Е.А. Гафарова, Н.А. Василькова, Г.А. Диденко, О.Н. Шварцкоп

ПЕДАГОГИЧЕСКОЕ ВЗАИМОДЕЙСТВИЕ В СОВРЕМЕННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: КИБЕРБЕЗОПАСНОСТЬ ЛИЧНОСТИ

Учебное пособие

Челябинск, 2024

УДК 371:681.14 (021)
ББК 74.00: 32.973я73
Г 24
Гафарова Е.А., Диденко Г.А., Шварцкоп О.Н. Педагогическое взаимодействие в современной информационно-образовательной среде: кибербезопасность личности [Текст]: Учебное пособие / Е.А. Гафарова, Г.А. Диденко, О.Н. Шварцкоп – 152 с.

ISBN

Учебное пособие предназначено для бакалавров специальности 44.03.04 «Профессиональное обучение (по отраслям)» и магистров 44.04.04 «Профессиональное обучение (по отраслям)». Пособие может быть использовано в качестве дополнительного при изучении дисциплин профессионального цикла, таких как «Основы информационной безопасности», «Цифровое образование», «Информационные системы управления профессиональным образованием». В пособии содержится теоретический материал, посвященный особенностям педагогического взаимодействия в условиях цифровой образовательной среды, а также - вопросам кибербезопасности личности. После каждого раздела имеются практические задания для лучшего усвоения материала, представлены библиографические источники.

Рецензенты:

Белевитин Владимир Анатольевич, д.т.н., профессор кафедры автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам ФГБОУ ВО «ЮУрГГПУ»

Степанова Оксана Александровна, к.п.н., доцент, доцент кафедры математики, медицинской информатики, информатики и статистики, физики ФГБОУ ВО «ЮУГМУ»

СОДЕРЖАНИЕ

Введение

В настоящее время стремительное развитие и массовое распространение цифровых технологий создает необходимость их применения и контроля во всех сферах деятельности общества и государства.

Информатизация сферы образования осуществляется в приоритетном порядке. Федеральный проект «Цифровая образовательная среда» направлен на создание и внедрение в образовательных организациях цифровой образовательной среды, а также обеспечение реализации цифровой трансформации системы образования. В рамках проекта ведется работа по оснащению организаций современным оборудованием и развитию цифровых сервисов и контента для образовательной деятельности.

Реализация указанных требований невозможна без организации безопасной цифровой среды.

Проблема педагогического взаимодействия в рамках цифровой образовательной среды актуализируется из-за появляющихся новых свойств и функционала информационных технологий, ограничения непосредственного общения, вследствие трансформации дидактических закономерностей.

Настоящее учебное пособие содержит необходимый теоретический материал для понимания современных тенденций цифровизации образования, изучения аспектов информационной безопасности, реализуемых в информационно-коммуникационных технологиях и возможных путем решения проблемы кибербезопасности личности.

Раздел 1 Педагогическое взаимодействие в современной информационно-образовательной среде: ключевые понятия, закономерности функционирования, актуальные тренды

В настоящее время одной из главных целей государственной политики является становление цифрового общества, в связи с чем, говоря о современной информационно-образовательной среде, мы говорим о цифровой образовательной среде (далее – ЦОС).

Для реализации данной цели нормативно-правовая документация сферы образования регулярно претерпевает изменения: вносятся поправки в ранее действующие законы и стандарты, разрабатываются приоритетные проекты, вступают в силу стратегические целевые программы федерального и регионального уровней.

Основой нормативно-правовой базы, нацеленной на становление цифрового образования и общества в Российской Федерации, является Указ Президента РФ от 09.05.2017 №203 «О Стратегии развития информационного общества в РФ на 2017 - 2030 годы». Данная стратегия устанавливает пути и порядок реализации государственной политики в области применения государственными организациями информационных и коммуникационных технологий при предоставлении услуг гражданам страны. Представленный в правовом акте приоритетный сценарий определит развитие информационного общества в России.

Из возможных вариантов регулирования информационного потребления с целью обеспечения безопасности детей в Российской

Федерации выбран вариант сорегулирования медиа и государства. Наряду с запретом информационной продукции, которая может принести вред развитию и здоровью ребенка, необходима организация последовательных и регулярных мероприятий, направленных на повышение уровня медиаграмотности детей, формирование навыков безопасного поведения в современном информационном пространстве.

Усилия семьи, общественных организаций и государства должны быть направлены на выработку у детей навыка самостоятельной оценки контента, умение анализировать информацию, противостоять манипулированию, рекламе асоциального поведения и дезинформации.

Отдельные аспекты информационной безопасности находят свое отражение в Законе РФ «Об информации, информационных технологиях и о защите информации». Настоящий Закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на конституционных правах и принципах:

– свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

– открытости информации о деятельности государственных органов и органов местного самоуправления и

свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

– установления ограничений доступа к информации только федеральными законами;

– достоверности информации и своевременности ее предоставления;

– равноправия языков народов РФ при создании информационных систем и их эксплуатации;

– обеспечения безопасности РФ при создании информсистем и их эксплуатации и защите, содержащейся в них информации;

– неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

– равноправие языков народов РФ при создании информационных систем и их эксплуатации.

Таким образом, в законах РФ затронуты основные аспекты правового регулирования цифровизации образования.

В Российской Федерации запущен и эффективно реализуется федеральный проект «Цифровая образовательная среда».

Цифровая образовательная среда (ЦОС) – это цифровое пространство, состоящее из открытой совокупности информационных систем, которые объединяют всех участников образовательного процесса – администрацию, педагогов, обучающихся и их родителей.

Основной задачей федерального проекта «Цифровая образовательная среда» проекта является создание современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования всех видов и уровней.

К 2030 году планируется обеспечить:

– внедрение целевой модели цифровой образовательной среды по всей стране;

– внедрение современных цифровых технологий в образовательные программы 25% общеобразовательных организаций 75 субъектов Российской Федерации для, как минимум, 500 тысяч детей;

– обеспечение 100% образовательных организаций в городах Интернетом со скоростью соединения не менее 100 Мб/с, в сельской местности – 50 Мб/с;

– создание сети центров цифрового образования «IT-куб», охватывающей в год не менее 136 тысяч детей (см. интернет-площадку проекта - https://edu.gov.ru/national-project/projects/cos/).

Проект позволяет обеспечить обновление содержания образования и предоставит возможность обучающимся свободно и безопасно ориентироваться в цифровом пространстве.

Цифровая образовательная среда обеспечивает повышение квалификации педагогов и оснащение образовательных организаций необходимой инфраструктурой. Создается цифровая экосистема, благодаря которой станет возможным переход к автоматизированному делопроизводству, работе с цифровыми

инструментами, использованию широкого спектра современных методик и технологий обучения.

Рассмотрим особенности внедрения Целевой модели цифровой образовательной среды, изложенной в приложении к Приказу Министерства просвещения РФ от 2 декабря 2019 г. N 649 “Об утверждении Целевой модели цифровой образовательной среды”.

В соответствии с методическими рекомендациями по вопросам внедрения Целевой модели цифровой образовательной среды в субъектах Российской Федерации внедрение целевой модели ЦОС осуществляется в образовательных организациях, осуществляющих деятельность в сфере общего образования, среднего профессионального образования и соответствующего дополнительного профессионального образования, профессионального обучения, дополнительного образования детей и взрослых, воспитания в рамках полномочий Минпросвещения России (далее – образовательные организации), органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования, органов местного самоуправления.

Внедрение целевой модели ЦОС в субъекте Российской Федерации осуществляется органом исполнительной власти субъекта РФ, осуществляющим государственное управление в сфере образования во взаимодействии с органом исполнительной власти субъекта Российской Федерации, осуществляющим государственное управление в сфере цифрового развития,

информатизации, связи и массовых коммуникаций по следующим направлениям:

– создание административно-управленских и организационно-технических условий для внедрения целевой модели ЦОС;

– внедрение и использование федеральной информационно-сервисной платформы цифровой образовательной среды;

– развитие материально-технической базы и информационно-телекоммуникационной и технологической инфраструктуры в образовательных организациях;

– развитие информационных систем и ресурсов (далее - региональные ИСИР), созданных за счет средств бюджета субъектов Российской Федерации в сфере образования, в том числе обеспечение их взаимодействия с информационными системами и ресурсами платформы ЦОС.

Цифровая образовательная среда (ЦОС) образовательной организации включает:

– комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы;

– совокупность технологических средств информационных и коммуникационных технологий: компьютеры, иное ИКТ оборудование, коммуникационные каналы;

– систему современных педагогических технологий, обеспечивающих обучение в современной ЦОС.

Подсистемы современной цифровой образовательной среды представлены на рисунке 1.

Рисунок 1 – Подсистемы цифровой образовательной среды

Цифровая информационно-образовательная среда образовательной организации должна обеспечивать:

- ✓ информационно-методическую поддержку образовательного процесса;
- ✓ планирование образовательного процесса и его ресурсного обеспечения;

- ✓ мониторинг и фиксацию хода и результатов образовательного процесса;
- ✓ мониторинг здоровья обучающихся;
- ✓ современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации;
- ✓ дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов управления в сфере образования, общественности), в том числе, в рамках дистанционного образования;
- ✓ дистанционное взаимодействие образовательного учреждения с другими организациями социальной сферы: учреждениями дополнительного образования детей, учреждениями культуры, здравоохранения, спорта, досуга, службами занятости населения, обеспечения безопасности жизнедеятельности.

ЦОС образовательной организации обеспечивает возможность осуществления в электронной (цифровой) форме следующих видов деятельности:

- планировать образовательный процесс;
- размещать и сохранять материалы образовательного процесса, в том числе работ обучающихся и педагогов, используемых участниками образовательного процесса информационных ресурсов;
- фиксировать ход образовательного процесса и результатов освоения основной образовательной программы;

– использовать данные, формируемые в ходе образовательного процесса, для решения задач управления образовательной деятельностью;

– взаимодействовать между участниками образовательного процесса, в том числе дистанционно посредством сети Интернет;

– контролировать доступ участников образовательного процесса к информационным образовательным ресурсам в сети Интернет (ограничение доступа к информации, несовместимой с задачами духовно-нравственного развития и воспитания обучающихся);

– осуществлять взаимодействие образовательного учреждения с органами, отвечающими за управление в сфере образования, и с другими образовательными учреждениями, организациями.

Цели формирования и использования ЦОС отражают интересы учителя, обучаемого, а также родителей и предусматривают следующее.

Для обучающегося:

– расширение возможностей построения собственной образовательной траектории;

– доступ к самым новым образовательным ресурсам;

– растворение рамок образовательных организаций до масштабов всего мира.

Для родителя:

– расширение образовательных возможностей для ребенка;

– снижение затрат, вызванное усилением конкуренции на рынке образовательных услуг;

– увеличение прозрачности образовательного процесса;

– облегчение общения со всеми участниками образовательного процесса;

– сокращение бюрократической нагрузки за счет автоматизации;

– повышение удобства мониторинга образовательного процесса;

– формирование новых условий мотивации учащихся при создании и выполнении заданий, организация условий для выработки индивидуальной образовательной траектории учащегося.

Для педагога:

– снижение бюрократической нагрузки за счет автоматизации;

– повышение удобства мониторинга образовательного процесса;

– формирование новых условий мотивации учащихся при создании и выполнении заданий, организация условий для выработки индивидуальной образовательной траектории обучающегося.

При этом открытая цифровая образовательная среда, формирует умения конкурировать в цифровом пространстве, сотрудничать, взаимодействовать, давать объективную оценку и вносить коррективы с учетом возможностей обучающихся.

Таким образом, цифровая образовательная среда образовательной организации представляет собой управляемую и динамично развивающуюся с учетом современных тенденций модернизации образовательную систему эффективного и комфортного предоставления информационных и коммуникационных услуг, цифровых инструментов объектам процесса обучения.

Программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р, выдвигает новые требования к системе профессионального образования.

Цифровизация экономики сопровождается и цифровизацией профессионального образования, призванных обеспечивать все отрасли экономики и социальной сферы высококвалифицированными кадрами.

Вслед за принятием термина «цифровая экономика» в широкий оборот вводятся и другие термины, в том числе «цифровое образовании», «цифровая образовательная среда», «цифровые образовательные технологии» и др.

Под цифровизацией обучения, как правило, понимается применение инновационных образовательных технологий, построенных на алгоритмах, при реализации которых обеспечивается высокая эффективность образовательного процесса с применением современного программного обеспечения.

В отечественной педагогической науке и практике ещё нет чёткого толкования новых терминов, связанных с развитием

цифрового образования. Анализируя мнения разных авторов относительно содержания терминов «цифровое образование», можно сформулировать следующее определение понятия «цифровое образование».

Цифровое образование – это процесс организации взаимодействия между преподавателями и обучающимися при движении от цели к результату в цифровой образовательной среде, основными средствами данной среды являются цифровые технологии, цифровые инструменты как результаты учебной деятельности в цифровом формате.

Необходимо отметить, что в процессе организации цифровой образовательной среды может возникать ряд рисков.

Риск 1: недостаточное финансирование и/или увеличение финансовой нагрузки на образовательную организацию. Подключение образовательных организаций к высокоскоростному Интернету, повышение квалификации педагогических работников по вопросам внедрения цифровых технологий в образовательный процесс, закупка оборудования финансируются из федерального и регионального бюджета. Несмотря на то, что использование электронных библиотек в учебном процессе может снизить затраты на закупку учебно-методической литературы, финансовая составляющая все же может быть недостаточной для целей формирования целостной ЦОС.

Риск 2: недостаточное кадровое обеспечение на начальном этапе становления цифровой образовательной среды. Эффективность образования всегда зависела от уровня подготовки

педагога. Сегодня преподаватель по-прежнему остаётся ведущим звеном всего процесса обучения, однако, интеграция информационных технологий и образования способствует формированию новой роли педагога. Повышение квалификации педагогических работников, осуществляющих образовательную деятельность, является одной из задач регионального проекта «Цифровая образовательная среда» и позволяет обеспечить актуализацию знаний, умений и навыков ведущего кадрового состава системы образования в части внедрения и использования современных цифровых технологий в образовании, тем не менее необходимым является введение должности «Заместитель директора по ИКТ» и/или организация наставничества по вопросам цифровизации.

Риск 3: неразработанность цифровой дидактики. Относительная инертность педагогики как науки идет вразрез с быстрым, молниеносным внедрением цифровых технологий.

Риск 4: технические неполадки, сбои, происходящие в техногенной среде, являющейся программно-аппаратным базисом ЦОС.

Риск 6: замена живого общения уроками в режиме онлайн отрицательно скажется на качестве образования.

Риск 7: риск подмены цифровизации образования оцифровкой. Для педагогически неэффективной «оцифрованной» дидактической практики характерны в том или ином сочетании, следующие особенности:

– использование информационно-коммуникационных технологий, не сфокусированных на решение конкретных педагогических задач;

– использование в оцифрованном виде традиционных дидактических элементов образовательного процесса (содержания, форм, методов, приемов обучения, прежней системы оценивания и контроля знаний) без какой-либо принципиальной их трансформации.

Риск 8: обеспечение информационной безопасности цифровой образовательной среды на ненадлежащем уровне, в частности, кибербезопасность личности.

Создание и функционирование цифровой образовательной среды образовательной организации должно соответствовать всем требованиям информационной безопасности. Именно тогда она позволит обеспечить модернизацию образовательного процесса, внедрить в педагогическую практику технологии электронного обучения, модели смешанного обучения, автоматизирует процессы управления качеством образования, формирование у студентов навыков обучения в цифровом мире, умению создавать цифровые проекты для своей профессии, присутствие в образовательной организации в сети Интернет.

Практические задания к разделу 1.

Задание 1.1. Подготовьтесь к семинарскому занятию. Вопросы для обсуждения:

1. Каково современное развитие цифровых учебно-

методических материалов, инструментов и сервисов, включая цифровое оценивание?

2. Сделать обзор по цифровым технологиям и изменению способов учебной работы, организации совместной работы учащихся посредством виртуальных площадок.
3. Каковы внешние и внутренние факторы информатизации образования? Каково современное состояние внедрения цифровых технологий в образовательный процесс?
4. Перечислите методические и психолого-педагогические аспекты использования мультимедиаресурсов в учебном процессе.
5. Сделайте мини-доклад по темам: «Технологии искусственного интеллекта в образовании», «Технология виртуальной реальности», «Технология блокчейн в образовании».
6. Предложите меры для устранения цифрового неравенства.

Задание 1.2. Разработайте интерактивные упражнения на одной из популярных цифровых платформ: Онлайнтестпад, Яндекс-формы, iSpring.

Задание 1.3. Составьте план урока, на каждом этапе которого используйте цифровые инструмент. Образец выполнения представлен ниже.

Урок по теме «Носители информации».

1. Этап мотивации и целеполагания.

Взаимное приветствие, знакомство с аудиторией. Озвучивание новой темы: «Носители информации». Можно принести носители информации (диски, флеш-память) и показать их аудитории, чтобы наглядно ознакомить с тем, о чем пойдет речь. Допустимо представить цифровые иллюстрации.

Рисунок 2 – носители информации

2. Этап актуализации знаний.

Опросить студентов по темам вычислительной техники (классификация ЭВМ, устройство персонального компьютера). Показать ментальную карту на сайте Mindmeister, по прошлым темам, см.рисунок 3:https://www.mindmeister.com/ru/2391525449/

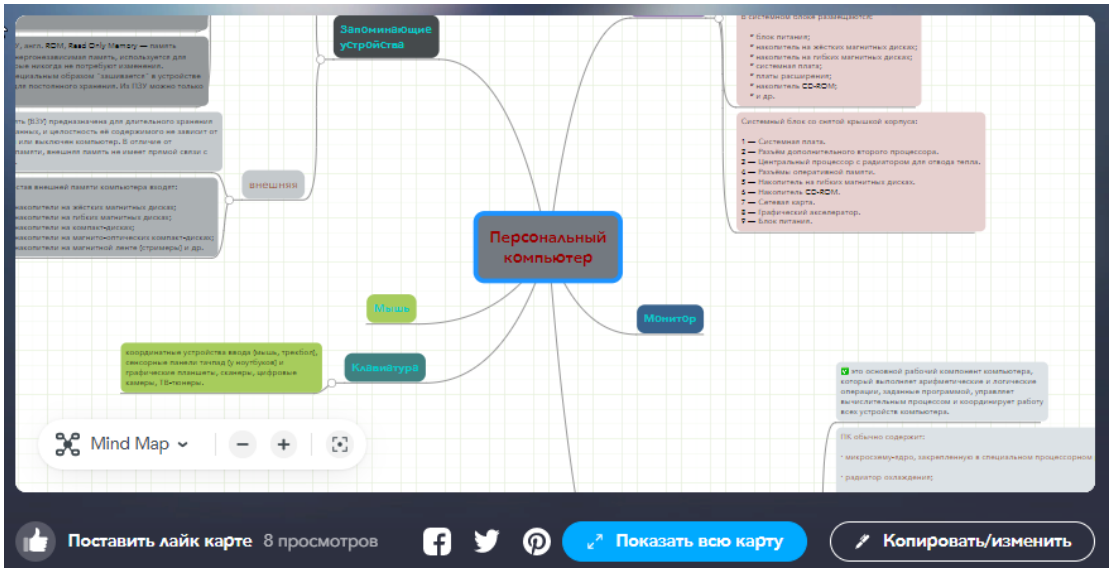

Рисунок 3 – ментальная карта.

3. Этап изучения новых знаний.

Провести лекцию студентам по заданной теме.

Лекция представлена в облачном хранилище:

https://www.sites.google.com/site/informatikadzabasova/tehniceskie-sredstva-informatizacii/nositeli-informacii

https://www.youtube.com/watch?v=77n3f76UmrM

Показать студентам модели носителей информации, которые показывались в начале занятия.

Рисунок 4 – носители информации

4. Этап закрепления полученных знаний.

Студенты пересаживаются за компьютеры и составляют графические карточки по теме занятия.

В сервисе достаточно разнообразный, яркий выбор шаблонов, но он на английском языке, поэтому при работе нужно включить автоматический перевод страницы.

https://www.easel.ly

Рекомендуется создать карточку с помощью другого сервиса – Visme. Сервис также на английском языке, поэтому требуется включить перевод страницы.

https://www.visme.co/ru/sozdat-infografika

Студентам предлагается выбрать любой из сервисов и создать карточку по теме занятия.

5. Этап самооценки, рефлексии.

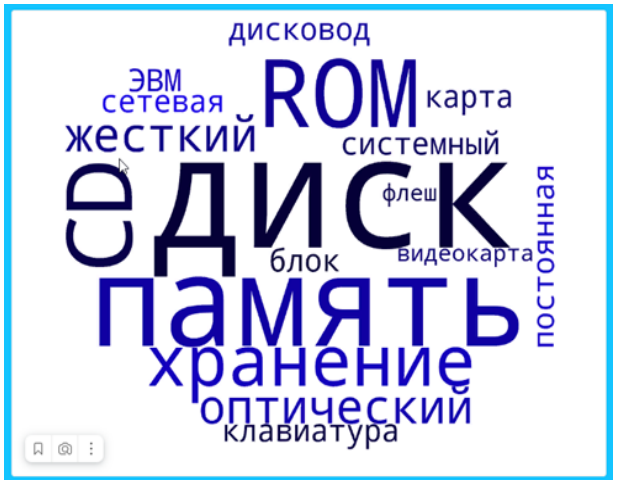

Рисунок 5 – облако слов для рефлексии

Опросить студентов как прошло занятия, есть ли какие-то вопросы, проанализировать затруднения. Предложить студентам пройти облако слов для рефлексивных оценок. Каждому студенту достанется одна из предложенных карточек, его задача: отыскать слова по теме занятия.

Список источников по разделу 1

1. Белевитин В.А., Е.А. Гафарова. Теоретико-методологическое аспекты цифровой трансформации современного педагога образовательной организации / В.А. Белевитин, Е.А. Гафарова // Вестник Южно-Уральского государственного гуманитарно-педагогического университета. — 2022. — № 5 (171). — ISSN: 2618–9682.

2. Гафарова Е.А. «Информация», «творчество», «креативность»: междисциплинарный анализ понятий. [Текст] / Е.А. Гафарова, В.А. Белевитин, Г.А. Диденко, Н.А. Василькова, О.Н. Шварцкоп // Современная наука: актуальные проблемы теории и практики. Серия: «Гуманитарные науки». — 2021. — № 9. — С. 43–47. — ISSN: 2223–2982.

3. Главный тренд российского образования – цифровизация. [Электронный ресурс] // URL: http://www.ug.ru/article/1029/ (дата обращения: 18.03.2024)

4. Информатизация образования. [Электронный ресурс] // Российская педагогическая энциклопедия. Режим доступа: https://pedagogicheskaya.academic.ru/1241/ (дата обращения: 18.03.2024)

5. Информационный сервис для профессионального образовательного сообщества «Агрегатор новостей образования» [Электронный ресурс] // URL: https://akvobr.ru/cifrovaya_obrazovatelnaya_sreda_ehto. html (дата обращения: 18.03.2024)

6. Меняйся или уходи. Цифровое образование бросает вызов преподавателям вузов. [Электронный ресурс] // URL: http://www.poisknews.ru/theme/edu/31969/ (дата обращения: 18.03.2024)

7. Об утверждении Целевой модели цифровой образовательной среды: [приказ Министерства просвещения РФ от 02.12.2019 № 649, зарегистрирован в Минюсте РФ 24.12.2019, регистрационный № 56962] [Электронный ресурс] // Правовая база Гарант. — 2020. — URL: https://www.garant.ru/ (дата обращения: 18.03.2024)

8. Образовательные экосистемы для общественной трансформации. Доклад Global Education Futures [Электронный ресурс] / П. Лукша, Дж. Кубиста, А. Ласло // Образование для сложного общества. – С. 77. URL: https://drive.google.com/file/d/0B9ZvF6mQ5FMbSTFKVmhodU5rNTNiTX pUZ2QwZktiR0pzSmJR/view (дата обращения: 18.03.2024).

9. Приказ Министерства просвещения РФ от 2 декабря 2019 г. N 649 “Об утверждении Целевой модели цифровой образовательной среды”

10. Приоритетный проект в области образования «Современная цифровая образовательная среда в Российской Федерации». [Электронный ресурс] // URL: http://neorusedu.ru/about/ (дата обращения: 18.03.2024).

11. Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы Цифровая экономика Российской

Федерации» [Электронный ресурс] // URL: base.garant.ru/71 734 878 (дата обращения: 12.08.2020)

12. Цифровые образовательные технологии: дидактические возможности и риски / Н.А. Василькова, Е.А. Гафарова, Г.А. Диденко, О.Н. Шварцкоп. — Челябинск: ЗАО "Библиотека А. Миллера", 2023. — 99 с. — 50 экз. — ISBN: 978-5-93162-751-9

13. Электронный ресурс: https://edu.gov.ru/national-project/projects/cos/ - (дата обращения: 18.03.2024)

Раздел 2 Кибербезопасность личности как педагогическая проблема

Появление информационных технологий кардинальным образом воздействовало на представление о коммуникационных способностях человека. С каждым годом появляется все более и более новых возможностей, которые в настоящее время еще не до конца изучены.

Ход глобализации непосредственно объединён с информационным пространством, которое на сегодняшний день все глубже уходит в виртуальную сферу и тесно связано с современными информационными технологиями. Любой пользователь глобальной сети попадает в огромную и нескончаемую «реку» информации, начинает погружаться все глубже, впитывая в себя информацию. Именно появление глобальной информационной сети с открытым доступом определило новую проблему безопасности личности в целом – кибербезопасность личности.

На сегодняшний день мы пытаемся получить доступ к большому объёму информации и экстраполировать её в своих интересах. На фоне этого вполне очевидно свою нишу заняли социальные сети, как нескончаемые источники информации и удобнейший ресурс для навязывания своего мнения. Конечному пользователю необходимо научиться прокладывать себе путь через нескончаемые потоки информации, чтобы в конечном итоге получить интересующие его знания.

Глобальные информационные технологии заметным образом изменили привычные всем методы изучения и изменения информации. Человечество получило в свои руки инструменты и системы для межсетевого общения, которые облегчили коммуникацию и перевернули привычное общение.

Для того, чтобы встретиться и пообщаться с другим человеком, раньше требовалось заранее договорится о встрече или позвонить по телефону, сейчас же - достаточно обычного сообщения в любой социальной сети или видеозвонка. Именно поэтому одним из самых популярных сервисов глобальной сети являются социальные сети.

Впервые понятие социальных сетей в реальном мире ввел Дж. Барнс в 1954 году. Он определял их как социальное поле, в рамках которого люди являются друзьями или просто знакомы друг с другом. Похожее определение было дано в 1987 г. психологами М.С. Денофф и П.А. Пилконис, которые определили социальную сеть как набор межличностных отношений, связывающих людей.

В социальных сетях правдивость и реальность информации устанавливаются за счет реальных знакомств между людьми, которые входят в сообщество и знакомы друг с другом за пределами социальных сетей. В таких сообществах все участники следуют правилам установленными администраторами и руководителями данной сети.

Социальные сети — это своего рода отголосок виртуального мира, он подчиняется тем же правилам и имеет ту же

конструкцию.

По направленности сообщества в социальных сетях могут быть узкотематическими, полемическими, информационными и т.п. Одна из самых важных составляющих, непосредственно влияющих на жизнеспособность сети, является её экономическая составляющая, поэтому в социальных сетях можно найти и много различных сообществ, представляющих конкретные фирмы и организации из реального мира. Это продиктовано тем, что в современном обществе проще всего воздействовать на многомиллионную аудиторию через лидеров мнений, которые в большом достатке обитают в социальных сетях. Они помогают сформировать положительное мнение о продукте, навязать молодой аудитории свою точку зрения и вынудить приобрести продукцию рекламодателя.

Одним из самых эффективных способов воздействия на целевую аудиторию в социальных сетях является предоставление информации, восхваляющей или порочащей какой-либо товар, услугу или даже человека. Данный прецедент принято называть инфоповодом. Иногда такие средства становятся откровенной информационной ложью, которая в свою очередь наносит сильный ущерб имиджу человеку, товара или услуги. Однако, такие действия попадают под нарушение статьи 7 Федерального закона «О персональных данных ФЗ-152: «Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если

иное не предусмотрено федеральным законом».

На сегодняшний день множество людей не может даже представить своей жизни без социальных сетей. Зачастую люди становятся зависимы от общественного мнения и социальных сетей. Социальные сети сопровождают человека на протяжении всего дня с момента пробуждения, до того момента как человек ляжет в кровать. В такой ситуации человек почти полностью теряет контроль над собственной жизнью. Находясь в виртуальной среде социальных взаимодействий человек теряет возможность трезво оценивать свою жизнь, ему необходимо чтобы общество делало это за него посредством комментариев, лайков/дизлайков. В погоне за статусом человек теряет понимание о рамках приличия, дозволенности и безопасности.

С другой стороны, социальные сети помогают человеку избавиться от одиночества. Здесь он может пообщаться с людьми, которых никогда не знал в жизни, он активно включается в коммуникацию между личностями, хотя при этом реальное общение замещается виртуальным.

Социальные сети активно влияют на процесс коммуникации, в результате чего, отношение людей к окружающему миру изменяется, деформируется. Чувство нарциссизма противопоставляется семейным и национальными связям пользователя.

Этот процесс, по мнению антрополога Ш. Теркл, включает в себя: исчезновение одиночества как части процесса социализации; зависимость от социальных сетей и гаджетов, обеспечивающих

непрерывный процесс «виртуальной коммуникации» в ущерб «традиционным» социальным практикам общения; исчезновение причастности в региональной культуре; зависимость от гаджетов, часто западного производства; деформация процесса общения; отчуждения в семье; деформация языкового общения; формирование новой этики; потенциальное разрушение личного пространства.

Особенно подвержены влиянию социальных сетей дети и подростки. Они прикованы взглядами к своим кумирам и вторят их действиям и мышлению не задумываясь о том, к чему может привести такого рода мышление, как пример мы можем увидеть влияние запрещенной на территории РФ организации «ФБК» на разум и сознание детей, они не пытаются и не хотят анализировать реальную ситуацию в стране, а просто по призыву, как марионетки, выходят на улицы и скандируют опасные лозунги.

На сегодняшний день в социальных сетях особенно активно проходят различные информационные кампании, которые нацелены на создание положительного образа на конкретные информационные события по актуальным экономическим, политическим, социальным и другим вопросам. Благодаря социальным сетям появились и продолжают появляться все новые инструменты воздействия на человеческое сознание, манипуляции вкупе с внушением и убеждением.

Именно такое положение дел вызывает обеспокоенность педагогов и психологов.

Возникает реальная проблема кибербезопасности личности, состоящая в неконтролируемом влиянии на мотивы, потребности, поведение и индивидуальные качества личности пользователя кураторов интернет-ресурсов.

Непрекращающаяся информационная война переместилась в пространство социальных мессенджеров и социальных сетей, где главным объектом воздействия выступает человек, его психика, нравственный и духовный мир, социально-политические, психологические ориентации, установки, отношения, рациональные и иррациональные аспекты поведения, системы общественного мнения и принятия решений.

Угрозы, исходящие от сетевого коммуникативного пространства, реальны. Их обычно рассматривают в контексте проблемы обеспечения информационной безопасности, которая в российских нормативно-правовых актах определяется как состояние защищенности информационной среды и деятельность по предотвращению утечки защищаемой информации, по защите от несанкционированных и непреднамеренных воздействий на нее. Соответственно, информационная безопасность личности в интернет-пространстве определяется как состояние сохранности информационных ресурсов личности и защищенности законных прав в информационной сфере.

Как правило, состояние защищенности трактуется как защита конфиденциальности (обеспечение доступа к информации только авторизированным пользователям), целостности (обеспечение достоверности и полноты информации и методов ее

обработки) и доступности (обеспечение доступа к информации и связанным с ней активам авторизированных пользователей по мере необходимости) информации.

Однако существующая защищенность информационных ресурсов не гарантирует пользователю кибербезопасности личности.

Из-за вседозволенности создателей интернет-ресурсов возникает проблема вовлечения пользователей в террористическую деятельность, а также оказания влияния на психические и психологические характеристики индивида - пользователя.

Определенная часть пользователей не обладает базовой информацией о защите своего личного информационного пространства и попадаются на различные уловки, как пример каждый год в полицию обращаются огромное количество девушек и парней, которым злоумышленники отправили угрозу опубликовать их личные данные, фото или видео, если они не переведут условную сумму на подставной кошелек. И с ростом пользователей социальных сетей количество киберпреступников не идет на спад, а наоборот только растёт.

Таким образом, можно сделать вывод о том, что отражение возникающих информационных угроз, напрямую зависит об осведомленности пользователей о способах их отражения.

Как уже говорилось ранее, наиболее опасными источниками угроз можно считать манипулирование сознанием человека посредством формирования вокруг него среды с измененным

«более правильным» мнением, что приводит его к неизбежному следованию за новыми идеалами.

Так же к отрицательным остаткам можно отнести информационную перегрузку личности, которая возникает при формировании интернет-зависимости, вследствие чего человек начинает ощущать дефицит новой информации, межличностного общения и прочих видов потребностей, которые он никак не может утолить. В свою очередь, это приводит к обесцениванию устоявшихся норм и правил привычной жизни.

Одним из наиболее опасных источников угроз для людей является использование его же персональных данных против него. Инструментарий социальных сетей позволяет с легкостью надавить на уязвимые психические триггеры и выставить любое лицо в необходимом свете. Помимо этого, к угрозам можно так же отнести прямые угрозы или распространение ложной информации о личности.

Новые электронные медиа обладают почти безграничными возможностями передачи любой информации любым ее отправителем в различных направлениях, но медийные информационные потоки формируются в интересах владельцев транснациональных информационных агентств. Процесс монополизации на медиарынке приводит к угрозам манипулирования общественным мнением по отношению к тем или другим значимым событиям и, что еще более серьезно, к деформации моральных устоев общества, его национальной культуры путем навязывания ему чужих ценностей.

Разумеется, сетевые коммуникации сами по себе являются просто эффективной технологией для успешного развития бизнеса владельцев транснациональных информационных агентств. Западный бизнес ставит своей целью разрушение нормативно-ценностной системы общества, стремится распространить свои «правила игры», свою логику экономического, социального действия с тем, чтобы реализовывать коммерческие проекты в адаптивной для себя среде.

Попутно глобальный медиарынок выполняет заказы, продиктованные ведущими геополитическими игроками. Ярким тому примером является мощная подача в информационных международных агентствах заведомо ложной информации о нападении России на Грузию в августе 2008 году. А в настоящее время, с начала специальной военной операции на Украине, СМИ и интернет-ресурсы становятся полноценным оружием в комплексной войне, в которой сочетаются и «горячая фаза» на линии боевого соприкосновения с «холодной», информационной атакой, имеющей целью сформировать некий новостной концепт в интересах противника.

По данным аналитиков, число опасных Интернет-ресурсов за последнее время увеличилось в три раза. Эксперты по Интернет-безопасности утверждают, что сегодня атаки на ресурсы Всемирной паутины происходят каждые четыре с половиной минуты. Во многих странах отмечается увеличение объемов утечки данных, при этом только около 20% происходит из-за хакерских атак. По данным МВД, в 1 квартале 2022 года

Количество IT- преступлений выросло на 83,9%, а удельный вес таких деяний достиг 19,9% от общего числа. В основном из-за этого фактора уровень преступности в стране в целом вырос на 4%.

Во Всемирной паутине сегодня существуют различного рода закрытые сети. Сетевые структуры эффективно используются организациями в условиях конспирации. Их главным козырем становится молниеносность распространения информации и новые возможности дистанционного управления террористическими актами. Террористические группы и мафиозные структуры используют нелегальные, полулегальные и криминальные методы политической борьбы, игнорируя правовые нормы и традиции, нарушая законы, расшатывая политический строй обществ.

Бесспорно опасный источник угроз в условиях сетевой коммуникации — это непрерывно разрастающееся влияние информационных войн и распространение информации, напрямую влияющее на сознание и мировоззрение людей.

Существуют также методы ведения информационной войны на территории информационной среды противника с целью полной дезинформации и создания хаоса и паники посредством методов и технологий дающих воздействовать на информационную среду. И.Л. Морозов различает три вида информационно-психологического оружия относительно стратегии нападения:

1. Системы дистанционного искажения или уничтожения

информации: компьютерные вирусы общего и специализированного назначения (программы, проникающие извне и разрушающие систему); логические бомбы, тайно внедряемые в компьютер на этапе заводской сборки, которые при активизации парализуют работу компьютера;

2. Системы хищения информации: электронные шпионы (программы, проникающие извне и производящие незаметный для пользователя сбор служебной и непосредственно личной информации);

3. Системы комплексного воздействия на психику пользователя: мультимедийные сайты в виде информационно развлекательных или аналитических страниц с «горячей», «сенсационной» информацией.

Существует мнение, что повышение уровня «прозрачности» и доступности информации для всех участников политического процесса (например, в случае проведения президентских и парламентских выборов) облегчает общественный контроль за ним со стороны общественности. Однако, исследователи выделяют два блока угроз, ведущих к подрыву политических режимов: системные и периферийные угрозы.

Первый тип угроз направлен на дестабилизацию конкретных политических систем или их сегментов со стороны враждующего государства и затрагивает в основе своей атаки на информационное поле оппонента с использованием информационно-психологических атак властных и околовластных структур.

Не менее серьезную опасность представляют угрозы второго типа, которые связаны с деятельностью широкого спектра внесистемных сил — от международных террористических организаций до всевозможных хакерских групп. Неструктурируемость и непрогнозируемое возникновение периферийных информационных угроз крайне затрудняют выработку действенной защиты от них.

Сетевые пользователи, составляющие внесистемную оппозицию, делятся им на две группы — легальное «самобытное сопротивление», которое находит себе опору в традиционных и нетрадиционных ценностях сообщества, и на нелегальные криминально-мафиозные сети. Основной силой легального и нелегального сопротивления является исключительно сетевая, децентрализованная форма организации и политических действий. Характерным примером такого сопротивления становится стремительно нарастающее движение антиглобалистов, которое строится на основе национальных и международных сетей, активно используется Интернет, и при этом сети не только обеспечивают организацию их деятельности, но и совместное использование информации.

Децентрализованный, неуловимый характер сетевых структур сопротивления антиглобалистов и других самобытных движений (экологисты, «зеленые», женские движения, различные молодежные субкультуры, представленные, в частности, в блогосфере) во многом затрудняет их восприятие и идентификацию со стороны государственного управления.

В конечном итоге можно выделить следующие основные категории информационных угроз, оказывающих свое влияние на общество, государство и личность посредством сетевых коммуникаций:

— Угрозы безопасности личности, связанные с манипуляцией над сознанием и информационной перегрузкой человека, с непосредственным увеличением в информационную зависимость, сюда же можно отнести и использования личных данных во вред личности, таких как сбор личных данных с целью внедрения таргетированной рекламы конкретному человеку;

— Угрозы, связанные с управлением и манипуляцией над общественным мнением, появлением особых механизмом управления массы людей с целью организации процессов направленных на разрушение привычных ценностей общества;

— Угрозы безопасности всех государственных структур, на которые пытаются повлиять посредством международной преступности и терроризма.

— Угрозы стабильности существующих режимов власти, обусловленные неконтролируемыми всплесками высказывания и активизации опасной оппозиции в социальной и сетевой коммуникации.

Таким образом, проблема обеспечения кибербезопасности личности является многоаспектной, социальной, педагогической и психологической проблемой, для разрешения которой потребуются усилия специалистов различных профилей. Педагогика может внести свой посильный вклад в снижение

остроты существующего противоречия между потребностью граждан взаимодействовать в социальных сетях, мессенджерах, в виртуальном интернет-пространстве, с одной стороны, и необходимость обеспечить информационную безопасность личности в названной среде – кибербезопасность.

Практические задания к разделу 2.

Задание 2.1. Ознакомьтесь с основными терминами, представленными в теоретической части. Ответьте на вопросы.

1. Какие социальные сети вы знаете? Перечислите их.

2. Сравните две любые социальные сети, определив их отличия.

3. Перечислите возможности социальных сетей, которые может использовать современный студент.

4. Перечислите возможности социальных сетей, которые можно использовать в образовательном процессе.

5. Чем отличаются открытая, закрытая и частная типы групп?

6. Можно ли лишить участников сообщества возможности комментировать записи на стене? Каким способом?

7. За какие нарушения сообщество может быть заблокировано администрацией «ВКонтакте»?

Задание 2.2. Рассмотрите использование современных социальных сетей в образовательном процессе на примере сети «ВКонтакте» с точки зрения кибербезопасности.

Задание 2.3. Работа с личной страницей в «ВКонтакте»

Зайдите в социальную сеть (https://vk.com/), используя свой логин и пароль. Если вы не авторизованы – создайте новый аккаунт.

Ознакомьтесь с основными разделами личной страницы профиля, найдите аватар, основную информацию, разделы бокового меню, стену.

Отредактируйте информацию о себе. Добавьте в раздел Образование свой факультет и вуз.

Добавьте в друзья присутствующих одногруппников, воспользовавшись поиском. Используйте дополнительные параметры поиска: страна, город, возраст, пол и т.д.

Обменяйтесь личными сообщениями с тремя одногруппниками, воспользовавшись разделом Мессенджер.

Студент, сидящий за компьютером № 3, создает беседу, состоящую из всех присутствующих в аудитории. Для этого нажмите «+» в верхнем правом углу раздела Мессенджери добавьте в беседу всех участников. Пригласите в беседу преподавателя, поучаствуйте в общем чате. Ответьте на любое сообщение, используя смайлы или стикеры ВК.

Придумайте сообщество с образовательной функцией по вашему направлению обучения (например, клуб обучения английскому языку; биология для начинающих; группа подготовки к экзамену по отечественной истории; репетитор по математике и т.д.).

Заполните поля, представленные на вкладке Создание сообщества информацией о создаваемом сообществе. Укажите

название, тематику. Поставьте тип Открытая (в дальнейшем можно сделать сообщество закрытым, частным после сдачи работы преподавателю). Нажмите Создать сообщество.

Оформите сообщество. Воспользовавшись Интернетом, подберите аватар для сообщества. Добавьте необходимые сведения. Самостоятельно ознакомьтесь с полезной информацией по управлению сообществом.

Задание 2.4. Изучите регламент цифрового присутствия, разработайте собственный план обеспечения минимизации цифрового следа.

Регламент (методы) цифрового присутствия

Данный регламент описывает основные принципы формирования эффективной модели цифрового присутствия с учетом необходимости тщательной защиты персональных данных человека.

1. Контролируемые зоны

Для реализации эффективной модели цифрового присутствия необходимо использование принципа контролируемых зон, заключающегося в разграничении доступа к персональным данным в зависимости от текущей использующейся контролируемой зоны. Применение данного принципа важно для формирования культуры взаимодействия со своей цифровой личностью и обеспечения безопасности цифрового присутствия. Несмотря на название, данный принцип предусматривает некую гибкость, смещение

рамок контролируемых зон в сторону ужесточения или смягчения накладываемых ограничений на основе решения субъекта.

Контролируемые зоны определяют доступность персональных данных субъекта в реальном мире. К примеру, в рабочей обстановке пользователь может использовать рабочий, общедоступный телефон для связи с общественностью, а на территории своего домохозяйства – личный телефон для связи с узким кругом близких и друзей.

Контролируемая зона определяется территорией субъекта персональных данных, на которой исключено пребывание лиц или объектов, не имеющих допуска. В таблице ниже продемонстрирован принцип формирования контролируемых зон.

Таблица 1. Концепция контролируемых зон

	Концепция контролируемых зон		
	Нулевая	Первая	Вторая
Присутствие недопущенных лиц	ДА	НЕТ	НЕТ
Наличие недоверенных подключенных/ неподключенных к Интернету приборов	ДА	ДА	НЕТ
Защита периметра	НЕТ	НЕТ	ДА

Как видно из таблицы, в условиях второй, самой защищенной контролируемой зоны, субъект персональных данных может

ограничить присутствие посторонних лиц, отключить устройства от Интернета и при необходимости защитить параметр от утечек персональных данных с помощью сторонних аппаратных средств (например, от съема акустических колебаний стекол). Таким образом, субъект сможет находиться в безопасности, не опасаясь утечек персональных данных и нежелательных последствий, которые могут возникнуть впоследствии. Во второй контролируемой зоне под защитой специальных средств могут храниться финансовые сведения, сведения о здоровье, информация о частной жизни субъекта и т.п.

Для формирования цифрового присутствия субъект персональных данных может применить на практике контролируемую зону нулевого или первого уровня, в зависимости, требуется ли присутствие лиц, с которыми необходимо осуществлять социальное взаимодействие.

Контролируемая зона предусматривает один или несколько периметров. Каждый из периметров отдельно может быть как охраняемым, так и не охраняемым, в зависимости от уровня существующей угрозы и модели правонарушителя. Физически могут существовать как периметр допуска на территорию организации, требующий одного уровня разрешения, а также внутренний периметр допуска в отдельные помещения, требующий дополнительное разрешение. В каждой контролируемой зоне применяются различные технические средства и способы защиты и контроля.

2. Профили

Информация, которую субъект персональных данных передает в цифровую среду, остается привязанной к источнику и идентифицирует его. Каждый "шаг" цифрового присутствия фиксируется, анализируется и позволяет определить субъекта, узнать новые сведения.

Каждый год появляются новые накопители и источники данных: датчики и носимые устройства, умная бытовая техника и др. Появляются новые сервисы и приложения, запрашивающие и собирающие данные о пользователях.

Но у размещения информации в Интернете две стороны. Так, публичное размещение геолокации в сообщении привлекает потенциальных злоумышленников: информирует об отсутствии пользователя в жилище, например. Но также позволяет быстро и удобно оформить заказ на сайте доставки.

Поэтому пользователю необходимо определять, кому и какие сведения о нем открыты, а для кого - закрыты. Описанная концепция профилей позволяет этого достичь.

Принцип профилей субъекта персональных данных в цифровой среде напоминает концепцию контрольных зон, как показано в таблице 2 ниже.

Таблица 2 Концепция профилей с предоставлением данных по выбору пользователя

	ОСНОВНОЙ	ПУБЛИЧНЫЙ	РАБОЧИЙ	ГОСУСЛУГИ	БАНКОВСКИЙ	ЛИЧНЫЙ	СЕРВИСНЫЙ
ФИО (или псевдоним)							
Портрет							
Отпечатки пальцев							
Место работы							
Должность							
Звания, степени							
Домашний адрес							
Рабочий адрес							
Домашний телефон							
Рабочий телефон							
Мобильный телефон							
Специальный телефон							
Основной адрес электронной почты							
Дополнительный адрес электронной почты							
Рабочий адрес электронной почты							
Временный адрес электронной почты							
Мессенджер							
Сайт							
Авто							
Документ							
Банковская карта							

Пользователь формирует вокруг своей цифровой личности уникальные контролируемые зоны, которые отличаются набором доступных исходящих персональных данных и набором допущенных входящих сервисов, приложений и других лиц. В

зависимости от используемого приложения/сервиса или устройства пользователь предоставляет только те данные, которые необходимы для эффективного взаимодействия с ним в цифровой среде (с учетом, что обеспечивается должная степень защиты персональных данных). В таблице выше приведен краткий вариант концепции, которая на самом деле гибка и имеет множество вариаций (контролируемых зон), зависящих от субъективных потребностей пользователя.

Приведенные поля являются именно примерами и могут регулироваться по потребностям пользователей.

Так, публичный профиль может подразумевать использование некоего обнародованного псевдонима, общедоступного аккаунта в социальной сети и номера телефона, по которому может дозвониться любой желающий. Личный профиль наоборот, предполагает применение личного телефонного номера, реального имени и личной закрытой страницы в социальной сети.

Представленная в таблице концепция профилей носит исключительно демонстрационный характер; количество профилей и данные, которые предоставляются в рамках каждого из них, регулируются самим субъектом персональных данных. При этом следует учитывать, что чем меньше персональных данных предоставляется, тем меньше вероятность их утечки и реализации угрозы безопасности в адрес субъекта.

3. Разрешения на обработку персональных данных

На данный момент времени должные меры по контролю за сбором, обработкой и хранением персональных данных обеспечиваются не в полной мере. В виду этого, для обеспечения максимальной степени защиты от потенциального воздействия угроз безопасности персональных данных, следует свести подтверждение разрешений к минимуму. В случае, если разрешение на обработку персональных данных для формирования эффективной модели цифрового присутствия необходимо, следует внимательно ознакомиться с текстом документа и предоставить минимальный набор персональных данных (если такое возможно), либо воспользоваться программой/услугой, не предусматривающей доступ к персональным данным пользователя (либо сводящей его к минимуму).

При наступлении момента прекращения использования программы/услуги, для которой разрешение на обработку персональных данных предоставлено, необходимо вручную отозвать разрешение и обязать соответствующего оператора персональных данных (со стороны разработчика программного обеспечения или владельца предоставляемой услуги) удалить персональные данные с целью предупреждения угрозы их несанкционированного использования.

4. Настройка аппаратно-программного комплекса

Так как в настоящее время культура цифрового присутствия только формируется и его участники не задумываются о рисках

присутствия в цифровых средах, необходимо всеобъемлющее оповещение и обучение нормам безопасности. Данные нормы касаются не только контроля предоставляемых данных, но и максимально возможных мер по защите от угроз безопасности, способных повлечь несанкционированное раскрытие, уничтожение, изменение, блокирование, копирование, распространение персональных данных. Помимо профилирования цифрового присутствия и соблюдения принципа контролируемых зон, необходимо использовать нескомпрометированное аппаратное и программное обеспечение, а также конфигурировать его должным образом.

Важно отметить, что описываемые принципы настройки программного оборудования не гарантируют стопроцентной защиты от утечек персональных данных, поэтому должны использоваться совместно с организацией офлайн- и онлайн-присутствия.

Необходимо тщательно подходить к вопросу выбора аппаратного обеспечения, по возможности ориентируясь на устройства без явных фактов дискредитации. Выбираемые устройства должны поддерживать последние разработки в плане защиты персональных данных и работать под управлением актуальных версий операционных систем с последними обновлениями, позволяющими закрыть известные бреши в системе безопасности.

Конфигурации устройств не должны поддерживать возможность несанкционированного доступа, как по сетевым каналам, так и с помощью внешних устройств и оптических дисков. Кроме того, не допускается использование стандартных (дефолтных) паролей для доступа к аппаратному обеспечению.

Носители информации в устройствах должны поддерживать и использовать шифрование данных.

При продаже или уничтожении устройств, хранящих данные (к примеру, оперативной памяти или жестких дисков), необходимо убедиться в тщательном удалении (уничтожении) данных на носителе и невозможности их восстановления. Для этого используются специальные программные или аппаратные инструменты.

Практически все устройства находятся под управлением нескольких наиболее распространенных операционных систем. Среди этих устройств – смартфоны, телевизоры, настольные компьютеры и ноутбуки, планшетные компьютеры, автомобили и многое другое. Важно критически подходить к выбору операционной системы своего устройства – и не использовать те, о которых имеются сведения о дискредитации. Также необходимо учитывать важный аспект, касающийся использования только официальных версий систем. Версии, находящиеся во взломанном виде в открытом доступе, могут содержать зловредное программное обеспечение. Пользователь должен обладать

достаточным сетевым опытом и техническим бэкграундом, чтобы отличить безопасную сборку от небезопасной.

Необходимо опираться на следующие принципы, относящиеся как к операционным системам, так и к прикладному программному обеспечению:

1. Пользоваться лицензионными версиями программного обеспечения;
2. По возможности/при необходимости делать выбор в пользу защищенных операционных систем;
3. Скачивание приложений производить только через официальные источники;
4. Всегда проверять надежность производителя приложения (не ограничиваться исключительно рейтингами других пользователей и отзывами) и официальность сборки (проверять хэш-сумму загруженного файла и другие методы);
5. Устанавливать только минимум нужных приложений и своевременно удалять неиспользуемые программы. Особенно это касается уязвимого программного обеспечения, такого Java и Flash;
6. Отдавать предпочтение программному обеспечению, которое обладает функционалом защиты от утечек персональных данных;

7. Внимательно и осознанно предоставлять доступ к персональным данным при появлении запросов от устанавливаемого программного обеспечения;
8. Внимательно анализировать лицензионные соглашения на предмет обязанностей пользователя и разработчика;
9. Своевременно обновлять программное обеспечение и драйверы используемых устройств
10. В случае подключения к точкам доступа Wi-Fi, Bluetooth, а также базовым станциям оператора сотовой связи по возможности удостоверяться в надежности устройства связи. Не осуществлять подключение к публичным (открытым) точкам доступа к цифровой среде. Отключать неиспользуемые интерфейсы связи;
11. Использовать надежные парольные политики. Не допускать использование стандартных (дефолтных) паролей для доступа (а также открытого доступа) к программному обеспечению. По возможности следует использовать системы многофакторной аутентификации с помощью нескомпрометированных устройств;
12. Применять средства антивирусной и антифишинговой защиты.

Также недопустимо относиться к личным портативным устройствам как публичным, доступным для обмена с другими пользователями, возможными для временного использования

другими лицами. Такое поведение упрощает доступ к операционной системе со стороны недоверенных лиц и нарушает конфиденциальность данных.

Отдельно стоит обращать внимание на браузерные приложения – им после операционных систем доступен наиболее обширный пласт данных о пользователе. Как и в случае с прочим программным обеспечением, следует делать выбор в сторону программ, акцентирующих внимание на отсутствие элементов отслеживания действий пользователя и предоставляющих дополнительные меры по защите от угроз безопасности персональных данных.

При выборе любого другого программного обеспечения следует руководствоваться теми же принципами, а также не допускать возможности установки программного обеспечения недоверенными лицами.

5. Превентивные меры

В вопросах информационной безопасности, как и любых сферах предупреждения рисков, важно предпринимать меры, предупреждающие риск. Деятельность по устранению последствий, по сути своей, не является направленной на поддержание безопасности.

Поэтому пользователь должен осознавать связь пользования устройством с угрозами такого использования, учитывая рост информационных рисков.

В большинстве полноценных сервисов пользователи используют учетные записи. Учетная запись используется для сохранения настроек, авторизации и для синхронизации между устройствами.

Рекомендуемой практикой является создание не менее двух учетных записей, одна из которых предоставляет права администратора, а другая – права обычного пользователя. При работе в условиях повышенного риска следует использовать запись с ограниченными правами. Даже если запись пользователя будет взломана, без прав администратора злоумышленник не сможет нанести серьезного вреда.

Также необходимо использовать разные учетные записи на разных устройствах и не синхронизировать их между собой, по крайней мере, в автоматическом режиме.

Между тем, пользователь должен предпринимать шаги на случай своей ошибки или на случай обхода злоумышленников мер безопасности, поэтому пользователю необходимо через определенные промежутки времени создавать резервные копии чувствительных данных и хранить их на нескомпрометированном устройстве в безопасном месте.

Принятие превентивных мер позволит существенно снизить уровень информационных угроз в обществе.

При использовании программных средств и Интернет-сервисов следует делать выбор в пользу тех, которые:

1. Не дискредитированы;
2. Запрашивают разрешение на минимальный набор персональных данных (либо не запрашивают вовсе);
3. Обладают средствами сквозного шифрования персональных данных в цифровом периметре и доказали эффективность этих средств исследованиями соответствующих органов и организаций;
4. Реализуют дополнительные меры защиты персональных данных (к примеру, не допуская их хранение или осуществляя удаление через короткое или определенное время) пользователей; а также допускающих подключение через защищенные протоколы связи;
5. Допускают удаление персональных данных автоматически или вручную (очистка истории посещений в браузере, удаление журнала использования программы и т.п.).

Аналогичными мерами можно воспользоваться и в реальной жизни:

- Пользоваться для общения помещениями и местами открытого пространства, исключающими несанкционированный сбор информации (отсутствуют посторонние лица, не установлены устройства сбора информации и т.п.);
- При общении через Интернет или телефонные сети указывать минимальное количество персональных данных.

Помнить о возможности посреднической атаки, при которой невидимый собеседник может быть скомпрометирован;

- При общении через Интернет или телефонные сети использовать кодовые фразы и прочие ассоциации с целевой информацией, предоставляя ее в открытом виде собеседнику только при личном контакте в безопасной контролируемой зоне;

- По возможности, не использовать физические объекты для хранения конфиденциальной информации (не хранить пароли на бумажных носителях на рабочем столе), либо хранить такие объекты в местах, исключающих доступ посторонних лиц (к примеру, сейфах);

- Удалять данные о себе, если необходимость в них отсутствует.

Описанные меры, хотя и не позволяют достичь стопроцентной гарантии безопасности цифрового и нецифрового присутствия, дают возможность уменьшить риск утечки персональных данных и нанесения потенциального ущерба субъекту персональных данных.

Список источников по разделу 2

1. Акмасова А.А., Информационно-психологическая безопасность личности [Электронный ресурс] // URL: http://www.bla.by/public/conf_2/1_2003.pdf (дата обращения 05.03.2024)

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2018. — 336 с. — (Высшее образование) [Электронный ресурс] // URL: https://publications.hse.ru/mirror/pubs/share/direct/218576514 (дата обращения: 05.03.2024).

3. Бритвин Н.И. Социальные сети как прообраз общественного устройства Власть. 2008. №1. Стр. 45-49 [электронный ресурс] // URL: https://cyberleninka.ru/article/n/sotsialnye-seti-kak-proobraz-obschestvennogo-ustroystva/viewer (дата обращения 10.04.2024)

4. Вихорев С.В., Классификация угроз информационной безопасности [Электронный ресурс] // URL: https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения 07.03.2024)

5. Владимирова Т.В. Сетевые коммуникации как источник информационных угроз [Электронный ресурс] // URL: http://ecsocman.hse.ru/data/2011/09/20/1267451215/Vladimirova.pdf (дата обращения 05.03.2024)

6. Горбатюк Я.С., Кибербуллинг как педагогическая проблема — Актуальные проблемы физической культуры и безопасности жизнедеятельности, Сборник научных трудов факультета физической культуры и безопасности жизнедеятельности. Под редакцией Л.В.

Кашицыной. Саратов, 2022, с. 53-57

7. ГОСТ Р 50922-96: «Защита информации. Основные термины и определения» (дата обращения 20.03.2024)

8. Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И.Ф.Кефели, Р.М.Юсупова. ИД «Петрополис», Санкт-Петербург, 2021. —300 с. 32 рис., 8 табл.

9. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2021. — 368 с.

10. Уголовный кодекс Российской Федерации от 13.06.1996 N 63- ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021)

11. Федеральный закон от 27.07.2006 N 152-ФЗ // Статья 7. Конфиденциальность персональных данных (ред. от 24.04.2020) «О персональных данных»

12. Федеральный закон от 30 декабря 2020 г. N 489-ФЗ «О молодежной политике в Российской Федерации»

13. Формирование готовности студенческой молодежи к противодействию вовлечению в киберэкстремистскую деятельность. [Текст] / Е.А. Гнатышина, Н.В. Уварина, В.А. Белевитин, Г.А. Диденко, Е.А. Гафарова // Педагогический журнал. — 2021. — № 11. — С. 174–189. — ISSN: 2223–5434

14. Черных А. И. Социология массовых коммуникаций: учебное пособие. М.: Изд. дом ГУ-ВШЭ, 2008 [электронный ресурс] // URL: https://publications.hse.ru/mirror/pubs/share/folder/ox5oymyz2c/direct/549271 00.pdf (дата обращения 15.03.2024)

Раздел 3 Формирование умений в области информационной безопасности

3.1 Характеристика существующей системы подготовки в области информационной безопасности студентов колледжа

Тенденции развития мирового сообщества свидетельствуют о возрастании потребностей в специалистах, владеющих новейшими информационными и коммуникационными технологиями, обладающих высокой информационной культурой и умеющих применять в своей профессиональной деятельности знания и навыки по обеспечению информационной безопасности.

По мере развития и углубления многомерных и многовекторных процессов, сопровождающих информатизацию современного общества, возрастает внимание к ее социальным и психологическим аспектам, связанным с необходимостью учета физического, психического и социального начал личности. Все это обусловливает внимание государства и общества к проблемам информационной безопасности, направленное на формирование нормативной базы, совершенствование системы защиты информации и системы защиты государственной тайны, углубление научных изысканий, организацию подготовки кадров в области информационной безопасности. В частности, по-прежнему актуальной остается задача «создания единой системы подготовки кадров в области информационной безопасности и информационных технологий», обеспечивающей не только подготовку квалифицированных специалистов в области

информационной безопасности и защиты информации, но и изучение проблематики информационной безопасности всеми другими категориями специалистов, подготавливаемых в системе профессионального образования.

На государственном уровне под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Для обеспечения национальных интересов в информационной сфере выделены четыре составляющих:

– гуманистическая, направленная на обеспечение конституционных прав и свобод личности, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма;

– политическая, включающая информационное обеспечение государственной политики по доведению достоверной информации до российской и международной общественности;

– технологическая, обеспечивающая развитие современных информационных технологий и отечественной индустрии информации;

– секьюритологическая, рассматривающая задачи защиты информационных ресурсов от несанкционированного доступа, обеспечения безопасности использования информационных и телекоммуникационных систем.

В соответствии с вышеперечисленными составляющими деятельности по обеспечению национальных интересов в информационной сфере группируются виды угроз информационной безопасности (ИБ).

Воздействию угроз ИБ РФ наиболее подвержены информационные и учетные автоматизированные системы, обеспечивающие деятельность общества и государства в различных сферах; системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности.

Таким образом, подготовка в области информационной безопасности и защиты информации для студентов важна и актуальна.

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.

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

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.

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.

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 том числе, на информационном праве, высокой информационной культуре.

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. рисунок 6). 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.

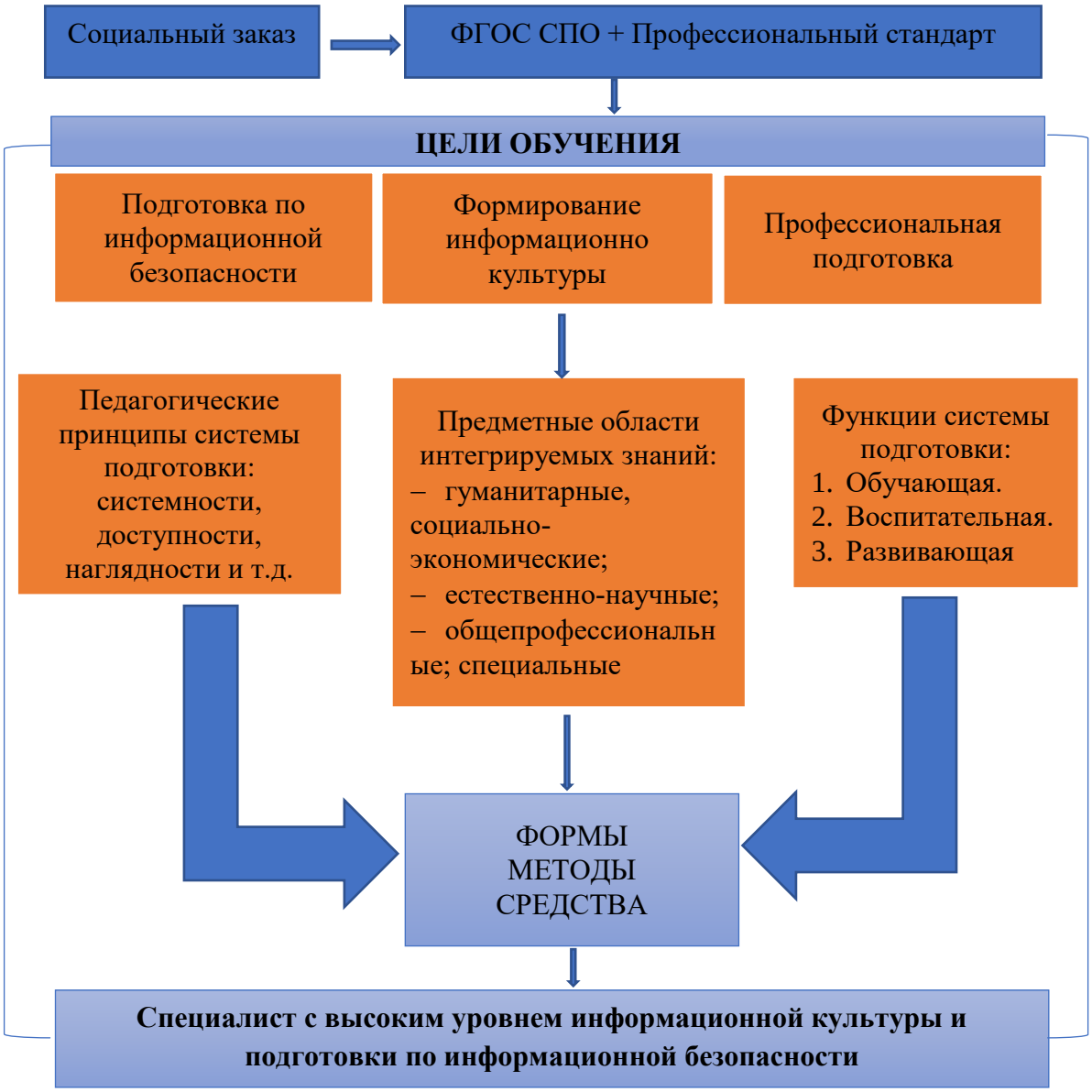

Рисунок 6 − Модель системы обучения основам информационной безопасности

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.

Таким образом, глубокое понимание проблематики информационной безопасности подготавливаемыми в системе среднего профессионального образования специалистами 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 и среднего профессионального образования дидактических единиц, объективно отражающих значимость и научный уровень решения этой проблемы, создания и укрепления внутридисциплинарных связей дисциплин информационного цикла и междисциплинарных связей с дисциплинами других разделов.

3.2. Содержательные линии информационной безопасности в дисциплинах информационного цикла

В качестве содержательных линий информационной безопасности в информационной подготовке, согласно педагогическому опыту, мы будем рассматривать структуру содержания обучения.

Содержание обучения рассматривается нами как системообразующий элемент в методической системе обучения информационной безопасности, компоненты которого не только соответствуют основным знаниям и умениям будущего специалиста в соответствии с его квалификационной характеристикой, указанной в соответствующем Федеральном государственном образовательном стандарте среднего профессионального образования, но и отвечает за наполнение каждого из них конкретными понятиями согласно содержательным линиям обучения, которые, в свою очередь, предопределяют

основные разделы содержания обучения, реализуют основную доминанту в обучении и позволяют, согласно этой доминанте, выстраивать изложение учебного материала, а также изучение базовых понятий и всего цикла учебных дисциплин в рамках, например, предметной или специальной подготовки обучающихся.

Как уже отмечалось выше, информационная подготовка студентов должна строиться в соответствии с профессиональными требованиями, отраженными в соответствующих профилю и направлению подготовки Федеральных государственных образовательных стандартах и профессиональных стандартах.

Особую остроту приобретает гуманистическая составляющая проблемы информационной безопасности, предполагающая при подготовке специалистов решение задач «защиты от информации», адекватного гражданского воспитания, основанного, в том числе, на информационном праве, высокой информационной культуры.

Компонентами системы обучения основам информационной безопасности являются цели и ожидаемые результаты обучения, содержание обучения и методическое обеспечение, включающее методы, организационные формы и средства обучения.

В свою очередь, компонентами содержания обучения по информационной безопасности выступают знания, накопленные в этой предметной области (научно обоснованные факты, дефиниции, законы и закономерности, гипотезы и теории), опыт осуществления способов деятельности по обеспечению информационной безопасности и защиты информации.

Содержание подготовки будет определяться соответствующими содержательными линиями.

Структурно детерминированная модель содержания обучения основам информационной безопасности может быть построена на основе системного анализа основных объектов предметной области будущей профессиональной деятельности обучающихся, соотнесенных с матрицей опасностей и угроз для выявленных информационных процессов. Результатом такого анализа должно стать выявление базовых объектов изучения, их взаимосвязей (процессов взаимодействия), методов и технологии их изучения.

Для углубления знаний и навыков в области информационной безопасности в рамках дисциплин «Информатика» и «Информационные технологии в профессиональной деятельности» необходимо, с учетом интегративного подхода, использовать имеющиеся внутрипредметные связи, прослеживаемые между традиционными разделами информатики и проблематикой информационной безопасности, акцентируя внимание на таких вопросах, как безопасность операционных систем, безопасность офисных приложений, безопасность в базах данных, безопасность при работе в локальных и глобальных сетях и т.п. (таблица 3).

Таблица 3- Вопросы информационной безопасности в дисциплинах информационного цикла

№ п/п	Темы дисциплин информационного цикла	Вопросы информационной безопасности
	Операционные системы	Средства обеспечения информационной безопасности (идентификация и аутентификация, профили пользователей, разрешение доступа к папкам и файлам, передача прав владения, шифрующие файловые системы, использование служебных программ, групповых политик, сертификатов, средств мониторинга системы)
	Офисные приложения	Доступ к файлам по паролю, открытие документов по паролю или только для чтения, защита книги, листа, ячейки, раздела документа от изменений, использование шаблонов, шифрование баз данных, использование цифровой подписи
	Работа в Интернет	Настройки безопасности, настройки браузеров, защита от спама, использование антивирусных средств, операции с цифровой подписью
	Информационные системы	Меры обеспечения информационной безопасности при работе с профессиональными информационными системами

Несмотря на жесткие временные рамки реализации учебных планов по информатике и информационным технологиям, тематика информационной безопасности должна найти в нем соответствующее ее значимости место в подготовке обучающихся, в том числе и с учетом резервов самостоятельной работы студентов. При этом качество подготовки может быть улучшено за счет более эффективного использования внутрипредметных связей.

При подготовке в области обеспечения информационной безопасности также должны эффективно использоваться межпредметные связи, устанавливающие корреляцию дисциплин информационного цикла с другими областями:

1) в области общих гуманитарных и социально-экономических дисциплин – философия, социология, политология, культурология, право (для освещения роли и значения информации и информационных ресурсов в современном обществе, в том числе для обеспечения прав и свобод личности, важности их гуманитарного, морально-этического, культурологического, правового аспектов);

2) в области общих математических и естественнонаучных дисциплин – математика и ее приложения (для освещения вопросов о применении математических методов преобразования данных с целью их защиты);

3) в области общепрофессиональных и специальных дисциплин должны найти адекватное отражение аспекты безопасности хозяйственной деятельности в электронной среде.

Для укрепления межпредметных связей в состав изучаемых дисциплин могут быть включены дисциплины, конкретизирующие и углубляющие такое взаимодействие. Учебная дисциплина «Основы информационной безопасности» как системообразующий элемент подготовки по информационной безопасности. Несмотря на междисциплинарный характер проблемы информационной безопасности, в состав изучаемых курсов должна быть включена дисциплина «Основы информационной безопасности», главная

цель которой – повышение эффективности подготовки специалистов по обеспечению информационной безопасности при использовании ИКТ в сфере профессиональной деятельности.

Наряду с традиционно рассматриваемыми аспектами ИБ и защиты информации в ней должны найти отражение методологические, социально-философские, культурологические, правовые, организационно-управленческие аспекты информационной безопасности.

Данная учебная дисциплина должна дать обучаемым комплекс сведений о современном состоянии проблемы обеспечения информационной безопасности применительно к сфере будущей деятельности подготавливаемого специалиста, существующих угрозах, видах обеспечения ИБ, методах и средствах защиты информации, основах построения систем защиты. Особое место должны занимать правовой и морально-этический аспекты обеспечения информационной безопасности. В утвержденных Министерством образования РФ примерных Федеральных образовательных государственных стандартах по дисциплине «Информационные технологии профессиональной деятельности» для раздела «Основные угрозы и методы обеспечения информационной безопасности» дидактические единицы могут быть сведены в три основные группы, ориентированные на различные аспекты ИБ, что вполне корреспондирует с положениями Доктрины информационной безопасности РФ (таблица 4).

Таблица 4 − Аспекты ИБ в подготовке студентов колледжа

Социальные аспекты	*Правовые аспекты*	*Технологические и секьюритологические аспекты*
1.Информационная структура РФ 2.Информационная безопасность и ее составляющие 3. Угрозы безопасности информации и их классификация 4.Основные виды защищаемой информации 5.Проблемы информационной безопасности в мировом сообществе	1. Законодательные и иные правовые акты РФ, регулирующие правовые отношения в сфере информационной безопасности и защиты государственной тайны 2. Система органов обеспечения ИБ в РФ 3. Административно-правовая и уголовная ответственность в информационной сфере	1. Защита от несанкционированного вмешательства в информационные процессы 2. Организационные меры, инженерно-технические и иные методы защиты информации, в том числе сведений, составляющих государственную тайну 3. Защита информации в сетях, антивирусная защита 4. Специфика обработки конфиденциальной информации в компьютерных системах

Такая декомпозиция позволяет сформировать и наполнить подготовку в области информационной безопасности прежде всего социальным содержанием, поскольку именно социальные аспекты информационной безопасности носят гносеологический основополагающий характер. Их изучение позволяет выявить значимость проблемы ИБ как на цивилизационном, так и на личностном уровне в полном соответствии с гуманитарной составляющей информационной безопасности.

В результате изучения учебных вопросов этого блока обучаемые должны знать суть проблемы обеспечения

информационной безопасности и ее особенности, основные угрозы для информационных ресурсов во всех социально значимых областях человеческой деятельности, роль человеческого фактора в решении задач обеспечения информационной безопасности. Именно люди составляют наиболее уязвимый «компонент» информационных ресурсов и представляют наибольшую опасность для них как в корпоративной среде, так и при индивидуальном использовании информационных и коммуникационных технологий. Поэтому среди направлений решения проблемы информационной безопасности, таких, как создание безопасных операционных систем и приложений, улучшение средств защиты, совершенствование законодательной базы, – важную роль играет система просвещения (образования).

В контексте информационной безопасности должны быть рассмотрены проблемы компьютерной этики, возникающие в связи с отсутствием ясности в вопросах о том, каковы же этические ограничения при применении компьютерных технологий. Одним из основных результатов изучения социальных аспектов информационной безопасности должно быть осознание обучаемыми того обстоятельства, что безопасность информационных систем и технологий не является их врожденным, эмерджентным свойством, а является следствием диалектического взаимодействия деструктивных факторов (угроз и опасностей различной этимологии) и механизмов комплексной системы защиты информации, обеспечивающей их предотвращение, блокирование, устранение, минимизацию рисков.

Обязательным компонентом подготовки по информационной безопасности является изучение основ ее правового обеспечения. В числе задач, решаемых государством в сфере обеспечения информационной безопасности, является интенсивное развитие правового регулирования отношений в области противодействия угрозам; закрепляются приоритетные интересы в информационной сфере, чему способствует принятие соответствующих законодательных актов. Это предопределяет обязательность изучения основ правового обеспечения информационной безопасности, содержательным наполнением которого должно стать представление о сложностях правового регулирования отношений в информационной сфере, обусловленных самим понятием «информация», отсутствием единства его толкования в юриспруденции. В контексте информационного права должны изучаться аспекты информационной безопасности в системе национальной и экономической безопасности страны, соответствующие конституционные нормы и правовые акты, а также уровни правового регулирования в области информационной безопасности.

В рамках изучения технологических и секьюритологических аспектов обеспечения информационной безопасности компьютерных систем и технологий предметом изучения должны стать принципы и содержание организационного обеспечения информационной безопасности (политика безопасности, контроль, разграничение и ограничение доступа к информационным ресурсам); принципы создания комплексных систем защиты

информации; методы и средства обеспечения информационной безопасности (аутентификация и идентификация пользователей и технических средств, организация защиты информации в персональных компьютерах, криптографическое преобразование информации и электронная подпись); особенности защиты информации в базах данных и в сетях телекоммуникаций; основы компьютерной вирусологии, методы и средства защиты от компьютерных вирусов и вредоносных программ; требования к пользователям и рекомендации по обеспечению личной информационной безопасности.

Для углубления знаний и навыков в области информационной безопасности в рамках дисциплин «Информатика» и «Информационные технологии в профессиональной деятельности» необходимо, с учетом интегративного подхода, использовать имеющиеся внутрипредметные связи, прослеживаемые между традиционными разделами информатики и проблематикой информационной безопасности, акцентируя внимание на таких вопросах, как безопасность операционных систем и офисных приложений, безопасность в базах данных, безопасность при работе в локальных и глобальных сетях и т.п.

При этом качество подготовки может быть улучшено за счет более эффективного использования внутрипредметных связей. Основным в построении «технологического блока» является его структуризация и такой отбор содержания, который обеспечил бы понимание обучаемыми того обстоятельства, что, несмотря на множество опасностей и угроз, возможно поддержание

необходимого и достаточного уровня информационной безопасности и минимизации рисков при соответствующей организации, вложении средств и уровне подготовки пользователей.

Одним из важных направлений развития системы обучения является разработка деятельностного компонента содержания, т.е. включения в обязательный минимум содержания образования специально отобранных способов деятельности, техник и технологий, ключевых компетенций и иных процедурных элементов, которыми необходимо овладеть обучающимся.

3.3. Состав и структура дисциплины «Информационная безопасность»

Для разработки электронного педагогического практикума необходимо провести анализ учебно-программной документации и учебного материала дисциплины «Информационная безопасность» с целью получения следующих результатов:

– выявление тематического содержания дисциплин (разделов) для определения количества тестов текущего контроля – каждый тест текущего контроля на каждый раздел + итоговый (выходной) тест по всем разделам дисциплины.

– определении количества учебных единиц и их содержание в дисциплине и их разделение по разделам для формулирования заданий тестов.

Дополнительно анализ учебно-программной документации позволит определить: место дисциплины в структуре программы

подготовки специалиста среднего звена, цели, задачи и требования к результатам обучения; объем и виды учебной работы обучающихся.

Основной дисциплиной, формирующей первоначальную общепрофессиональную базу в области информационной безопасности будущего техника-программиста (09.02.07 Информационные системы и программирование), является дисциплина «Информационная безопасность» на освоение которой выделено 128 часов, распределённых на комбинированные лекционные занятия, практические занятия и самостоятельную организованную деятельность студентов.

Целью дисциплины в общепрофессиональном цикле является формирования у обучающихся базовых и основополагающих понятий и навыков в области информационной безопасности и комплексного подхода к защите информации в автоматизированной системе и на объектах информатизации.

В результате освоения учебной дисциплины обучающийся должен обладать общими компетенциями, включающими в себя практические умения и знания, представленные в таблице 5.

Таблица 5 - Целевые знания и умения при изучении дисциплины «Информационная безопасность»

Знания и умения	Описание
Практические умения	– применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности; – выявлять основные угрозы информационной безопасности; – производить установку и настройку типовых программных средств защиты информации; – обеспечивать антивирусную защиту; – фильтровать сетевые пакеты межсетевым экраном; – использовать типовые криптографические средства и методы защиты информации, в том числе электронную цифровую подпись; – выполнять операции резервного копирования и восстановления данных.
Знания	– сущность и понятие информационной безопасности, характеристику её составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды угроз информационной безопасности; – основные положения комплексного подхода к защите информации; – основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ и ФСТЭК РФ в данной области; – принципы архитектурной безопасности; – современные программно-технические средства обеспечения информационной безопасности; – виды систем идентификации и аутентификации; – типовые модели управления доступом; – типовые средства и методы ведения аудита; – основные понятия криптографии; – типовые криптографические алгоритмы, применяемые для защиты информации; – типовые методы скрытия информации; – методы резервного копирования данных.

Для получения соответствующих знаний и умений по дисциплине комбинированные, лекционные, практические и самостоятельные занятия при разработке рабочей программы предлагаем разбить на несколько разделов, представленных в таблице 6.

Таблица 6 – Содержания разделов по целевым знаниям и умениям дисциплины «Информационная безопасность»

Разделы дисциплины	Содержание разделов и типы занятий	
Раздел 1. Основы информационной безопасности (ИБ)		
Тема 1.1. Понятие и основные составляющие ИБ	Содержание учебного материала	
	1	*Сущность и понятие ИБ*
	2	*Место ИБ в системе национальной безопасности страны. Составляющие ИБ*
	Практические занятия 1. Анализ примеров нарушений ИБ. Выявление значимых составляющих ИБ и характеристик ИС в конкретных ситуациях.	
Тема 1.2. Виды угроз ИБ	Содержание учебного материала	
	1	*Понятие угрозы*
	2	*Угрозы нарушения конфиденциальности*
	3	*Угрозы нарушения целостности.*
	4	*Угрозы нарушения доступности.*
	Практические занятия 1. Решение ситуационных задач: выявление угроз ИБ в конкретных ситуациях. Демонстрация подлога при разрешении символьного имени в IP-адрес путём модификации файла hosts. Изложение схемы атаки на отказ в обслуживании (атаки SYN-шторм, ICMP-шторм).	
	Самостоятельная работа обучающихся 1. Создание описания одного из методов фишинга, оценка угрозы и разработка рекомендаций по её предотвращению. 2. Решение задачи на обнаружение и исправление в программном коде ошибки, способной привести к	

	успешному выполнению SQL-инъекции. 3. Решение задачи на обнаружение и исправление в программном коде ошибки типа «переполнение буфера».	
Тема 1.3. Вредоносное программное обеспечение (ПО)	Содержание учебного материала	
	1	*Понятие вредоносного ПО и каналы его распространения*
	2	*Классификация вредоносного ПО*
	3	*Классификация вредоносного ПО*
	4	*Признаки заражения компьютера вредоносным ПО*
	5	*Принципы работы антивирусного ПО*
	Практические занятия 1. Определение функциональных возможностей и принципов работы троянской программы на примере клавиатурного шпиона. 2. Выполнение проверки компьютера на наличие признаков заражения вредоносным ПО: исследование настроек браузера, запущенных процессов, элементов автозапуска, сетевой активности. 3. Обоснование применения норм уголовного права в конкретных ситуациях, связанных с созданием и использованием вредоносного ПО. 4. Выполнение установки антивирусного ПО. Обоснование выбора устанавливаемых компонентов. Обновление антивирусных баз. Выполнение настройки параметров антивирусной и проактивной защиты. Настройка уведомлений. Выполнение антивирусного сканирования с заданными параметрами	
	Контрольные работы	
	Самостоятельная работа обучающихся 1. Создание отчёта о возможностях клавиатурного шпиона и методах защиты от него. 2. Создание конспекта по статьям УК РФ, предусматривающих ответственность за действия, связанные с созданием и использованием вредоносного ПО. 3. Создание отчёта о настройке и результатах антивирусного сканирования.	
Раздел 2. Организационно-правовое обеспечение ИБ		
Тема 2.1. Правовые основы	Содержание учебного материала	
	1	*Структура правового обеспечения ИБ*
	2	*Классификация информации по видам тайн.*

обеспечения ИБ		*Защита прав собственности на информацию*
	Практические занятия 1. Решение ситуационных задач: нахождение применимых правовых норм в заданных условиях.	
	Самостоятельная работа обучающихся 1. Определение возможности ограничения доступа к информации и порядка защиты информации на основании ФЗ «Об информации, информационных технологиях и защите информации» 2. Определение состава персональных данных на основании ФЗ «О персональных данных». 3. Определение сведений, которые не могут быть отнесены к коммерческой тайне на основании ФЗ «О коммерческой тайне».	
Тема 2.2. Оценочные стандарты и технические спецификации в области ИБ	Содержание учебного материала	
	1	*«Оранжевая книга».*
	2	*ИБ распределённых систем. Рекомендации X.800*
	3	*«Общие критерии». Стандарт ISO/IEC 15408*
	4	*Управление ИБ. Серия стандартов ISO/IEC 27000*
	5	*Руководящие документы ФСТЭК (Гостехкомиссии) и ФСБ*
	6	*Спецификации RFC*
	Практические занятия 1. Изложение практических рекомендаций по управлению ИБ по отношению к одному из сервисов безопасности, описанных в ГОСТ Р 17799-2005. 2. Определение класса ИС персональных данных (ИСПДн) для ИС гипотетической организации в соответствии с совместным приказом ФСТЭК, ФСБ и Мининформсвязи РФ № 55/86/20 от 13 февраля 2008 г. 3. Выполнение оценки исходной степени защищённости ИСПДн, выделение актуальных угроз безопасности в соответствии с «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн».	
	Самостоятельная работа обучающихся 1. Создание предварительного перечня угроз ИБ для ИС гипотетической организации на основе описания наиболее часто реализуемых сетевых угроз и типовых моделях угроз согласно «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн». 2. Определение недостатков предложенной модели угроз для ИС гипотетической организации.	
Тема 2.3. Организационные методы и	Содержание учебного материала	
	1	Административный уровень ИБ
	2	Процедурный уровень ИБ

средства обеспечения ИБ	Практические занятия 1. Решение ситуационных задач: разработка и обоснование программы безопасности для различных видов ИС гипотетической организации.	
	Самостоятельная работа обучающихся 1. Планирование восстановительных работ на основе предложенной модели угроз для ИС гипотетической организации.	
Раздел 3. Программно-технические средства обеспечения ИБ		
Тема 3.1. Принципы обеспечения ИБ на программно-техническом уровне	Содержание учебного материала	
	1	*Основные понятия программно-технического уровня ИБ*
	2	*Принципы архитектурной безопасности*
	Практические занятия 1. Решение ситуационных задач: обоснование применения принципов архитектурной безопасности в заданных условиях.	
Тема 3.2. Средства обеспечения конфиденциальности	Содержание учебного материала	
	1	*Построение систем защиты от угроз нарушения конфиденциальности*
	2	*Идентификация и аутентификация*
	3	*Управление доступом*
	4	*Протоколирование и аудит*
	5	*Симметричное и асимметричное шифрование*
	6	*Скрытие информации (стеганография)*
	7	*Экранирование и анализ защищённости*
	8	*Туннелирование*
	Практические занятия 1. Создание пользователей и групп в операционной системе (ОС) Windows. Решение задач поиска и сброса паролей пользователей. 2. Выполнение настройки системы парольной защиты в локальной политике безопасности ОС Windows. 3. Создание списков контроля доступа и назначение прав доступа на уровне файловой системы NTFS в заданных условиях. 4. Выполнение настройки параметров аудита в ОС Windows в заданных условиях. Получение и интерпретация результатов аудита. 5. Выполнение установки ПО для работы с инфраструктурой открытых ключей. Создание открытого и	

	закрытого криптографических ключей. 6. Выполнение установки ПО для стеганографического преобразования. Выполнение операций по скрытию и обмену скрытой информацией. 7. Выполнение установки сетевого сканера. Определение списка открытых портов в ОС Windows при помощи сетевого сканера. 8. Выполнение настройки межсетевого экрана: создание правил фильтрации пакетов для предотвращения доступа к внутренним сервисам. 9. Выполнение настройки межсетевого экрана: создание правил фильтрации пакетов для предотвращения доступа к внутренним сервисам.	
	Самостоятельная работа обучающихся 1. Проектирование системы групп пользователей в ОС Windows. 2. Создание перечня рекомендаций по выбору паролей и практической реализации парольных систем. 3. Решение задачи по оценке стойкости пароля ко взлому. 4. Создание отчёта по результатам поиска паролей пользователей и настройки системы парольной защиты. 5. Создание отчёта по результатам назначения прав доступа на уровне файловой системы NTFS. 6. Изложение функциональных возможностей одной из существующих систем обнаружения (предотвращения) вторжений. 7. Создание отчёта по результатам работы с инфраструктурой открытых ключей. 8. Создание отчёта по результатам стеганографического преобразования информации. 9. Создание перечня стандартных служб и портов в ОС Windows. Создание перечня рекомендаций по ограничению доступа к стандартным службам за счёт фильтрации пакетов. 10. Создание отчёта по результатам анализа защищённости при помощи сетевого сканера и настройки межсетевого экрана.	
Тема 3.3. Средства обеспечения целостности	Содержание учебного материала	
	1	*Построение систем защиты от угроз нарушения целостности*
	2	*Криптографические хеш-функции*
	3	*Электронная цифровая подпись (ЭЦП)*
	Практические занятия 1. Установка ПО для расчёта хешей. Определение целостности файла при помощи хеш-функций MD5 и SHA-1. 2. Выполнение операций по обмену открытыми	

<table>
<tr><td></td><td colspan="2">ключами через инфраструктуру открытых ключей, отправке и получению зашифрованных и подписанных ЭЦП документов.</td></tr>
<tr><td></td><td colspan="2">Самостоятельная работа обучающихся
1. Определение сведений, которые должен содержать сертификат ключа подписи, на основании ФЗ «Об электронной цифровой подписи».
2. Определение условий, при которых ЭЦП в электронном документе равнозначна собственноручной подписи в бумажном документе, на основании ФЗ «Об электронной цифровой подписи».
3. Создание отчёта по работе с зашифрованными и подписанными ЭЦП документами.</td></tr>
<tr><td rowspan="5">Тема 3.4. Средства обеспечения доступности</td><td colspan="2">Содержание учебного материала</td></tr>
<tr><td>1</td><td>Задача обеспечения высокой доступности</td></tr>
<tr><td>2</td><td>Построение систем защиты от угроз нарушения доступности</td></tr>
<tr><td>3</td><td>Управление информационными сервисами и сервисами безопасности</td></tr>
<tr><td colspan="2">Практические занятия
1. Выполнение настройки параметров резервного копирования дисков в соответствии с разработанным планом. Выполнение резервного копирования и восстановления данных.
2. Создание программного RAID-массива типа «зеркало». Выполнение замеров производительности и тестирование отказа одного из элементов RAID-массива.</td></tr>
<tr><td colspan="2">Контрольные работы</td></tr>
<tr><td colspan="2">Самостоятельная работа обучающихся
1. Разработка плана резервного копирования дисков на основе информации о характере их использования.
2. Создание отчёта о результатах резервного копирования и восстановления данных.
3. Создание отчёта о результатах настройки и работы программного RAID-массива.</td></tr>
</table>

Подобная структура позволит студентам получить базовые знания в различных областях ИБ изучить основные принципы и методы защиты информации в организациях различного типа, развить при выполнении лабораторных работ практические навыки по составлению модели угроз, расчету и анализу информационных

рисков, выбору рационального состава средств защиты. Кроме того, студенты смогут ориентироваться во множество правовой, нормативно-методической документации и стандартах в области ИБ. Это особенно актуально сейчас, в связи с выпуском новых версий стандартов в области информационной и комплексной безопасности, внесением поправок и изменений в ФЗ № 149 «Об информации, информационных технологиях и защите информации», вводом новой версии Доктрины информационной безопасности.

Полученные знания и отработанные в ходе выполнения практических работ умения позволят успешно сформировать у студентов ряд общекультурных и профессиональных компетенции предусмотренных ФГОС по данной специальности.

Практические задания по разделу 3.

Задание 3.1. Подготовьтесь к семинарскому занятию, ответьте на контрольные вопросы:

- Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?
- Перечислите основные критерии оценки надежности: политика безопасности и гарантированность образовательной организации.
- Понятия коммерческой тайны, служебной тайны и банковской тайны: приведите примеры и укажите возможные семантическое пересечения названных понятий.
- Каковы основные конституционные гарантии по охране и

защите прав и свобод в информационной сфере?

- Найдите понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации?
- В чем состоит уязвимость информации в автоматизированных системах обработки данных?

Задание 3.2. Составьте тестовые задания по одной из тем дисциплины по информационной безопасности Подберите материал к любой из тем, структурируйте материал по логическим блокам. По каждому логическому блоку составьте тестовые задания: не менее восьми заданий закрытого типа нескольких разновидностей, не менее четырех заданий открытого типа нескольких разновидностей. Распределите задания по уровню сложности. Составьте эталон правильных ответов. Разработайте критерии оценивания теста.

Задание 3.3. проведите декомпозицию профессиональной компетенции техника по защите информации, выделив компоненты знаний, умений и владений (опыта).

Список источников по разделу 3

1. Белов Е.Б. Образование в области информационной безопасности: принципы совершенствования подготовки кадров / Е.Б. Белов, В.П. Лось // Информация и связь. − 2012. − №2. −С. 94-96.

2. Богатырева Ю.И. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: автореф. дисс. … докт. пед. наук: 13.00.08 / Богатырева Юлия Игоревна. – Тула, 2014. – 42 с.

3. Гафарова Е. А. К вопросу актуализации содержания образования магистерских программ по направлению «Информационная безопасность» / Е. А. Гафарова, О. Н. Шварцкоп // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы : Сборник научных трудов, Челябинск, 13–30 января 2017 года. – Челябинск: Челябинский филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», 2017. – С. 43-49.

4. Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. N 646. – URL: http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (дата обращения: 03.03.2024).

5. Оладько В. С. Состав и структура дисциплины основы информационной безопасности [Текст] // Образование: прошлое, настоящее и будущее: материалы II Междунар. науч. конф. (г. Краснодар, февраль 2017 г.). — Краснодар: Новация, 2017. − С. 79-83. − URL https://moluch.ru/conf/ped/archive/211/11708/ (дата обращения: 02.03.2024).

6. Поляков В. П. Методическая система обучения информационной безопасности студентов вузов: диссертация ... доктора педагогических наук : 13.00.08 / Волж. гос. инж.-пед. ун-т.- Нижний Новгород, 2006.- 538 с.

7. Поляков В. П. О системе обучения студентов основам информационной безопасности // Финансы: Теория и Практика. 2006. №3. URL: https://cyberleninka.ru/article/n/o-sisteme-obucheniya-studentov-osnovam-informatsionnoy-bezopasnosti (дата обращения: 02.03.2024).

8. Свидетельство о государственной регистрации программы для ЭВМ № 2019664212 Российская Федерация. Электронный практикум по дисциплине «Информационная безопасность»: № 2019662986: заявл. 21.10.2019 : опубл. 01.11.2019 / О. Н. Шварцкоп; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный гуманитарно-педагогический университет» (ФГБОУ ВО «ЮУрГГПУ»).

9. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.07 Информационные системы и

программирование. – Доступ из СПС Гарант (дата обращения: 05.07.2022). – Текст: электронный.

10. Шварцкоп О. Н. Информационная безопасность в профессиональном образовании: УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ / О. Н. Шварцкоп, Ф. Х. Хабибуллин. – Челябинск: ЗАО "Библиотека А. Миллера", 2020. – 77 с. – ISBN 978-5-93162-403-7.

11. Шварцкоп, О. Н. Формирование профессиональных умений в области информационной безопасности как обязательный элемент подготовки студентов-бакалавров педагогического вуза / О. Н. Шварцкоп // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы : Сборник научных трудов Девятой Международной научно-практической конференции, Челябинск, 30 января 2018 года. – Челябинск: Челябинский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», 2018. – С. 177-184.

Раздел 4 Формирование готовности обучающихся к противодействию вовлечения в киберэкстремистскую деятельность

Сегодня проблема экстремизма затронула многие страны, в том числе Российскую Федерацию. Экстремизм выступает дестабилизирующим фактором, угрожающим национальной безопасности, целостности государства и охватывает практически все сферы общественной жизни, например, политику, культуру, межнациональные и меконфессиональные отношения.

Согласно Федеральному закону «О противодействии экстремистской деятельности» под экстремизмом понимается насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; публичное оправдание терроризма и иная террористическая деятельность, возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения.

А.С. Доколин выделяет следующие виды экстремизма: религиозный, политический, националистический, экономический, культурологический, экологический, технологический, информационный.

Религиозный экстремизм - экстремизм в религиозной сфере, связанный с неприятием идей других религиозных конфессий, агрессивным отношением к иноверцам, пропаганде незыблемости, «истинности» одного вероучения. Религиозный экстремизм следует рассматривать как крайнюю форму религиозного фанатизма.

Политический экстремизм – это экстремизм в политической сфере, нацеленный на радикальное изменение государственного строя и существующего политического режима.

Националистический экстремизм – экстремизм в сфере межнациональных отношений, основанный на мотивах национальной или расовой ненависти и вражды. Экономический экстремизм – экстремизм в сфере экономических отношений, направлен на ликвидацию конкуренции в предпринимательской деятельности путем применения противоправных действий.

Культурологический экстремизм – экстремизм в области культуры, основан на изоляции одной культуры от остальных. Выражается в уничтожении исторических памятников, являющихся национальным достоянием, и другими противоправными действиями в данной области.

Экологический экстремизм – экстремизм в области экологии, который направлен против государственной природоохранительной политики и научно-технического прогресса в этой сфере.

Технологический экстремизм – это экстремизм, направленный на использование или угрозу использования ядерного, химического или бактериологического оружия, радиоактивных и высокотоксичных химических и биологических веществ, а также захват ядерных или иных промышленных объектов, представляющих повышенную опасность для жизни и здоровья людей, ради достижения политических целей.

Остановимся более подробно на информационном экстремизме. Согласно мнению А.С. Доколина, под информационным экстремизмом следует понимать экстремизм в сфере распространения информации. Данный вид экстремизма предполагает предоставление искаженной недостоверной информации с помощью различных информационных технологий. К подвиду информационного экстремизма относят киберэкстремизм, как экстремизм распространяющийся только в сети Интернет посредством персональных компьютеров, мобильных телефонов, планшетов и др. С помощью таких устройств в социальных сетях, через почтовую рассылку, мобильные приложения осуществляется завуалированная и открытая Интернет-пропаганда крайних взглядов и идей. Социальная сеть представляет собой онлайн-сервис, веб-сайт, предназначенный для организации социальных взаимоотношений группы людей на одном сайте в Интернете, где каждый пользователь имеет возможность загружать свой контент и обмениваться им с другими людьми из группы.

Таким образом, киберэкстремизм – это приверженность к крайним взглядам, идеям и действиям, направленных на распространение принципов нетерпимости с использованием совокупности различных средств и методов сбора, обработки и передачи информации в киберпространстве.

С помощью сети Интернет экстремистские группы получили возможность отстаивать свою идеологию, вступать в дискуссии, спорить. Численность аудитории в данных группах достигает огромных показателей, при этом сами экстремисты могут оставаться незамеченными. Подобные ресурсы оказывают большое воздействие на сознание людей и трудно контролируемы со стороны государства и общественных институтов. В результате в ряды экстремистов попадают новые последователи идей крайних взглядов. С каждым годом увеличивается количество молодежи, вступающей в ряды экстремистских организаций, причем большинство попадает в экстремистские сети случайно, которые в силу психологических и возрастных особенностей еще осознают реальных последствий своих действий. Социальные сети в данном случае применяются для распространения информации экстремистского толка для определенной возрастной группы пользователей. Средний возраст более половины подписчиков сайтов, пропагандирующих религиозный фундаментализм, составляет молодые люди до 18 лет. Молодежь данной возрастной группы легко поддаются продвижению идей религиозного экстремизма из-за своей внушаемости.

По мнению Любина С.Ю., Яценко О.А.: «Молодежь в силу возрастной психологии наиболее подвержена манипулированию и склонна к принятию протестных идей и настроений. Энергия и стремления молодых людей часто становятся предметом политических спекуляций и поэтому молодежь наиболее привлекательна для вербовки во всевозможные группы и организации экстремистского толка».

К числу причин возникновения экстремистского настроения среди молодежи можно отнести политические, социально-экономические и культурно-воспитательные проблемы нашего общества. Отмечаются факты распада моральных устоев, сплоченности народов России, мировоззренческих ориентиров, стратегических жизненных целей. Отрицание традиционных духовных ценностей молодежью, кризис нравственности и морали приводят к тому, что молодые люди из добропорядочных граждан становятся сторонниками крайних взглядов.

Сталкиваясь с трудностями, неизбежно возникающими вследствие мнимых или подлинных неурядиц личной и общественной жизни, благопристойный член общества впадает в состояние внутренней подавленности, сопровождаемое гневом, раздражением и недовольством. В результате молодые люди переносят из киберпространства в реальную жизнь насильственные действия.

Чтобы устранить проблему киберэкстремизма среди молодежи, необходимо выработать соотносимые с текущими тенденциями развития информационно-коммуникативных

технологий, профилактико-воспитательные меры противодействия идеям экстремизма.

Готовность обучающихся к противодействию вовлечения в киберэкстремистскую деятельность будем понимать «сложное, динамично развивающееся качество личности студента, проявляющееся на субъективном уровне в виде системы, которая, интегрируя в себе когнитивно-целевой, процессуально-рефлексивный и аксиологический компоненты, обеспечивает ему противодействие вовлечения в киберэкстремистскую деятельность на основе осознанного понимания опасности киберэкстремизма, адекватной оценки ситуации и выбор поведения при работе с информацией экстремистского толка в киберпространстве.

С целью формирования готовности студентов колледжа к противодействию вовлечения в киберэкстремистскую деятельность нами была адаптирована, обоснована и реализована структурно-функциональная модель формирования готовности студентов колледжа к противодействию вовлечения в киберэкстремистскую деятельность.

За основу модели была взяты структурные (нормативно-целевой блок, методологический, содержательно-процессуальный, оценочно-результативный) и функциональные компоненты (функции педагога, функции готовности студентов к противодействию вовлечения в киберэкстремистскую деятельность) модели формирования готовности студентов вуза к противодействию вовлечения в киберэкстремистскую деятельность, выделенные А. С. Доколиным.

Выделенные компоненты были нами адаптированы для условий подготовки студентов колледжа, а содержательно-процессуальный блок модели наполнен авторским содержанием в соответствии с целью исследования.

Содержательно-процессуальный блок содержит комплекс педагогических условий и педагогическое обеспечение, представленное когнитивным, деятельностным и методическим компонентами, функциями педагога (информационной, мотивационно-сопроводительной, консультационной) и функциями студентов колледжа в противодействии вовлечения в киберэкстремистскую деятельность (адаптации, самоопределения, самореализации).

В состав содержательно-процессуального блока мы включили следующий комплекс педагогических условий: рефлексивно-ценностное сопровождение студентов при анализе ситуаций и выполнении заданий по информационной безопасности в киберпространстве; формирование системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения в учебной и внеучебной деятельности; включение в проектные задания по дисциплинам информационного цикла в качестве содержательного контента информации юридического, технологического и акмеологического направлений профилактики киберэкстремизма.

Выделенные педагогические условия образуют комплекс, так как они взаимосвязаны, объединены общей целью, взаимно

дополняют друг друга в совокупности и позволяют обеспечить готовность обучающихся колледжа к противодействию вовлечению в киберэкстремистскую деятельность, поскольку каждое из условий способствует формированию компонентов (аксиологического, процессуально-рефлексивного и когнитивно-целевого) системы готовности. На основе системно-процессного, аксиологического, личностно-деятельностного, рефлексивного подходов, анализа психолого-педагогической, методической литературы по теме исследования нами разработана методика реализации педагогических условий формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность. В структуре методики мы выделили совокупность взаимосвязанных компонентов: целевого, содержательного, процессуального и результативного, выделенных для каждого педагогического условия с целью активного взаимодействия участников образовательного процесса по формированию готовности обучающихся к противодействию вовлечению в киберэкстремистскую деятельность.

Целевой компонент методики является системообразующим и состоит из системы взаимосвязанных целей. Содержательный компонент регламентирован целевым компонентом методики и состоит из учебных тем дисциплин: «Информационные технологии», «Компьютерная графика», «Информационная безопасность», на которых обучающиеся выполняя задания, знакомятся с информацией по противодействию вовлечению в киберэкстремистскую деятельность. Процессуальный компонент

интегрирует в себе методы обучения, организационные формы учебного процесса и средства обучения, выделенные отдельно для каждого педагогического условия. Результативный компонент методики включает в себя систему результатов сформированности отдельных компонентов готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность (аксиологического, процессуально-рефлексивного и когнитивно-целевого).

Более детально методика реализации педагогических условий формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность представлена в виде методической карты - таблица 7.

Таблица 7 – Методическая карта по реализации комплекса педагогических условий.

Первое условие: рефлексивно-ценностное сопровождение студентов при анализе ситуаций и выполнении заданий по информационной безопасности в киберпространстве	
Методика реализации первого педагогического условия	
Целевой	Формирование аксиологического компонента системы готовности студентов колледжа к противодействию вовлечения в киберэкстремистскую деятельность.
Содержательный	Содержательное наполнение дисциплин: «Информационные технологии», «Компьютерная графика», «Информационная безопасность».
Процессуальный	**Методы:** словесные (рассказ, объяснение, беседа, рефлексивный диалог, дискуссия), наглядные (метод наблюдения, видеометод) и практические методы (упражнения, дидактические игры). **Средства:** задания, вопросы, информационные и компьютерные технологии, информационные образовательные ресурсы, облачные сервисы, компьютерные тесты. **Организационные формы:** проблемно-рефлексивные

	лекции, мультимедиа-лекции, практическое занятие, самостоятельная работа.
Результативный	Сформированность системы мировоззренческих взглядов и ценностных ориентаций личности студента колледжа к совершаемой им деятельности в сети Интернет посредством оказания преподавателем помощи, содействия, поддержки.
Второе условие: формирование системы внутреннего противодействия вовлечения в киберэкстремистскую деятельность посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения в учебной и внеучебной деятельности	
Методика реализации второго педагогического условия	
Целевой	Формирование процессуально-рефлексивного компонента системы готовности студентов колледжа к противодействию вовлечения в киберэкстремистскую деятельность посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения в учебной и внеучебной деятельности
Содержательный	Содержательное наполнение дисциплин: «Информационные технологии», «Компьютерная графика», «Информационная безопасность».
Процессуальный	**Методы:** словесные (беседа и мозговой штурм), наглядные (метод демонстрации) и практические методы (анализ конкретных ситуаций (АКС) и его разновидности: метод ситуационного анализа (кейс-стади), метод «инцидента», метод проигрывания ситуаций (инсценировки)). **Средства:** задания, ситуационные упражнения, аудиовизуальные и технические средства (мультимедийный проектор, компьютер), облачные сервисы, компьютерные тесты. **Организационные формы:** лекция-дискуссия, лекция с заранее запланированными ошибками (провокация), лекция-консультация, практическое занятие, самостоятельная работа, внеучебные мероприятия (беседы, встречи, тренинги и др.).
Результативный	Сформированность у студентов колледжа системы внутреннего противодействия вовлечения в киберэкстремистскую деятельность, включающее детальное оценивание ситуации и принятие ответственного решения о трансляции информации с четким осознанием последствий, даже если это решение противоречит внутренним убеждениям.

Третье условие: включение в проектные задания по дисциплинам информационного цикла в качестве содержательного контента информации юридического, технологического и акмеологического направлений профилактики киберэкстремизма	
Методика реализации третьего педагогического условия	
Целевой	Формирование когнитивно-целевого компонента системы готовности студентов колледжа к противодействию вовлечения в киберэкстремистскую деятельность при выполнении проектных заданий, содержащих информацию юридического, технологического и акмеологического направлений профилактики киберэкстремизма.
Содержательный	Содержательное наполнение дисциплин: «Информационные технологии», «Компьютерная графика», «Информационная безопасность».
Процессуальный	Методы: словесные (рассказ, объяснение), наглядные (демонстрации) и практические методы (метод проектов). Средства: дидактический материал, задания печатные и электронные, аудиовизуальные и технические средства, электронные образовательные ресурсы. Организационные формы: практические занятия и самостоятельная работа.
Результативный	Овладение обучающимися знаний о киберэкстремистскую деятельности и сформированность информационных умений противодействия угрозам в сети Интернет.

Рассмотрим методику реализации *первого* педагогического условия - рефлексивно-ценностное сопровождение студентов при анализе ситуаций и выполнении заданий по информационной безопасности в киберпространстве.

Реализуется рефлексивно-ценностное сопровождение процесса формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность через проблемно-рефлексивные лекции, мультимедиа-лекции, практические занятия, самостоятельную работу обучающихся с применением словесных (рассказ,

объяснение, беседа, рефлексивный диалог), наглядных (метод наблюдения, видеометод) и практических методов (упражнения, дидактические игры) при изучении дисциплин информационного цикла: «Информационные технологии», «Компьютерная графика» на первом курсе и «Информационная безопасность» на втором курсе. В качестве средств обучения мы применяли задания, вопросы, информационные и компьютерные технологии, информационные образовательные ресурсы, облачные сервисы и компьютерные тесты.

В качестве примера представлен фрагмент проблемно-рефлексивной лекции *«Антивирусное ПО. Назначение. Виды. Компьютерные сети. Локальные и глобальные» при изучении дисциплины «Информационные технологии».*

Лекцию начинаем со вступления преподавателя для привлечения внимания аудитории к вопросам лекции. Далее осуществляется постановка проблемы, ее актуальности, анализа существующих противоречий со ссылкой на документы, авторитетные высказывания, существующие точки зрения. На следующем этапе проблема разбивается на проблемные ситуации, вопросы.

При рассмотрении вопроса «Глобальная сеть Интернет», важно обратить внимание аудитории на появление такой формы девиации как киберэкстремизм и связанным с ним понятиями кибертерроризм и киберпреступность. В ходе рассказа и объяснения учебного материала важно показать студентам, что информационный век принёс нам не только развитие технологий и

компьютеризацию всей жизни, но и проблемы информационной безопасности в киберпространстве и нарастание киберэкстремизма среди молодежи. Можно кратко представить историографию проблемы проявления киберэкстремизма и кибертерроризма. Обучающимся предлагаем ответить на следующие вопросы:

1. *Что такое экстремизм, радикализм, терроризм, киберэкстремизм, кибертерроризм?*
2. *Какие виды экстремизма вы знаете? Назовите причины распространения молодежного киберэкстремизма.*

Обучающимися предлагаются гипотезы, идеи и обосновывается логика разрешения проблемных ситуаций. Далее излагается собственная позиция педагога и сравнение с другими точками зрения. На данном этапе применяются методы беседы, рефлексивного диалога, наблюдение за деятельностью обучающихся и приемы сопоставления, сравнения и анализа, которые помогают включить студентов в процесс поиска решения проблемы. В результате происходит развитие ценностно-смыслового потенциала личности, формируется рефлексивная позиция у обучающихся по безопасности в киберпространстве, устанавливается межличностный контакт и позитивный морально-психологический климат между преподавателем и обучающимися.

Следующий этап – обобщение, резюмирование сказанного. Утверждение главной идеи решения проблемы и ее перспективы.

Согласно большой советской энциклопедии, под экстремизмом понимают приверженность крайним взглядам, идеям и мерам, направленным на достижение своих целей

радикально ориентированными социальными институтами, малыми группами и индивидами.

Радикализм - глубокая приверженность идеологии экстремизма, способствующая совершению действий, направленных на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации.

Терроризм - идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Последний этап – рефлексия содержания учебного материала. Самоанализ студентами внутреннего состояния, собственных мыслей и точки зрения на изложенный материал. На этапе рефлексии можно применить различные методики, такие как «ПОПС-формула», «Плюс, минус, интересно», «Рефлексивный экран», «Рефлексивная мишень» и другие. Например, суть методики «ПОПС-ФОРМУЛА» заключается в следующем: студентам предлагаем раскрыть содержание ПОПС- формулы: П – позиция («Я считаю, что …»); О – объяснение («Потому что …»); П – пример («Я могу доказать это на примере …»); С – следствие («Исходя из этого, я делаю вывод о том, что …»). Таким образом, мы можем получить информацию о степени погруженности студента в материал, о степени понимания изучаемой проблемы и узнать собственное мнение студентов.

Далее рассмотрим фрагмент проведения мультимедиа лекции на тему «Понятие угрозы информационной безопасности» при изучении дисциплины «Информационная безопасность». Выбор данной формы организации связан с тем, что восприятие информации на звуковом и визуальном уровне способствует лучшему усвоению информации. Перед проведением лекции основной текстовый, графический и видео материал лекции мы размещаем на слайды. Подготовленную презентацию демонстрируем обучающимся с помощью мультимедийного проектора. Во вводной части лекции знакомим обучающихся с целью, задачами, планом лекции, списком литературы. В основной части раскрываем содержание лекционного материала. Согласно плану лекции, рассматриваем вопрос о сущности угрозы информационной безопасности информации, которая трактуется как «случайное или преднамеренное явление или событие, действие или процесс, которые могут привести к искажению, несанкционированному использованию или к уничтожению информационных ресурсов информационной системы, используемых программных и технических средств и соответственно прямому или косвенному моральному или материальному ущербу интересам общества, личности или государства».

Важно отметить обучающимся появление угроз *киберэкстремизма*, основанной на «криминальном использовании технологий приема, обработки, передачи, хранения и распространения информационных сообщений экстремистского

характера, содержащей оскорбления в адрес каких-либо социальных (прежде всего, этнических и религиозных) групп, призывы к насилию над ними» и *кибертерроризма* как «угрозы, реализуемые посредством применения компьютеров и/или сетей, с намерением причинить вред или дальнейшие социальные, идеологические, религиозные, политические последствия либо запугать любое лицо в целях содействия таким целям».

Детально рассматриваем классификацию угроз информационной безопасности (угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации, случайные воздействия, преднамеренные воздействия, внутренние и внешние угрозы). При рассмотрении видов угроз уделяем внимание внешним и внутренним киберэкстремистским угрозам. Данные угрозы относятся к угрозам национальной безопасности. «К внешним угрозам относятся поддержка иностранными государственными органами и организациями экстремистских проявлений в целях дестабилизации общественно-политической обстановки в Российской Федерации, а также деятельность международных экстремистских и террористических организаций, приверженных идеологии экстремизма. К внутренним угрозам - экстремистская деятельность радикальных общественных, религиозных, неформальных объединений, некоммерческих организаций и отдельных лиц».

Далее на лекции раскрываем понятия атаки, как «попытки реализации угрозы», злоумышленника, как «того, кто

предпринимает такую попытку» и источников угрозы как «потенциальных злоумышленников или носителей угроз». При анализе источников угроз безопасности информации выделяем три группы: антропогенные источники угроз, обусловленные действиями субъекта; техногенные источники угрозы, обусловленные техническими средствами и источники угрозы, обусловленные стихийными источниками.

В ходе беседы при рассмотрении вопроса о мероприятиях системы защиты информации важно также затронуть вопрос о методах превенции киберэкстремизма в молодежной среде.

С каждым годом увеличивается количество молодежи, вступающей в ряды экстремистских организаций, причем большинство попадает в экстремистские сети случайно, которые в силу психологических и возрастных особенностей еще осознают реальных последствий своих действий.

В настоящее время существует три направления профилактики киберэкстремизма среди молодежи: юридическое, технологическое и акмеологическое.

Юридическое направление связано с совершенствованием правовых инструментов в сфере борьбы с экстремизмом. К ним относятся: Федеральный закон Российской Федерации от 25 июля 2002 г. №114-ФЗ «О противодействии экстремисткой деятельности», Федеральный закон Российской Федерации от 6 марта 2006 г. №35-ФЗ «О противодействии терроризму». В данных федеральных законах определены правовые и организационные основы противодействия экстремисткой

деятельности и направлены на обеспечение целостности и безопасности Российской Федерации, защиту прав и свобод человека и гражданина, основ конституционного строя. В целях конкретизации положений Федерального закона от 25 июля 2002 г. N 114-ФЗ «О противодействии экстремистской деятельности» и Указа Президента Российской Федерации от 12 мая 2009 г. N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года" была принята стратегия противодействия экстремизму в РФ до 2025 года.

Технологическое направление профилактики киберэкстремизма, согласно программы «Цифровая экономика Российской Федерации» от 27 июля 2017 года №1632-р, связано с совершенствованием программно-технических средств анализа и фильтрации трафика в сети Интернет, средств защиты от противоправного контента, компьютерных атак, в том числе DDoS-атак, для создания безопасной информационной среды для молодежи.

Акмеологическое направление профилактики киберэкстремизма активно реализуется в сфере образования и связано с духовно-нравственным воспитанием, воспитанием межэтнической и межконфессиональной дружбы, патриотизма и гражданственности, культуры мирного поведения, с формированием системы ценностей у молодого поколения и готовности обучающихся противодействовать социально опасному поведению, в том числе вовлечению в экстремистскую деятельность.

В заключительной части лекции делаем выводы и обобщения.

Реализация первого педагогического условия на практических занятиях осуществлялась посредством методов упражнения, дидактической игры. Обучающимся на практических занятиях по дисциплине «Информационные технологии» мы предлагали выполнить следующие задания:

Задание 1. Сделать подборку статей в сети Интернет по проблемам киберэкстремизма в России и в мире, указав название статьи, автора, точный адрес сайта и ответить на следующие вопросы:

1. Какие основные проблемы киберэкстремизма и кибертерроризма в России затронуты в статьях?
2. Какую роль играет сеть Интернет в процессе вовлечения молодежи в киберэкстремизм (кибертерроризм)?
3. Какие ценности нужно формировать у молодого поколения для противодействия киберэкстремизму?
4. Какие методы превенции киберэкстремизма были предложены в статьях? Ваше мнение.
5. Какие сложности могут возникнуть в будущем, если не принимать своевременно меры по противодействию явлений киберэкстремизма?

Задание 2. Используя сеть Интернет, зайдите на сайт КонсультантПлюс (http://www.consultant.ru) и сделайте подборку нормативных документов по теме «Экстремизм». Ознакомьтесь более детально с Федеральным законом «О противодействии

экстремистской деятельности» от 25.07.2002 N 114-ФЗ и ответьте на следующие вопросы:

1. Согласно данного Федерального закона какие основные принципы противодействия экстремизма?

2. Согласно данного Федерального закона назовите основные направления противодействия экстремистской деятельности.

3. Какую ответственность несут граждане Российской Федерации, иностранные граждане и лиц без гражданства за осуществление экстремистской деятельности согласно данного Федерального закона.

Задание 3. На сайте КонсультантПлюс (http://www.consultant.ru) изучите Стратегию противодействия экстремизма в РФ до 2025 года и укажите основные источники угроз экстремизма в современной России, обратив особое внимание на сеть Интернет.

На практических занятиях по дисциплине «Информационная безопасность» метод дидактической игры можно реализовать путем проведения игры-предположения «Что было бы…» или «Что бы я сделал…». Игровая задача содержится в самом названии. Перед студентами создается проблемная ситуация, требующая анализа и последующего действия. При этом преподавателю необходимо оказывать помощь, сопровождение в решении поставленных задач. Примеры проблемных ситуаций:

1. «Что бы я сделал, если в социальной сети мне поступило предложение вступить в ряды экстремисткой организации?»

2. «Что было бы, если бы не осуществлялось государственное регулирование работы общественных или религиозных объединений».

3. «Что бы я сделал, если мой друг активно поддерживал экстремистские идеи?».

Рефлексивно-ценностное сопровождение студентов преподавателем осуществляется при анализе ситуаций вовремя проведения рефлексивных дискуссий по информационной безопасности в киберпространстве.

Проведение рефлексивных дискуссий способствует стимулированию познавательного интереса студентов по противодействию вовлечению в киберэкстремистскую деятельность, формированию рефлексивной позиции студента, ценностей, умений оценивать реальную действительность, регулировать свое поведение. Рефлексивную дискуссию проводим в виде «круглого стола», на котором обсуждаются острые, проблемные вопросы. Участники и преподаватель, как равноправный член группы, располагаются лицом друг другу в кругу. На данное мероприятие приглашаем специалистов по данным вопросам.

Преподаватель заранее подготавливает темы для обсуждения и раздает их микрогруппам для закрытой дискуссии, создает мотивацию анализа проблем и нацеливает аудиторию на получение результата, т.е. решения проблем. Примеры тем для дискуссии: «Киберэкстремизм - угроза современности», «Система «одобрения» – «лайк и перепост» как опасный источник

продвижения киберэкстремизма», «Международный киберэкстремизм», «Киберэкстремизм как угроза национальной безопасности», «Польза и вред сети Интернет», «Информация как эффективное средство манипулирования людьми», «Толерантность и национальный экстремизм», «Гражданин и патриот» и др. Далее проводим общую дискуссию, в ходе которой лидер микрогруппы докладывает ее мнение, затем это мнение обсуждают остальные участники, высказывают свое мнение, дополняют, спорят. В ходе обсуждения участникам важно показать актуальность данной проблемы и возможные варианты ее решения.

Приглашённые специалисты выступают в качестве жюри, ведут подсчет баллов за число и качество аргументов и предложенных вариантов решения проблем. Важная роль при проведении «круглого стола» принадлежит преподавателю. Рефлексивно-ценностное сопровождение студентов осуществляется им в течение всего мероприятия и направлено на создание для обучающегося благоприятных условий в принятии осознанного решения при обсуждении обозначенных проблем. Для этого необходимо обеспечить вовлечение в разговор всех участников «круглого стола», не оставляя без внимания различные суждения, в том числе неверные. Важно своевременно организовать критическую оценку неверных суждений, привлекая для обсуждения в первую очередь других обучающихся, экспертов и только потом высказывать свою точку зрения, проводить анализ и обсуждение. В конце дискуссии преподавателю важно совместно

с участниками пройти стадию рефлексии, т.е. выработать единое или компромиссное мнение, решение по обсуждаемым вопросам. На лекционных и практических занятиях мы активно применяли разработанный нами электронный образовательный ресурс «Профилактика киберэкстремизма среди обучающихся колледжа». Под электронным образовательным ресурсом мы понимаем ресурс, представленный в электронно-цифровой форме и включающий в себя структуру, предметное содержание и метаданные о них. Для разработки электронного образовательного ресурса мы использовали систему управления сайтами uCoz (рисунок 7).

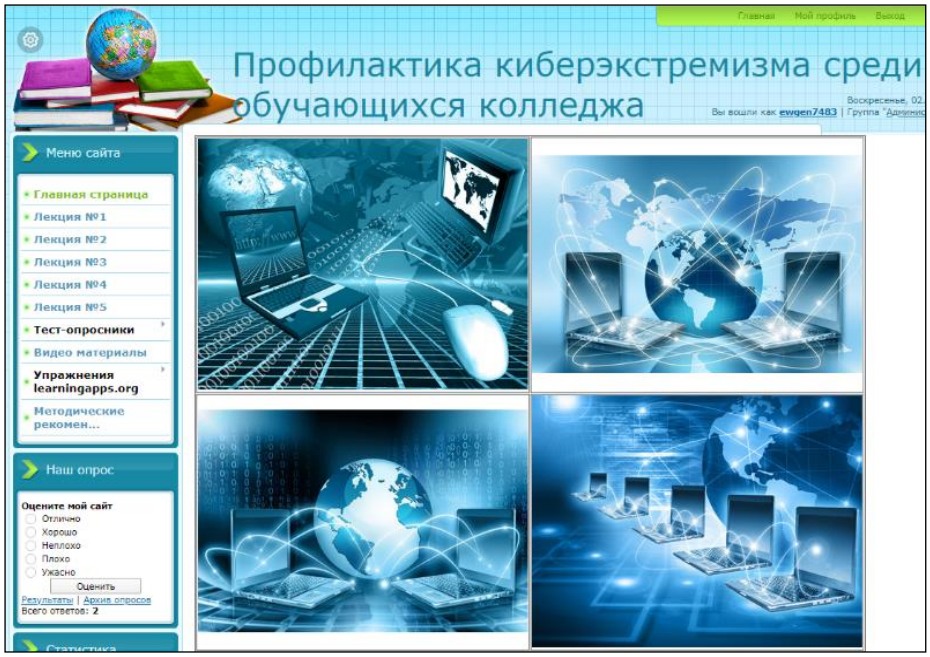

Рисунок 7 – Главная старница электронного образовательного ресурса «Профилактика киберэкстремизма среди обучающихся колледжа»

Электронный образовательный ресурс «Профилактика киберэкстремизма среди обучающихся колледжа» включает в себя следующий контент:

1) лекционный материал;

2) тест-опросники, разработанные в облачном сервисе Google Формы (результаты тест-опросников автоматически отправляются в таблицы Excel для статистической обработки данных);

3) ссылки на видеоматериалы по профилактике киберэкстремизма среди молодежи;

4) разработанные интерактивные задания в облачном сервисе LearningApps: игра «Парочки», упражнение «Хронологическая линейка» (рисунок 8), игра «Скачки», кроссворд, классификация (рисунок 9), пазл;

5) методические рекомендации по формированию готовности обучающихся колледжа к противодействию вовлечения в киберэкстремистскую деятельность.

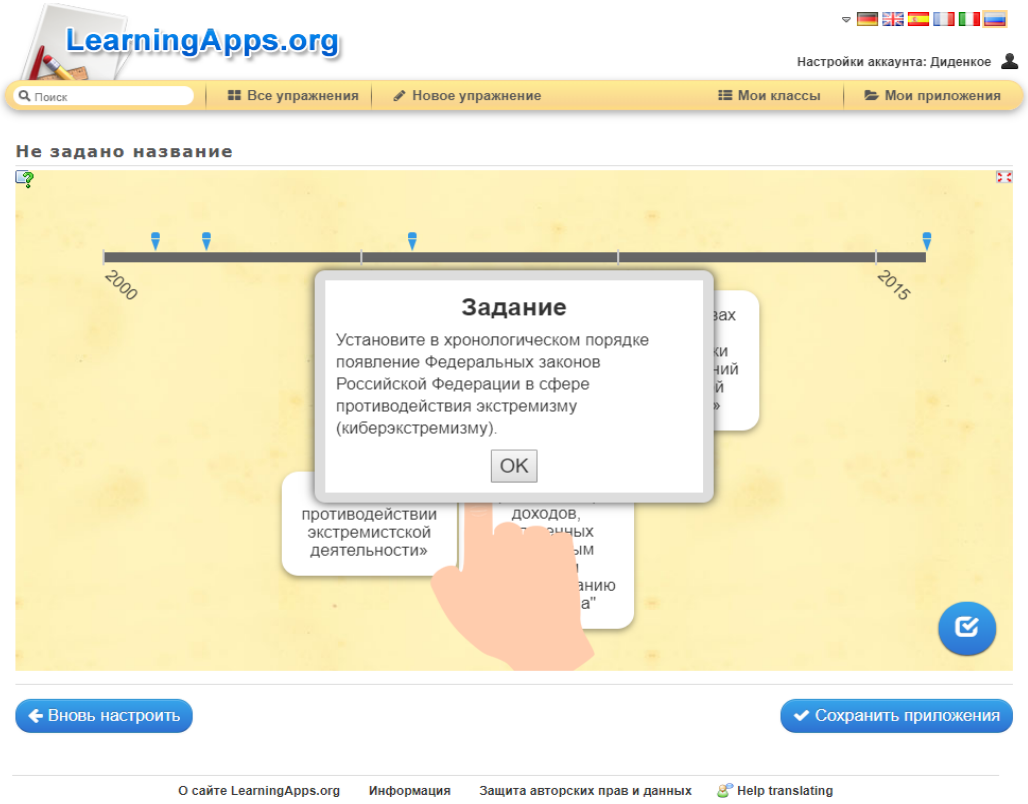

Рисунок 8 – Упражнение «Хронологическая линейка»

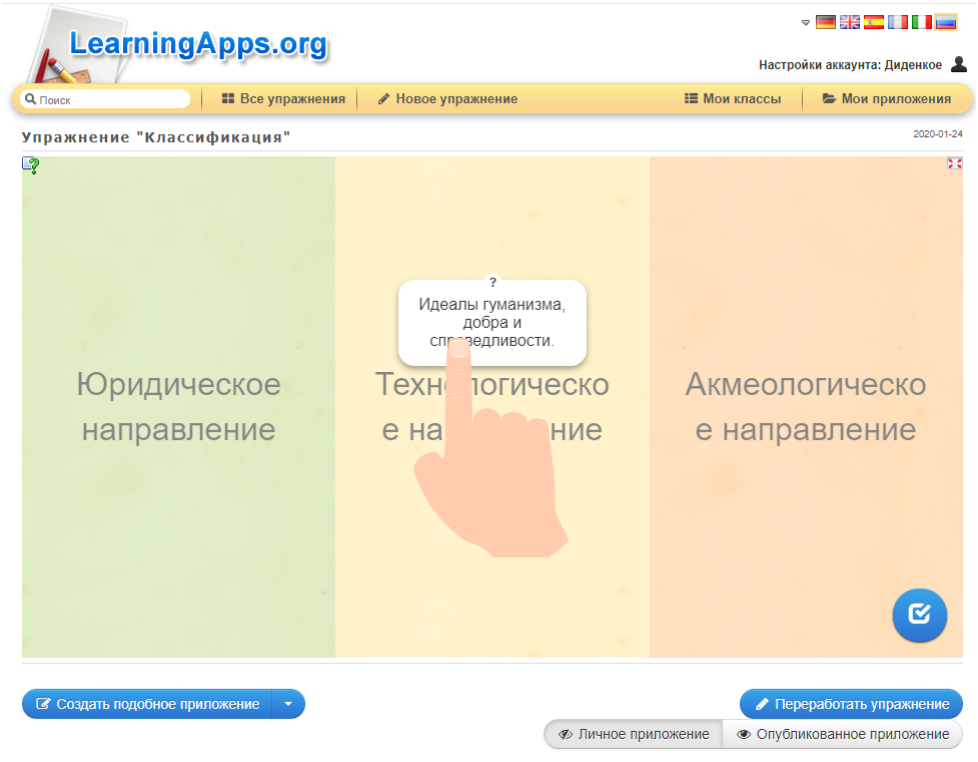

Рисунок 9 – Упражнение «Классификация»

В результате апробации методики реализации первого педагогического условия формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность у обучающихся при помощи, содействии и поддержки преподавателя формируется система мировоззренческих взглядов и ценностных ориентаций к совершаемой им деятельности в сети Интернет.

Перейдем к рассмотрению методики реализации *второго* условия эффективного формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность - формирование системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения в учебной и внеучебной деятельности.

Система внутреннего противодействия вовлечению в киберэкстремистскую деятельность формируется посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения и воспитательного воздействия в учебной и внеучебной деятельности. Принцип предосторожности заключается «в разграничении информации, ее детального оценивания и принятия ответственного решения о ее трансляции с четким осознанием последствий». Важно понимать, что следовать этому принципу и признавать ответственность за свою деятельность будут люди не на принципах цензуры, а только добровольно на основе нравственных ограничений. Обращение к

необходимости нравственных ограничений поведения людей в сети имеет смысл, так как ответственное отношение к деятельности пользователей в сети Интернет может способствовать уменьшению эскалации конфликтов в киберпространстве.

Система внутреннего противодействия вовлечению в киберэкстремистскую деятельность формируется через лекции-дискуссии, лекции с заранее запланированными ошибками (провокации), лекции-консультации, практические занятия, самостоятельную работу, внеучебные мероприятия (беседы, встречи, тренинги и др.) с применением словесных (беседа и мозговой штурм), наглядных (метод демонстрации) и практических методов (анализ конкретных ситуаций и его разновидности: метод ситуационного анализа (кейс-стади), метод «инцидента», метод проигрывания ситуаций (инсценировки)) при изучении дисциплин информационного цикла: «Информационные технологии», «Компьютерная графика» на первом курсе и «Информационная безопасность» на втором курсе. В качестве средств обучения мы применяли задания, ситуационные упражнения, аудиовизуальные и технические средства (мультимедийный проектор, компьютер), облачные сервисы, компьютерные тесты.

Рассмотрим фрагмент проведения лекции-дискуссии по теме *«Экранирование и анализ защищённости» при изучении дисциплины «Информационная безопасность».*

При изложении учебного материала лекции мы не только задаем вопросы обучающимся после рассмотрения отдельных

логически завершённых блоков информации, но и организуем обмен мнениями, идеями, взглядами, т.е. проводим дискуссию.

В течение лекции мы знакомим студентов с сервисами безопасности – экранированием и анализом защищенности.

Задача экранирования заключается в защите внутренней области сети от потенциально враждебной внешней. Данную функцию выполняют межсетевые экраны или firewall, которые устанавливают для защиты корпоративной сети организации, имеющей выход в Internet. Сервис анализа защищенности предназначен для выявления уязвимостей и их ликвидации. Примерами уязвимостей могут быть наличие вредоносного ПО, слабые пароли, небезопасные сетевые сервисы и т.д. К средствам анализа защищенности можно отнести сетевые сканеры (например, сканер Nessus) и антивирусные средства.

Далее обучающимся предлагаем ответить на ряд вопросов:

1. Что такое экранирование?
2. Какие функции выполняет экран?
3. Назовите классификацию межсетевых экранов.
4. Для чего предназначен сервис анализа защищенности? Приведите примеры.

Важно обратить внимание аудитории, что в образовательных учреждениях в целях информационной безопасности используют программные, аппаратные и программно-аппаратные комплексы: межсетевые экраны и шлюзы, антивирусные мониторы, фильтры, сканеры, криптографические средства и др.

Фильтрация контента в образовательном учреждении осуществляется на трех уровнях: провайдера, сервера и клиентской станции. Другим важным механизмом информационной безопасности является мониторинг интернет-ресурсов, позволяющий увидеть картину Web-серфинга. Отметим, что важно повышать компьютерную грамотность родителей в области применения механизмов защиты от нежелательного контента для посещения юными пользователями.

Реализация различных механизмов информационной безопасности в сети на уровне образовательных учреждений, семьи обеспечивают не только информационную безопасность в целом, но распространению идей киберэкстремизма и кибертерроризма среди молодежи.

В конце лекции предлагаем провести небольшую дискуссию на тему «Причины киберэкстремизма среди молодежи: внутренние (возрастные внутренние особенности) и внешние (среда). Пути решения», используя метод мозгового штурма. Обращаем внимание студентов, что, высказывая свою точку зрения, важно разграничивать анализируемую информацию, детально ее оценивать и принимать ответственное решение о ее трансляции с четким осознанием последствий, следуя тем самым принципу предосторожности. Таким образом, ответственное отношение к собственной деятельности в сети Интернет формирует у обучающихся систему внутреннего противодействия вовлечению в киберэкстремистскую деятельность.

Рассмотрим фрагмент лекции с заранее запланированными ошибками по теме *«Место информационной безопасности в системе национальной безопасности страны» при изучении дисциплины «Информационная безопасность».*

Целью занятия является научить студентов выступать в роли экспертов, оппонентов, оперативно анализировать и выискивать неточную информацию. Планируя материал лекции, мы заранее закладываем в нее ошибки содержательного характера и маскируем их. Ошибки выписываем в конспект, чтобы не упустить ни одной на занятии.

«Национальная безопасность Российской Федерации (далее - национальная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности». Структура национальной безопасности представлена на рисунке 10.

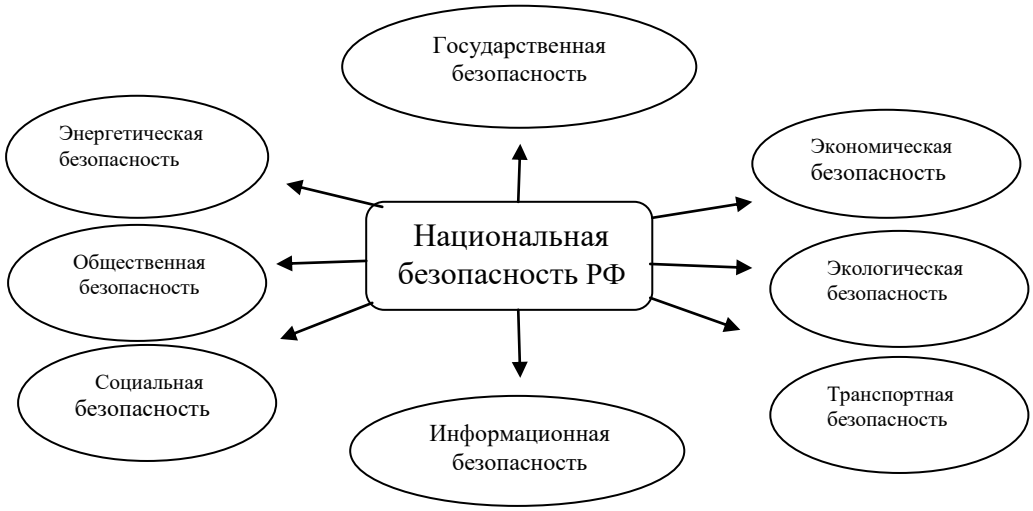

Рисунок 10 – Структура национальной безопасности

Ошибка 1. *В схеме вместо социальной безопасности должно быть безопасность личности.*

ИБ является одним из основных и в настоящее время доминирующих направлений в системе национальной безопасности РФ. Роль информационной безопасности и ее место в системе национальной безопасности страны определяются также тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое. (Роль ИБ в системе национальной безопасности https://studfile.net/preview/1848072/*)*

Важнейшей составляющей информационной безопасности является определение угроз и источников нежелательной

информации. Экстремизм представляет угрозу национальной безопасности Российской Федерации.

Наиболее опасные виды экстремизма - националистический, религиозный и культурологический.

Ошибка №2. *Согласно Стратегии противодействия экстремизму в РФ до 2025 года наиболее опасными видами экстремизма являются националистический, религиозный и политический.*

Обучающиеся в ходе лекции фиксируют ошибки в тетради, а потом обсуждают их с преподавателем. Задача преподавателя в течение занятия помогать и координировать деятельность студентов, осуществляя рефлексивно-деятельностное сопровождение, реализуя принцип предостороженности.

С целью формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность мы проводили лекции-консультации. Приведем фрагмент лекции на тему *«Структура правового обеспечения информационной безопасности» при изучении дисциплины «Информационная безопасность».*

Занятие проводится следующим образом: вначале кратко излагаем теоретический материал.

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия этим угрозам на основе норм и институтов различных отраслей права

(конституционного, гражданского, административного, уголовного и информационного).

Правовые нормы и институты, образующие правовое обеспечение информационной безопасности, закрепляются в нормативных правовых актах, являющихся источниками права в этой области и составляющих соответствующее федеральное законодательство (рисунок 11).

Рисунок 11 – Нормативно-правовые акты в Российской Федерации в области информационной безопасности

К федеральным законам, регулирующим информационные отношения, относятся:

ФЗ (федеральный закон) от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи», ФЗ от 07.07.2003 № 126-ФЗ «О связи», ФЗ РФ от

27.12.1991 № 2124-ФЗ «О средствах массовой информации», ФЗ РФ от 21.07.1993 № 5485-ФЗ «О государственной тайне»; ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»; ФЗ РФ от 28 июня 2014 г. N 172-ФЗ «О стратегическом планировании в Российской Федерации», ФЗ от 13.01.1995 № 7- ФЗ«О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»; ФЗ от 12.05.2009 № 95-ФЗ «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами»; ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»; ФЗ от 28.12.2010 № 390-ФЗ «О безопасности»; ФЗ от 28.07.2012 № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты».

Нормативно-правовые акты в сфере противодействия экстремизму и терроризму: ***Федеральный закон РФ от 25.07.2002г. №114-ФЗ*** *«О противодействии экстремистской деятельности»,* ***Федеральный закон РФ от 06.03.2006 г. № 35–ФЗ*** *«О противодействии терроризму», Указ Президента РФ от 21.12.2015 №683 «О стратегии национальной безопасности Российской Федерации», Концепция противодействия терроризму в Российской Федерации (утверждена Президентом РФ 5 октября 2009 года)», Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утверждена Президентом РФ 28.11.2014 г. № Пр-2753).*

После изложения теоретического материала студенты задают преподавателю вопросы. Ответам на них может отводиться половина учебного времени. В завершении занятия – небольшая дискуссия, где происходит обмен мнениями. При обсуждении вопросов применяем методы беседы и мозгового штурма. В конце лекции подводим итоги. Проведение данных лекций способствует формированию у студентов системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность, осознанному принятию решений.

На практических занятиях реализуем метод анализа конкретных ситуаций и его разновидности: метод ситуационного анализа (кейс-стади), метод «инцидента», метод проигрывания ситуаций (инсценировки).

Важно, чтобы, анализируя ситуацию, студент походил творчески и осознанно к ее разрешению. При этом преподавателю необходимо помочь найти и принять правильное решение, в зависимости от имеющегося времени и сложности анализируемой ситуации.

Рассмотрим метод кейс-стади, базирующийся в основном на моделях реальных ситуаций. В основе ситуации лежит прецедент, или случай (case), специально разрабатываемый по определенным правилам на основе фактического материала с последующим разбором на учебных занятиях. В отличие от ситуационных задач, в кейсах отсутствует набор исходных данных, которые нужно применять для принятия правильного решения. Кейсы имеют

множество вариантов решений и разных путей, приводящих к ним. Примеры кейсов:

Кейс №1

Компания «Лаборатория Касперского» провела исследование «Растим детей в эпоху Интернета» и получила следующие результаты:

«Российские дети проводят в Интернете значительно больше времени, чем представители молодого поколения во многих странах Европы и США. В Сети находятся более половины всех опрошенных несовершеннолетних пользователей в России (56%). Показатели по США и Европе ниже – 51% и 40% соответственно.

Пользователи младшей возрастной группы (8-10-лет) не так сильно привязаны к Интернету: почти постоянно присутствуют в Сети менее половины российских малышей (40%). Похожая ситуация и в США, где этот показатель составил 41%. В Европе эти цифры в основном ниже, например, в Германии – 9%, во Франции – 7%.

Чем старше дети, тем больше времени они проводят в Интернете. Так, 68% российских подростков (14-16 лет) почти постоянно находятся онлайн. В большинстве исследуемых стран этот показатель ниже. Например, в Великобритании он составил 60%, а в Германии 58%». - https://www.kaspersky.ru/about/press-releases/2016_news-12-05-16

Вопросы:

1. В чем причина высокой активности российских детей в сети Интернет?

2. Как данная тенденция связана с цифровой грамотностью родителей?

3. Какие меры можно принять для решения сложившейся ситуации?

Кейс №2

Середина 1990-х гг. – это время развития Интернета и всемирной компьютерной сети. В 1995 г. Дон Блэк бывший член Ку-Клукс-Клана создал первый сайт экстремистского толка. В 1996 г. насчитывалось около 70 подобных сайтов. В марте 2006 г. их было уже свыше 6 тысяч.

Вопросы:

1. Какую тенденцию отражают данные факты?

2. Являются или экстремистские сайты реальной угрозой?

3. Можно ли остановить киберэкстремизм и кибертерроризм?

Кейс №3

Роскомнадзор в 2017 году на основании требований Генпрокуратуры ограничил доступ к 13,5 тысячи сайтов с призывами к экстремизму, массовым беспорядкам и несанкционированным митингам, сообщил руководитель Роскомнадзора Александр Жаров (https://ria.ru/20180220/1514993958.html).

Почти 90 тысяч сайтов, содержащих противоправную информацию, в том числе террористического и экстремистского характера, было заблокировано в Южном федеральном округе РФ

за 2018 год, сообщил секретарь Совета безопасности России Николай Патрушев (https://ria.ru/20190913/1558642718.html).

Более 12 тысяч зарубежных сайтов, которые угрожали интересам России, были заблокированы в 2019 году, рассказал замдиректора Национального координационного центра по компьютерным инцидентам Николай Мурашов (https://radiomayak.ru/news/article/id/1250977/).

Вопросы:

1. *Какие выводы можно сделать по данной информации?*
2. *В соответствии с какими нормативными актами осуществляется блокировка сайтов экстремистского толка?*
3. *Почему информация в руках экстремистов является опасным оружием преступления?*
4. *Почему киберпреступления совершаемые экстремистами являются источником угрозы национальной безопасности всему миру?*

Принцип работы с кейсами следующий: студенты в группах выполняют анализ ситуации, которая может произойти в реальной жизни. Далее студенты выявляют проблему, предлагают свои идеи и решения в дискуссии с другими обучаемыми и вырабатывают совместное практическое решение. По итогам анализа студенты разрабатывают презентацию, содержащую решение проблемной ситуации, или сдают письменный отчет. Задачей преподавателя при решении кейсов является оказание своевременной помощи и поддержки студентов при разборе проблемной ситуации и выборе различных альтернатив ее решения.

В ходе анализа кейса студенты учатся работать «в команде», защищать свою точку зрения, слушать, аргументированно убеждать, проводить анализ ситуации и принимать решения, предусматривающие оценку положительных и отрицательных последствий принятых решений, возможных рисков и потенциальных проблем в будущем развитии событий. Так в процессе обучения реализуется принцип предосторожности.

В результате применения метода кейс-стади у студентов происходит формирование системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность, система ценностей, профессиональных позиций, жизненных установок, своеобразного мироощущения и миропреобразования.

Рассмотрим далее реализацию метода «инцидента». Студенты получают вместо подробной ситуации краткое описание инцидента, произошедшего с пользователями сети Интернет. Сообщение может быть устным или письменным типа «Случилось или произошло...». Для принятия правильного решения студентам необходимо собрать информацию об инциденте, разобраться в обстановке, определить проблемы и подумать, что нужно предпринять для принятия того или иного решения. В связи с недостаточной информацией студенты задают вопросы, начиная со слов «почему», «как», «какой», «зачем», «что», «где», «когда». Моя задача как преподавателя сразу сообщить необходимые данные или открыть дискуссию. Далее студенты в небольших подгруппах по 3-5 человек анализируют полученную информацию, принимают решение, и выносят его на общую дискуссию. Таким

образом студенты учатся анализировать ситуацию, принимать решение и нести за него ответственность.

Примеры инцидентов:

Ситуация 1. *Случилось следующее: один из Ваших знакомых активно пропагандирует экстремистские идеи, связанные с нарушением прав, свобод и законных интересов человека и гражданина в зависимости от его национальной принадлежности и является участником такой группы в Интернете.*

Вопросы:

1. *Вы разделяете данную точку зрения?*
2. *Какие Ваши действия в сложившейся ситуации?*
3. *Какие аргументы Вы могли бы привести, чтобы переубедить знакомого?*

Ситуация 2. *Случилось следующее: в социальной сети вы прочитали комментарии об отрицательном отношении к определенной религии и предложении прийти на встречу всех, кто разделяет данную точку зрения.*

Вопросы:

1. *Вы разделяете данную точку зрения?*
2. *Какие Ваши действия в сложившейся ситуации?*
3. *К каким последствиям может привести данная идеология?*

Ситуация 3. *Случилось следующее: 21 декабря 2010 г. был принят Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Этот*

закон внёс в другие федеральные законы ряд положений, предполагающих …

Вопросы:

1. *Какие положения, по вашему мнению, были внесены в другие законы?*
2. *Согласно данному закону, осуществляется ли фильтрация интернет-сайтов и блокировка Интернет-ресурсов?*
3. *Какие статьи из закона Вы знаете?*

Следующий метод, который мы применили на практических занятиях для реализации второго педагогического условия – это метод проигрывания ролей или метод инсценировки Целью данного метода является формирование способностей принимать решения в неожиданной ситуации, импровизировать. Студенты играют самих себя, демонстрируя свои ценности, культуру.

Перед началом мероприятия обучающимся предлагаем ответить на вопросы анкет «Уровень конфликтности», «Диагностика склонности к нарушению социальных норм и правил», «Проявляешь ли ты толерантность?», созданных в облачном сервисе Google формы. Студентам предлагаем выполнять анализ ситуации с помощью разыгрывания ситуации в ролях (role playing), т.е. инсценировки, которую записываем на видео и потом критически анализируем совместно со студентами. С помощью проигрывания ролей воссоздается перед аудиторией правдивая ситуация, которую студенты анализируют, оценивают поступки и поведение исполнителей игры. Причем участники

исполняют роль не по сценарию, а как сами считают нужным, т.е. импровизируют без подготовки, самостоятельно выбирая траекторию своего поведения. Например, следующая ситуация.

Ситуация: *Обучающиеся являются участниками ток-шоу «Мнение». Часть студентов выступают в роли экспертов. Ведущий предлагает экспертам ответить на ряд вопросов и поучаствовать в дискуссии.*

Вопросы:

1. *Что такое экстремизм?*

2. *Какие виды экстремизма Вы знаете? В чем суть политического, экономического, националистического, религиозного, внутригосударственного и межгосударственного экстремизма.*

3. *Какие формы экстремизма существуют? Что такое терроризм, фашизм, расизм, национализм?*

4. *Какие цели преследуют экстремистские организации? Какие механизмы используют экстремисты для дестабилизации обстановки в стране, психологического воздействия на людей?*

5. *В каком возрасте наступает ответственность за экстремистскую деятельность? (с 16 лет на территории РФ).*

6. *Согласно Уголовному кодексу РФ, какая ответственность предусмотрена за экстремистскую деятельность? (в виде штрафа и лишения свободы от 6 месяцев до 5 лет в зависимости от характера и тяжести содеянного, за участие в террористических актах - до пожизненного заключения).*

7. Что такое толерантность? Какие качества личности нужно развивать, чтобы не возникли идеи экстремизма (толерантность; уважение другого мнения, веры; прощение; сострадание; милосердие; сотрудничество; партнёрство).

8. Что такое патриотизм, гуманизм, интернационализм? Как данные качества личности могут помочь противодействовать идеям экстремизму?

После проведения ток-шоу переходим к анализу ответов студентов в видеоролике и результатов анкет. В конце занятия подводим итоги дискуссии: *«Экстремистские организации предлагают борьбу за свободу, свержение существующего режима, превосходство одних людей над другими. Но это достигается путем террора, насилия, ценой бессмысленных, жестоких убийств. Этот путь не может быть путем людей. Выбирайте путь мира, путь развития, путь создания своей жизни, а не разрушения чужой!»*.

Таким образом, метод анализа конкретных ситуаций выбран нами в качестве основного метода реализации второго педагогического условия формированию готовности студентов к противодействию вовлечению в киберэкстремистскую деятельность в связи с тем, что в процессе глубокого и детального исследования реальной или имитированной ситуации преподаватель в ходе рефлексивно-ценностного сопровождения помогает студенту найти и принять осознанное решение анализируемой ситуации.

Помимо учебных занятий формирование системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность осуществляем посредством воспитательных мероприятий. К их числу можно отнести беседы, встречи, тренинги по патриотическому воспитанию и профилактике киберэкстремизма в студенческой сфере.

Темы бесед, встреч, тренингов: «Профилактика экстремистских проявлений в молодежной среде», «Экстремизм. Что это?», «Национальность без границ», «Киберпреступность и кибертерроризм», «В единстве сила!», «За мир без террора!», «Нам нужен МИР!», «Вместе мы - сила».

При проведении встреч используем методы беседы, демонстрации ситуаций столкновения с экстремизмом, терроризмом, киберэкстремизмом с помощью фильмов, видеороликов или записанного при инсценировке ситуаций вовлечения в киберэкстремистскую деятельность. Демонстрация подготовленного материала осуществляется с помощью мультимедийного проектора и компьютеров. Данные мероприятия способствует эффективному формированию рефлексивной позиции по безопасности в киберпространстве.

Таким образом, рассмотренные методы, средства и формы реализации второго педагогического условия способствуют более эффективному формированию системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность и как следствие готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность.

Перейдем к рассмотрению методики реализации *третьего* педагогического условия формирования готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность. Суть его заключается во включении в проектные задания по дисциплинам информационного цикла в качестве содержательного контента информации юридического, технологического и акмеологического направлений профилактики киберэкстремизма.

Реализации третьего педагогического условия осуществлялась через практические занятия и выполнение самостоятельной работы, на которых осуществляется разработка и защита проектов с помощью словесных (рассказ, объяснение), наглядных (демонстрации) и практических (метод проектов) методов.

Методы рассказа и объяснение используется в организации помощи и поддержки студентов при объяснении сути проектного задания и выработки дальнейшей тактики в реализации проекта. Метод демонстрации позволяет с помощью мультимедийного проектора продемонстрировать проекты как образцы и итог работы студентов. Метод проектов направлен на организацию самостоятельной работы обучающихся: поиск проблемы, обработку информации из различных источников, разработку проектов и их защиту.

В основе метода проектов лежит выполнение проектных заданий, содержательным контентом которых является информация по противодействию и профилактике вовлечения в киберэкстремистскую деятельность.

Под проектным заданием мы понимаем средство обучения с помощью которого осуществляется управление проектной деятельностью обучающихся. Проектная деятельность представляет собой организованную самостоятельную работу обучающихся, выполненную под руководством преподавателя и направленную на создание информационных объектов средствами информационных и сетевых технологий. Формирование компетенций происходит в процессе целенаправленной, планируемой работы над проектом, осуществляемой при постоянном контроле и взаимодействии. Практическим результатом (идеальным информационным продуктом) выполнения проектного задания являются новые знания, идеи обучающихся, предметом – информация, которую обучающийся изучает и использует для реализации проекта, а объектом учебной деятельности - информационный объект.

Информационный объект представляет собой формализованную информацию, описывающую различные виды информационных продуктов, а также предметы, процессы, явления, рассматриваемые с точки зрения их информационных свойств. Информационный объект должен решать конкретную практическую задачу, обладать определенной потребительской ценностью. Так к простым информационным объектам относят: звук, текст, таблицу, рисунок. К комплексным относятся более структурированные объекты, например, база данных, гипертекст, гипермедиа, документ, презентация, Web-страницы и др. Отметим, что информационный объект должен обладать определенными

характеристическими свойствами, для работы с ним используются информационно-коммуникационные технологии, в том числе, облачные технологии. Обучающийся должен четко представлять какой информационный объект должен быть получен в процессе выполнения проекта: простой или комплексный.

Структуру проектных заданий представляем следующим образом: название проекта; цель проекта; задание (исходные данные разной степени сложности); требования к выполнению проекта; критерии оценки проекта; перечень литературы; инструктаж по выполнению задания.

Выполнение проектных заданий осуществлялось посредством следующих этапов: подготовительный (организационный): выбор темы проекта, типа проекта; конструктивный: постановка цели, задач, отбор содержания и средств; технологический: выбор среды разработки и реализация проекта; заключительный (презентационный).

Рассмотрим более подробно каждый этап. На подготовительном этапе при разработке проектного задания преподаватель совместно со студентами выбирают тему и тип проекта: индивидуальный, парный или групповой. Предварительно подготавливаем темы проектных заданий, исходя из содержания учебного материала рабочей программы дисциплины. В случае группового проекта обучающиеся делятся на группы, выбирается руководитель проекта.

На конструктивном этапе проектирования информационного объекта обучающиеся формулируют цель и задачи проекта, для

достижения которых создается информационный объект. Далее обучающиеся рассматривают возможные варианты выполнения данного проектного задания, определяют его содержание, этапы реализации. Руководитель распределяет работу по выполнению проектного задания между всеми участниками группы.

Технологическая разработка проекта включает в себя пошаговое, последовательное выполнение действий по созданию информационного объекта, что помогает развивать у студентов систематичность в выполнении задания. Обучающиеся, исходя из поставленных задач, выбирают самостоятельно или с помощью преподавателя среду разработки (облачный сервис, прикладная программа и др.), с помощью которого реализуется проект. Руководитель группы координирует работу по созданию информационного объекта. Участники группы выполняют свою часть задания, наполняя информационный объект необходимым контентом, во время учебного занятия или самостоятельно во внеучебное время. Далее осуществляется корректировка информационного объекта обучающимися с учетом замечаний преподавателя. Выполнение данного вида работы способствует развитию интереса к исследовательской работе, профессиональному становлению. Разработка проекта ведется обучающимися самостоятельно, преподаватель координирует и контролирует их деятельность. На заключительном этапе обучающийся оформляет выполненную работу согласно предъявленным требованиям, презентует ее перед аудиторией и отвечает на вопросы.

Критерии оценки проекта: конструктивный, технологический и эстетический критерии.

Проектные задания могут быть разного уровня сложности: учебно-познавательные, учебно-исследовательские, учебно-творческие. Учебно-познавательные проектные задания классифицируются как репродуктивные (низкий уровень), учебно-исследовательские как эвристические (средний уровень), учебно-творческие как творческие (высокий уровень). Состав, структура заданий определяют сложность деятельности по их выполнению (уровень проблемности, самостоятельности).

Модель учебной деятельности на практических занятиях по выполнению учебно-познавательных проектных заданий предполагает «простую коммуникацию» между преподавателем и обучающимися. Преподаватель является консультантом, помогающим обучающимся выстроить траекторию проектной деятельности с опорой на их опыт и теоретические знания. Данная работа заключается в совместной постановке цели и задач проектного задания, рассмотрении вариантов и этапов его выполнения. Обучающимся предлагается готовая инструкция или подробный алгоритм выполнения задания. Если при выполнении проекта обучающийся встречает какие-либо новые понятия, то преподаватель может дать необходимые пояснения. То есть учебно-познавательные проектные задания должны быть разработаны преподавателем таким образом, чтобы они были в первую очередь обучающими, а не контролирующими.

Модель учебной деятельности на практических занятиях по выполнению учебно-исследовательских проектных заданий предполагает «сложную коммуникацию» между преподавателем и обучающимися, когда идет совместное осмысление содержания задания и формирование научного мышления. Проектные задания среднего уровня предполагают частично-исследовательскую деятельность, отсутствие готового алгоритма выполнения задания. Обучающийся может воспользоваться лишь краткими инструкциями. При выполнении учебно-исследовательского проектного задания преподаватель совместно с обучающимися составляет план выполнения проекта. Технологическая разработка проекта ведется обучающимися самостоятельно, преподаватель координирует, контролирует их деятельность, задает вопросы. В случае затруднения, студент может обратиться к кратким инструкциям по выполнению проектного задания данного типа.

Модель учебной деятельности на практических занятиях по выполнению учебно-творческих проектных заданий предполагает коммуникацию между обучающимися. Согласно данной модели учебной деятельности «преподаватель перестает быть источником информации (знаний)». Участие преподавателя сводится к минимуму, он лишь контролирует деятельность студентов. Обучающиеся становятся исследователями, разработчиками информационного объекта, демонстрирующими имеющийся у них опыт самостоятельного овладения знаниями в процессе работы над созданием информационного объекта. Разработка учебно-творческих проектных заданий предполагает творческую

самостоятельную деятельность обучающихся на практических занятиях, нестандартный подход к решению задачи. На учебном занятии, при выполнении учебно-творческих проектных заданий, обязательной является коммуникация между обучающимися, в ходе которой обучающиеся учатся взаимодействовать между собой и совместно выполнять учебные цели. При разработке учебно-творческих проектных заданий необходимо обратить внимание преподавателя на реальность реализации проекта. Не следует его делать слишком сложным. Не нужно стремиться учесть абсолютно все характеристики предметной области. Необходимо четко сформулировать цель, ограничив перечень задач, для достижения которых создается информационный объект. Инструкций по выполнению проектного задания данного типа не предусматривается.

В результате проектной деятельности у студентов повышается познавательная активность, формируются коммуникативные и информационные умения. При этом обучение носит активно-деятельностный, проектный характер. Обучающиеся выполняют проектные задания разного уровня сложности, при этом осваивают разные модели учебной деятельности, в основе которых распределение функций учебной деятельности и организация коммуникации между преподавателем и обучающимися, и обучающихся между собой.

Для эффективной подготовки студентов колледжа к противодействию киберэкстремистской деятельности содержательный контент проектов мы разделили согласно

направлениям профилактики киберэкстремизма на юридический, технологический и акмеологический.

Юридический контент включает в себя нормативно-правовую базу Российской Федерации, например, Федеральный закон Российской Федерации от 25 июля 2002 г. №114-ФЗ «О противодействии экстремисткой деятельности», Федеральный закон Российской Федерации от 6 марта 2006 г. №35-ФЗ «О противодействии терроризму», Указ Президента Российской Федерации от 12 мая 2009 г. N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года», Стратегия противодействия экстремизму в РФ до 2025 года.

Технологический контент включает в себя информацию о программно-технических средствах анализа и фильтрации трафика в сети Интернет, средствах защиты от противоправного контента, компьютерных атак и т.д.

Акмеологический контент включает в себя информацию о духовно-нравственном воспитании, воспитании межэтнической и межконфессиональной дружбы, патриотизма и гражданственности, культуры мирного поведения, о формировании системы ценностей у молодого поколения по противодействию экстремистской деятельности.

Проектные задания могут выполняться в течение одного или нескольких практических занятий, индивидуально или коллективно, а также во время внеаудиторной самостоятельной работы. Самостоятельная работа студентов при выполнении проектных заданий особо актуальна, так как формирует

познавательный интерес к предмету и стимулирует студентов к исследовательской деятельности.

В проектные задания по дисциплинам информационного цикла включено создание следующих информационных объектов: разработка презентаций, электронных учебных пособий, компьютерных тестов, сайтов, рисунков и т.д.

Например, после изучения возможностей графических редакторов по дисциплине «Компьютерная графика» студенты выполняют индивидуальные проектные задания по темам: «Молодежь против киберэкстремизма», «Экстремизму – нет!», «Осторожно - ЭКСТРЕМИЗМ!», «Терроризм: будьте бдительны!», «Молодежь за мир!», «Предупрежден, значит вооружен!», «Мир без насилия», «Киберпреступности и кибертерроризму – СТОП!», «Интернет может быть опасным!».

При изучении дисциплины «Информационные технологии» обучающиеся знакомятся с офисным программным обеспечением: MS Word, MS PowerPoint и др., с его интерфейсом и возможностями. На практике студенты разрабатывают презентации, доклады, рефераты, содержательным наполнением которых является информация по профилактике экстремизма.

Темы содержательного контента формулируются преподавателем и выдаются студентам на занятии (Таблица 8).

Таблица 8 – Темы содержательного контента проектов

Содержательный контент	Темы
ЮРИДИЧЕСКИЙ	1. Организационно-правовые основы противодействия киберэкстремизму и терроризму в РФ. 2. **Федеральный закон РФ от 25.07.2002г. №114-ФЗ** «О противодействии экстремистской деятельности». 3. **Федеральный закон РФ от 06.03.2006 г. № 35-ФЗ** «О противодействии терроризму». 4. Указ Президента РФ от 21.12.2015 №683 «О стратегии национальной безопасности Российской Федерации». 5. Концепция противодействия терроризму в Российской Федерации (утверждена Президентом РФ 5 октября 2009 года). 6. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утверждена Президентом РФ 28.11.2014 г. № Пр-2753).
ТЕХНОЛОГИЧЕСКИЙ	1. Программно-аппаратные механизмы противодействия кибертерроризму. 2. Кибертерроризм как угроза государственной безопасности, личности и общества. 3. Системы контроля безопасности контента в Интернете. 4. Контент-фильтрация в сети Интернет. 5. Обеспечение информационной безопасности в образовательных учреждениях. 6. Технические средства защиты информации в сети Интернет. 7. Программные, аппаратные и программно-аппаратные комплексы по защите информации. 8. Криптографические средства защиты информации в сети Интернет. 9. Антивирусные средства защиты информации в сети: мониторы, фильтры, сканеры. 10. Роль межсетевых экранов и шлюзов в защите информации в сети. 11. Мониторинг интернет-ресурсов как механизм обеспечения информационной безопасности.

	12. Безопасность в социальных сетях. 13. Основы безопасной работы в электронной почте. 14. Кибербуллинг в сети Интернет. 15. Фишинг в сети Интернет. 16. Цифровая репутация в сети Интернет. 17. Киберпреступления в сети Интернет. 18. Информационная война. 19. Кибертерроризм: история и современность.
АКМЕОЛОГИЧЕСКИЙ	1. Идеалы гуманизма, добра и справедливости. 2. Ценности гражданского общества. 3. Молодежный радикализм как совокупный эффект социоструктурных изменений в российском обществе. 4. Многокультурность – фактор стабильного развития общества. 5. Воспитание в духе миролюбия, веротерпимости, патриотизма и толерантности. 6. Роль семьи в воспитании у подрастающего поколения патриотических чувств и норм толерантности. 7. Терпимость и уважительное отношение к представителям других национальностей и конфессий. 8. Борьба с проявлениями ксенофобии и экстремизма. 9. Патриотизм как основа национального самосознания. 10. Национальная идея – основа сильного государства. 11. Моя страна – Россия. 12. Ассамблея народов России. 13. Патриотизм и религиозные учения. 14. Социально-психологические факторы развития киберэкстремизма. 15. Современные проблемы общечеловеческих ценностей. 16. Меры профилактики киберэкстремизма. 17. Культура современного мира. 18. Экстремизм – проблема современности. 19. Противодействия идеологии киберэкстремизма средствами СМИ. 20. Терроризм – угроза обществу. 21. Межличностные, межконфессиональные

	противоречия – почва для террористической и экстремистской деятельности. 22. Традиции и обычаи народов России. 23. Я – гражданин РФ. 24. Нравственность как общечеловеческая ценность.

В ходе выполнения проектных заданий у студентов формируются четкие представления о киберэкстремистской деятельности, методах вовлечения в данный вид деятельности и способах противодействия этому явлению; формируются обобщенные информационные умения противодействия угрозам в сети Интернет и ценностные ориентации личности в ситуациях вовлечения в киберэкстремистскую деятельность.

Для решения объективной проблемы в системе профессиональной подготовки студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность нами был разработан следующий комплекс педагогических условий:

1)рефлексивно-ценностное сопровождение студентов при анализе ситуаций и выполнении заданий по информационной безопасности в киберпространстве;

2)формирование системы внутреннего противодействия вовлечению в киберэкстремистскую деятельность посредством реализации принципа предосторожности во время рефлексивно-ценностного сопровождения в учебной и внеучебной деятельности;

3)включение в проектные задания по дисциплинам информационного цикла в качестве содержательного контента

информации юридического, технологического и акмеологического направлений профилактики киберэкстремизма

Такой комплекс обеспечивает сформировать готовность обучающихся к противодействию вовлечения в киберэкстремистскую деятельность.

Практические задания к разделу 4.

Задание 4.1. Подготовьте план мероприятия по противодействию вовлечения обучающихся в киберэкстремистскую деятельность.

Задание 4.2. Подготовьте эссе на одну из тем:

- Многокультурность – фактор стабильного развития общества.
- Воспитание в духе миролюбия, веротерпимости, патриотизма и толерантности.
- Роль семьи в воспитании у подрастающего поколения патриотических чувств и норм толерантности.
- Терпимость и уважительное отношение к представителям других национальностей и конфессий.
- Борьба с проявлениями ксенофобии и экстремизма.
- Патриотизм как основа национального самосознания.
- Национальная идея – основа сильного государства.
- Моя страна – Россия.
- Ассамблея народов России.

Список источников к разделу 4

1. Аминов, Д.И. Молодежный экстремизм [Текст]/ Д. И. Аминов, Р. Э. Оганян; под науч. ред. Р. А. Адельханяна. - М. : Триада ЛТД, 2005 (Тип. Триада ЛТД). - 194 с.

2. Диденко Е.В. К вопросу о формировании готовности студентов колледжа ИТ-специальностей к противодействию вовлечению в киберэкстремистскую деятельность [Текст] /Диденко Е.В., Диденко Г.А. // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы: сб. материалов IX Международной науч.-практ. конф. – Челябинск: Челябинский филиал РАНХиГС, 2018. – С.43-47.

3. Диденко, Е.В. Экстремизм в сети интернет[Текст] /Диденко Е.В., Гафарова Е.А., Диденко Г.А. //Информационно-телекоммуникационные системы и технологии (ИТСиТ-2018): Материалы Всероссийской научно-практической конференции, г. Кемерово, 11-13 октября 2018 г.; Кузбас. гос. техн. ун-т им. Т.Ф. Горбачева. – Кемерово, 2018. – С. 35-37.

4. Диденко, Е.В. Анализ результатов экспериментальной работы по формированию готовности обучающихся колледжа к противодействию вовлечения в киберэкстремистскую деятельность [Текст] / Диденко Е.В., Гафарова Е.А., Степанова О.А., Диденко Г.А., Шамаева Т.Н. // Современные наукоемкие технологии. – 2019. – № 8 – С. 112-116; Режим доступа: http://www.top-technologies.ru/ru/article/view?id =37640 (Рец. ВАК №1875 Перечень рецензируемых научных изданий (по состоянию на 02.03.2024).

5. Диденко, Е.В. Анализ состояния проблемы киберэкстремизма среди молодежи [Текст] /Диденко Е.В. // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы: сб. научных трудов. – Челябинск: Челябинский филиал РАНХиГС, 2019. – С.37-41.

6. Диденко, Е.В. О формировании готовности студентов колледжа ИТ-специальностей к противодействию вовлечению в киберэкстремистскую деятельность [Текст] /Диденко Е.В., Коняева Е.А. // Тенденции развития науки и образования. «Тенденции развития науки и образования» Ноябрь 2018 г. №44, Часть 1 Изд. НИЦ «Л-Журнал», 2018. – С. 24-27.

7. Диденко, Е.В. Педагогические условия формирования готовности обучающихся колледжа к противодействию вовлечению в киберэкстремистскую деятельность [Текст] / Диденко Е.В., Гафарова Е.А., Диденко Г.А. // Современные наукоемкие технологии. – 2019. – №3-2. – С. 280-283 – Режим доступа : https://top-technologies.ru/ru/article/view?id=37479 (дата обращения : 26.05.2019). (Рец. ВАК №1875 Перечень рецензируемых научных изданий (по состоянию на 09.03.2024).

8. Диденко, Е.В. Рефлексивно-ценностное сопровождение обучающихся при анализе ситуаций и выполнении заданий по информационной безопасности в киберпространстве [Текст] /Диденко Е.В., Диденко Г.А. // Научно-технический прогресс: актуальные и перспективные направления будущего: сб. материалов VIII Международной науч.-практ. конф. (16 июля 2018 г.). – Кемерово : ЗапСибНЦ, 2018. – С. 76-80.

9. Доколин, А.С. Формирование компетенций по противодействию киберэкстремистской деятельности у студентов колледжа [Текст] / А.С. Доколин, Е.В. Чернова, Л.Ф. Ганиева, О.Л. Колобова //Фундаментальные исследования. – 2015. – № 9. – С. 434-439.

10. Доколин, А.С. Формирование готовности студентов колледжа к противодействию вовлечению в киберэкстремистскую деятельность [Текст]: дис. ... канд. пед. наук : 13.00.08 / Доколин А.С. - Магнитогорск, 2017. 196 с.

11. Любин, С.Ю., Яценко, О.А. Профилактика экстремизма в молодежной среде [Текст] // Феномен экстремизма и ксенофобии в современной России: факторы генезиса, пути и способы противодействия: материалы Всерос. с межд. участием науч.-практ. конф., 9-10 дек. 2010 г. -Краснодар: Краснодар. ун-т МВД России, 2010, с. 151-152

12. Мамытов, Т.Б. Религиозный и националистический экстремизм. [Электронный ресурс] - URL: https://ipi1.ru/images/PDF/2016/47/religioznyj-i-natsionalisticheskij.pdf (дата обращения: 02.03.2024)

13. Матвеев В.А. Информационная безопасность: Учебно-методическое пособие [Текст]. – Нижний Новгород: Нижегородский госуниверситет, 2017. - 24с.]

14. Национальная политическая энциклопедия [Электронный ресурс] URL: http://politike.ru/termin/ekstremizm.html (дата обращения:02.03.2024)

15. Понятие и формы экстремизма [Электронный ресурс] - URL: https://studopedia.org/12-18315.htm (дата обращения:03.03.2024)

16. Старикова Е.В. Сценарий часа общения по профилактике экстремизма [Электронный ресурс] Режим доступа: https://infourok.ru/scenariy-chasa-obscheniya-po-profilaktike-ekstremizma-2820571.html).

17. Старкова, Н.А., Старков, А.Н., Чернова, Е.В. Киберэкстремизм в молодежной среде как социальная проблема [Электронный ресурс] // Фундаментальные исследования. – 2014. – № 12-7. – С. 1550-1554; URL: http://fundamental-research.ru/ru/article/view?id=36402 (дата обращения: 06.03.2024).

18. Традиционный анализ конкретных ситуаций [Электронный ресурс] URL: https://studme.org/88217/pedagogika/traditsionnyy_analiz_konkretnyh_situatsiy (дата обращения: 07.03.2024)

19. Федеральный закон "О противодействии терроризму" от 06.03.2006 N 35-ФЗ (последняя редакция).

20. Федеральный закон "О противодействии экстремистской деятельности" от 25.07.2002 N 114-ФЗ.

21. Чупров, В.И. Молодежный экстремизм: сущность, формы проявления, тенденции [Текст] : монография / В.И. Чупров, Ю.А. Зубок. – М.: Academia, 2009. – 320 с.

Учебное пособие

Елена Аркадьевна Гафарова, Галина Александровна Диденко,
Ольга Николаевна Шварцкоп

ПЕДАГОГИЧЕСКОЕ ВЗАИМОДЕЙСТВИЕ В СОВРЕМЕННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: КИБЕРБЕЗОПАСНОСТЬ ЛИЧНОСТИ

Издательство «Библиотека А.Миллера»
454080, г. Челябинск, ул. Свободы, 159
8,74 усл.- печ. л.