Ильина // Научно-методическое обеспечение оценки качества образования – 2016 –№ 1/ – С. 48-51.

47. Коваленко, А.П. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) / А.П. Коваленко, Е.Б. Белов // Научные и методологические проблемы информационной безопасности/под ред. ВП Шерстюка. – М.: МЦНМО. – 2004.

48. Концепция информационной безопасности детей (утв. распоряжением Правительства Российской Федерации от 2 декабря 2015 года № 2471-р). – URL: http://www.consultant.ru/document/cons_doc_LAW_190009/ (дата обращения: 26.01.2022).

49. Кузьмина, Н.В. Методы системного педагогического исследования / Н.В. Кузьмина. – Л., 1980. – 141 с.

50. Лапчик, М.П. Методика преподавания информатики: Учеб. пособие для студентов вузов, обучающихся по специальности 030100 «Информатика» / М.П. Лапчик, И. Г. Семакин, Е. К. Хеннер; под общ. ред. М. П. Лапчика. – Москва: Academia, 2006. – 621 с.

51. Михалева, Г.В. Современная британская стратегия информационной безопасности детей и молодежи [Электронный ресурс] // Вестник ЧелГУ. 2013. №22 (313). – URL: https://cyberleninka.ru/article/n/sovremennaya-britanskaya-strategiya-informatsionnoybezopasnosti-detey-i-molodezhi (дата обращения: 12.01.2022).

52. О признании утратившим силу приказа Министерства труда и социальной защиты Российской Федерации от 8 сентября 2015 г. № 608н «Об утверждении профессионального стандарта «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования»: Приказ Министерства труда и социальной защиты Российской Федерации от 26.12.2019 № 832н. – URL: http://publication.pravo.gov.ru/Document/View/0001202006020037 (дата обращения: 20.12.2021).

53. Обеспечение информационной безопасности организации. – URL: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата обращения: 20.01.2022).

54. Окуловский, О.И. Компетенции и компетентностный подход в обучении / О.И. Окуловский // Молодой ученый. – 2012. – №12. – С. 499-500. – URL https://moluch.ru/archive/47/5841/ (дата обращения: 23.01.2022).

55. Осипова, С.И. Информатизация образования как объект педагогического анализа / С.И. Осипова, И.А. Баранова, В.А. Игнатова // Фундаментальные исследования. – 2011. – № 12-3. – С. 506-510. – URL: http://fundamental-research.ru/ru/article/view?id=29192 (дата обращения: 13.01.2022).

56. Официальный сайт ГБПОУ «Южно-Уральский государственный технический колледж». – URL: https://sustec.ru/ (дата обращения: 22.01.2022).

57. Пимонов, В.А. Основные проблемы обеспечения информационной безопасности субъектов образовательного процесса / В.А. Пимонов // Психология и право. 2011. № 4. – URL: http://psyjournals.ru/psyandlaw/2011/n4/49302.shtml (дата обращения: 26.01.2022).

58. Письмо Минпросвещения России от 07.06.2019 N 04-474 «О методических рекомендациях» (вместе с «Методическими рекомендациями 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») [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_328805/ (дата обращения: 26.01.2022).

59. Правительство России. Национальный проект «Образование». – URL: http://government.ru/rugovclassifier/833/events/ (дата обращения: 15.01.2022).

60. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. – М.: Генезис, 2017. – 224 с.

61. Привалов, А.Н. Основные угрозы информационной безопасности субъектов образовательного процесса / А.Н. Привалов, Ю.И. Богатырева // Известия ТулГУ. Гуманитарные науки. 2012. №3. – URL: https://cyberleninka.ru/article/n/osnovnye-ugrozy-informatsionnoy-bezopasnosti-subektov-obrazovatelnogo-protsessa (дата обращения: 12.01.2022).

62. Роберт, И.В. Информационные и коммуникационные технологии в образовании [Текст]: учеб.-метод. пособие для пед. вузов / И.В. Роберт,

С.В. Панюкова, А.А. Кузнецов, А.Ю. Кравцова ; под ред. И.В. Роберт; ИИО РАО. – М., 2006. – 374 с.

63. Саати, Т. Принятие решений - Метод анализа иерархий / Т. Саати. – М.: Радио и Связь, 1993. - 278 с.

64. Самерханова, Э.К. Основные направления и принципы развития информатизации образовательного учреждения / Э.К. Самерханов // Журнал «Наука и школа», 2010. – URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-i-printsipy-razvitiya-informatizatsii-obrazovatelnogo-uchrezhdeniya. (дата обращения: 13.01.2022).

65. Сериков, Г.Н. Образование: аспекты системного отражения / Г.Н. Сериков. – Курган: Зауралье, 1997. – 464 с.

66. Смурова, Н.Ф., Филимонюк Л.А. Проектирование индивидуального образовательного маршрута профессионального роста педагога / Н.Ф. Смурова, Л.А. Филимонюк // Мир науки, культуры, образования. – 2021. – № 2 (87). – С. 162-164.

67. Толковый словарь терминов понятийного аппарата информатизации образования / составители Роберт И.В., Лавина Т.А. – М.: ИИО РАО, 2009. – 96 с.

68. Филимонюк, Л.А. РАЗВИТИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ / Л.А. Филимонюк, Н.Н. Иванова // Проблемы современного педагогического образования. 2021. №71-3. – URL: https://cyberleninka.ru/article/n/razvitie-professionalnyh-kompetentsiy-pedagogicheskih-rabotnikov-srednego-professionalnogo-obrazovaniya (дата обращения: 09.01.2022).

69. Хуторской, А.В. Ключевые компетенции как компонент личностно-ориентированной парадигмы / А.В. Хуторской // Народное образование. - 2003. - № 2. - С. 58-64.

70. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Солдатова Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю. – М.: Фонд Развития Интернет. 2013. – 144 с.

71. Шадриков В.Д. Профессиональные компетенции педагогической деятельности / В.Д. Шадриков, И.В. Кузнецова. – URL: https://publications.hse.ru/mirror/pubs/share/folder/2yuzgtr57q/direct/133941571 (дата обращения: 25.01.2022).

72. Шерстюк, В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности / В.П. Шерстюк // Информационное общество. – 1999. – №. 5. – С. 3-5.

73. Шпагина, Е.М. Информационная безопасность в контексте защиты прав детей в Российской Федерации / Е.М. Шпагина // Психология и право. – 2016. Том 6. № 4. С. 86–94.

74. Шпагина, Е.М. Компетентность педагогов и психологов в области информационной безопасности детей / Е.М. Шпагина, Р.В. Чиркина // Психология и право. – 2019(9). № 3. С. 261-277.

75. Livingstone S., Cagiltay K., Ólafsson K. EU Kids Online II Dataset: A cross-national study of children's use of the Internet and its associated opportunities and risks / British Journal of Educational Technology. Vol 46. No 5, 2015. P. 988–992 doi:10.1111/bjet.12317.

76. Stallings W. et al. Computer security: principles and practice. – Upper Saddle River, NJ, USA: Pearson Education, 2012. – С. 978-990.

77. Thaw D. B. Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets: дис. – UC Berkeley, 2011.

ПРИЛОЖЕНИЯ

Приложение 1

Анкета для педагогов и сотрудников образовательной организации «Информационная безопасность личности»

Данная анкета является социологическим исследованием, проводимым с целью изучения проблем информационной безопасности личности. Нас интересует Ваше отношение к данной проблеме. Анкетирование проводится анонимно.

Инструкция к заполнению анкеты: Поставьте отметку рядом с выбранным Вами вариантом ответа или в графе «другое» напишите свой вариант.

Заранее благодарим Вас за участие в исследовании!

1. Ваш пол:

□ мужской

□ женский

2. Ваш возраст:

□ до 15

□ 15-20

□ 21-30

□ 31-40

□ 41-50

□ старше 51

3. Ваше образование:

□ неполное среднее

□ среднее

□ неполное высшее

□ высшее

4. Профиль полученного образования:

□ технический (специалист по информатике)

□ технический, но не связанный с информационными технологиями

□ гуманитарный

□ другой _____

5. Есть у Вас дети:

□ да

□ нет

6. Как часто Вы используете компьютер в течение дня?

□ более 15 часов

□ 10-14 часов

□ 5-9 часов

□ 2-4 часа

□ менее 1 часа

7. Сколько времени ежедневно Вы проводите в Интернете?

□ 15-30 минут

□ 30-60 минут

□ 60-120 минут

□ более 120 минут

8. Большую часть времени за компьютером, вы…

□ решаете профессиональные задачи

□ ищите какую-либо информацию

□ общаетесь в социальных сетях, чатах, форумах

□ читаете свежие новости

□ играете в компьютерные игры

□ другое _____

9. Считаете ли Вы, что личность в современном обществе подвергается информационным угрозам:

□ да

□ нет

□ затрудняюсь ответить

10. При выполнении какой учебной или профессиональной деятельности Вы наиболее подвержены различным информационным угрозам:

□

□

□

11. Считаете ли Вы, что личность школьника в современном информационном обществе следует защищать от информационных угроз (опасностей), если «да», то перечислите их:

□

□

□

12. Имеете ли Вы опыт защиты личной или профессионально значимой информации в компьютере?

□ не имею

□ имею достаточный опыт

□ небольшой опыт, но достаточный для _____

13. Знаете ли Вы признаки и методы профилактики Интернет-зависимости?

□ да

□ нет

□ затрудняюсь ответить

14. Свой уровень подготовки в области информационной безопасности и защиты информации Вы оцениваете, как

□ нулевой

□ низкий

□ средний

□ высокий

□ другой _____

15. Ощущаете ли Вы потребность в повышении уровня знаний и умений в области информационной безопасности, а также в получении практического опыта противостояния информационным угрозам:

- □ да
- □ нет
- □ другое _____

Приложение 2

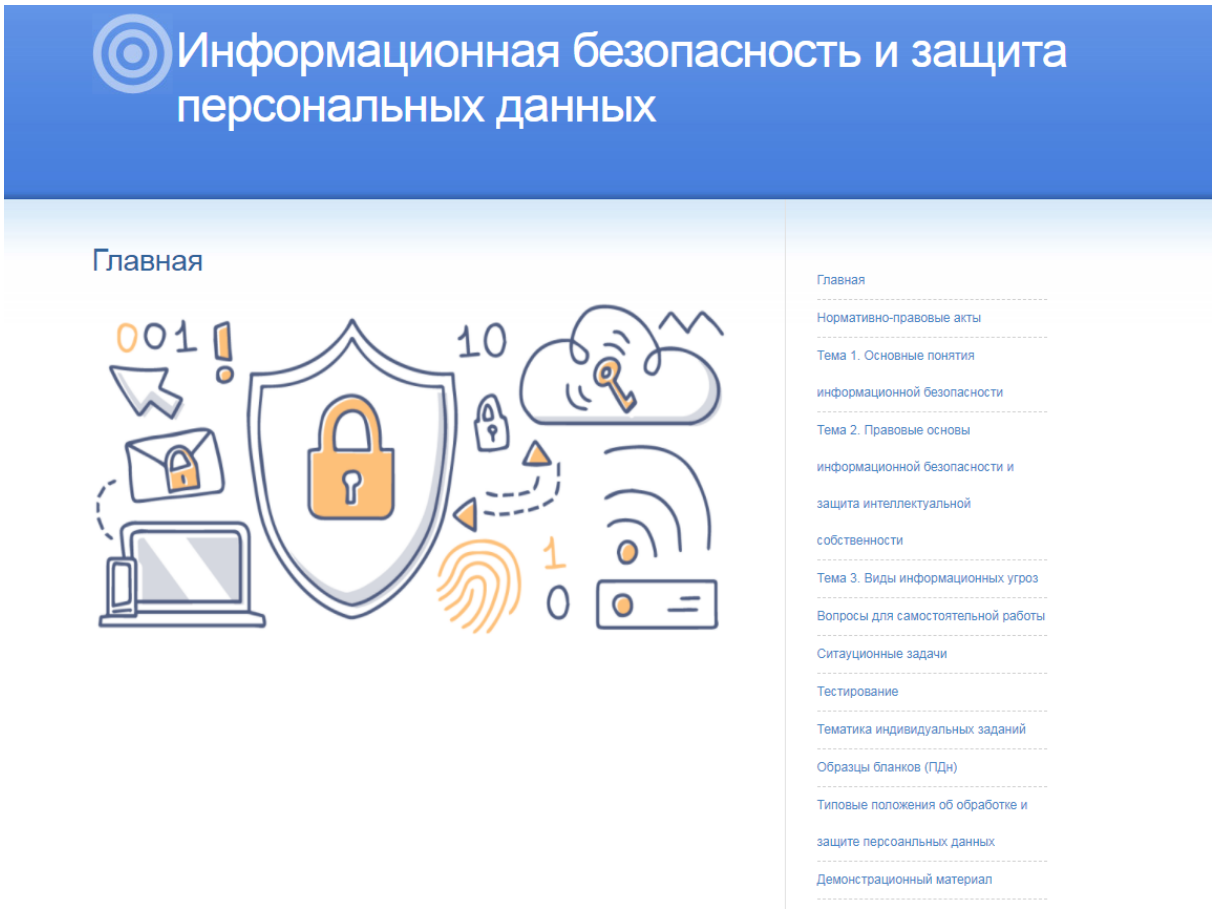
Для обучения сотрудников колледжа ГБПОУ «ЮУрГТК» по организации работы с персональными данными разработано электронное учебно-методическое обеспечение к курсу повышения квалификации «Информационная безопасность и защита персональных данных».

Структура электронного учебно-методического обеспечения: 6 разделов, которые расположены в блоке управления.

Блок управления располагается в левой части сайта и позволяет мгновенно перемещаться между разделами.

Электронное учебно-методическое обеспечение содержит: лекционный и практический материал к курсу, нормативные документы, положения по обсечению персональных данных работников, воспитанников и их законных представителей, методические рекомендации, демонстрационный материал и др.

Главная страница - страница приветствия представлена на рисунке 1.



Для организации обучения необходим компьютерный класс, оснащенный следующим образом (таб. 1, 2).

Таблица 1 - Перечень оборудования кабинета вычислительной техники

№	Устройство	Наименование	Количество, шт.
1	Системный блок	Intel® Core™ i3-7100 CPU @ 3/90GHz 3/90 GHz, ОЗУ не менее 8 Гб или аналоги, NVIDIA GeForce GT 720, CD/DVD-RW, HDD (Гб) 500	10-15
2	Монитор	23.8" Монитор LG 24MP59G-P	10-15
3	Клавиатура	Logitech K280e	10-15
4	Мышь	Мышь проводная A4Tech X-710BK черный	10-15
5	Принтер	HP LaserJet Pro M28w (W2G55A)	1
6	Проектор	Проектор Canon LV-X320	1
7	Демонстрационный экран	100" (254 см) Экран для проектора DEXP WM-100	1
8	Доска	-	1

Таблица 2 - Минимальное программное обеспечение кабинета вычислительной техники для изучения дисциплины «Информационные технологии»

№	Наименование
1	Операционная система Windows 7 и выше
2	Microsoft Office – профессиональный выпуск версии 2010 или 2016
3	Электронное учебно-методическое обеспечение «Информационная безопасность и защита персональных данных»

Программно-технические требования к электронному учебно-методическому обеспечению:

- Core i3 и выше;
- Оперативная память: не менее 8 Гb;
- Видеокарта: не менее 2 Гb;
- Операционная система: Windows7/8/10/;
- Манипулятор мышь;
- Наличие пакета MSOffice.