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

Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Электронная рабочая тетрадь по МДК. 05.01 «Проектирование и дизайн информационных систем» как средство организации самостоятельной работы студентов профессиональной образовательной организации

Выпускная квалификационная работа
по направлению: 44.03.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Информатика и вычислительная техника
Форма обучения очная

Проверка на объем заимствований:
69,72% авторского текста

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

Выполнил(а):
Студент(ка) группы ОФ-409-079-4-1
Васильева Аделина Витальевна

Научный руководитель:
Гисс Елена Ивановна, кандидат педагогических наук, доцент

Челябинск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Цифровая грамотность является основой продуктивного и безопасного использования цифровых технологий для решения практических задач в условиях всеобщей цифровизации и цифровой трансформация образования. Отсутствие цифровой грамотности создает угрозу для физического и психологического здоровья, социального благополучия личности, ограничивает человека в реализации гражданских прав, получении государственных услуг, онлайн-коммуникации и совместной работы, подвергает опасностям кибермошенничества и нарушения информационной безопасности. Информатика как учебная дисциплина обладает широким дидактическим потенциалом в сфере формирования цифровой грамотности. Однако содержание информатики требует своей модернизации в аспекте цифровой составляющей.

С развитием современных технологий сформировались условия к появлению нового вида преступлений, совершаемых в киберпространстве (киберпреступлений). Большинство из этих преступлений являются экономическими и способны причинить реальный вред отношениям собственности и нормальному порядку осуществления предпринимательской или иной экономической деятельности. В науке уголовного права и криминологии активно ведутся дискуссии о понятии, природе, видах киберпреступлений и мерах противодействиях им.

Этому новому виду преступности необходимо противопоставить действенные меры, в число которых входят и меры уголовно-правового воздействия. Однако действующее отечественное уголовное законодательство не всегда успевает реагировать на вызовы современной преступности. Поэтому новые реально опасные деяния, совершаемые в киберпространстве, нередко остаются вне сферы действия уголовного закона, а в отношении уже криминализированных деяний возникают существенные проблемы их

правовой оценки и привлечения виновных к ответственности. Данное обстоятельство и обуславливает актуальность темы исследования.

Актуальность исследованию придаёт и тот факт, что размер причиняемого экономическими киберпреступлениями ущерба за последние годы многократно вырос. По мнению многих ученых, доходы теневого бизнеса в социальных сетях могут сравниться с прибылью от незаконной торговли наркотиками. Ежегодные потери мировой экономики от экономических преступлений, совершаемых в киберпространстве, составляют 500 миллиардов долларов. Тенденция роста киберпреступлений имеется и в России, где уже ежедневно совершается 44 хищения из систем дистанционно-банковского обслуживания. Более того, согласно статистическим данным Европола за 2013-2014 годы, большинство хакеров и киберпреступников в Европе — это граждане России и стран СНГ. Одновременно на эффективность противодействия киберпреступлениям негативно влияет очень высокий уровень латентности, как экономических преступлений, совершаемых в киберпространстве, так и преступлений в сфере компьютерной информации.

На сегодняшний день сложилось противоречие между необходимостью формирования навыков кибербезопасности у студентов профессиональной образовательной организации с одной стороны, и недостаточным методическим и материально-техническим обеспечением формирования навыков кибербезопасности с другой.

Проблема исследования: как формировать навыки кибербезопасности в социальных сетях у студентов профессиональной образовательной организации.

Цель исследования**:** проанализировать процесс формирования навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации при преподавании дисциплин профессионального цикла и разработать учебно-методический комплекс для повышения эффективности данного процесса.

Объект исследования: процесс профессиональной подготовки студентов колледжа.

Предмет исследования: формирование навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации при преподавании дисциплин профессионального цикла.

Задачи исследования:

1. Проанализировать угрозы и способы защиты персональной информации в социальных сетях.

2. Исследовать сущность навыков кибербезопасности в социальных сетях.

3. Разработать электронный учебно-методический комплекс как средство формирования готовности к кибербезопасности в социальных сетях.

4. Разработать методические рекомендации по кибербезопасности в социальных сетях для обучающихся.

5. Провести проверку сформированности навыков и проанализировать полученные результаты.

Теоретико-методологическую основу исследования составили труды: Кричевский, В. Б., Степанов, Е.А., Пидкасистый, П. И., Беспалько, В. Колмогоров, Л. С., Фридман, Л. М., Семененко, В.А., Федоров, А. В.

Методы исследования*:* изучение учебной и специальной (анализ ФГОС СПО по направлению подготовки (09.02.07 Информационные системы и программирование) и рабочей программы ОП.13 Информационная безопасность) литературы по информационной безопасности и кибербезопасности в социальных сетях; изучение и анализ учебно-программной, изучение Интернет-ресурсов по проблеме исследования; метод апробации.

База исследования – ГБПОУ «Южно-Уральский государственный колледж».

Выпускная квалификационная работа имеет следующую структуру: введение, две главы, выводы по главам, заключение, список используемых

источников, приложение. В списке литературы 43 источника, в тексте работы 6 таблиц, 33 рисунка.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ НАВЫКОВ КИБЕРБЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ У СТУДЕНТОВ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Кибербезопасность в социальных сетях: проблемы и перспективы

Кибербезопасность – совокупность методов и средств защиты личной информации от атак хакеров по различным техническим устройствам, например, компьютеру, телефону, планшету и другим электронно-вычислительным системам [2].

Серьезной проблемой, с которой в настоящее время пришлось столкнуться обществу, является рост негативного воздействия информационно-телекоммуникационных сетей на студентов-подростков. В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, делается акцент на том, что в настоящее время происходит усиление влияния на молодёжь негативной информации, в результате чего национальные нравственные ценности стираются. В частности, молодое поколение нуждается в особой защите государства в современных условиях развития информационного общества, и на проблемах обеспечения информационной безопасности несовершеннолетних нужно обратить большее внимание. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ раскрывает термин «информационная безопасность детей» как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью или физическому, психическому, духовному, нравственному развитию».

Развитие информационных технологий и социальных сетей с каждым годом растет и развивается, современые люди не представляют своей жизни без телефона или персонального компьютера. Постепенно наступает эра всемирной информатизации [1]. Интернет – глобальная сеть, которая

обеспечивает связь для пересылки сообщений электронной почты, передачи файлов, соединения с другими компьютерами и получения доступа к информации, существующей в самых различных формах. Взрослым и детям представлен широкий спектр возможностей в Интернете для выражения собственной индивидуальности, обучения и образования, по этой причине дети в особенности являются одной из наиболее быстрорастущих групп пользователей Интернет. Несмотря на положительные моменты, появляются вопросы информационной безопасности детей. Важная задача как для России, так и для всех развитых стран мира – защитить несовершеннолетних от интернет-угроз, но сеть Интернет невозможно контролировать, поэтому возникает много нерешенных разнообразных проблем [3].

Стоит отметить, что кибербезопасность – это часть такого понятия как информационная безопасность. Кибербезопасность имеет более узкую направленность и изучает охрану важных данных, в то время как информационная безопасность изучает всё о безопасности информации и данных в целом. Слово «информация» происходит от латинского слова «informatio», что означает разъяснение, высказывания, осведомлённость. Само слово информация не так давно стало превращаться в научный термин. До этого информацию воспринимали как то, что присутствуют в языке, письме или передаётся при общении [10].

Киберпреступления – это приступная деятельность, основной задачей которой является неправомерное использования компьютера, компьютерной сети или сетевого устройства с целью получения материальной выгоды [2].

Согласно предоставленным данным Cyber Polygon, в 2021 году доминирующими были классические атаки – фишинговые сайты на тему коронавируса, оформление якобы подлинных документов о вакцинации, мошеннические операции с услугами, реклама проектов, приносящих мгновенных доход. Такие злонамеренные действия составили более 85 % атак. Примерно 10 % атак, зафиксированных в 2021 году, пришлись на программы-вымогатели, которые были нацелены на корпорации. Более 60% российских

пользователей отправляют личные и рабочие переписки даже мало знакомым людям, делаться другими личными данными и материалами на страницах в социальных сетях, что в дальнейшем приводит к утечкам данных в даркнет ресурсы. 20 апреля 2020 года аналитики Cyble сообщили об обнаружении в даркнете данных 267 млн аккаунтов Facebook. Они приобрели их у хакеров за $540, то есть по 0,0002 цента за аккаунт. Данные содержали уникальный идентификационный номер в Facebook, номер телефона, полное имя и временную метку и в основном касались пользователей в США [9].

Киберэкстремизм является современной формой экстремизма, использующая в качестве оружия – пропаганду. Распространяя свои радикальные идеи посредством персональных компьютеров и мобильных аппаратов через социальные сети, третированную рекламу, почтовую рассылку и другие средства электронной передачи информации.

С точки зрения идеологии, в экстремизме зачастую используются лозунги и призывы, создающие яркий образ врага, против которого необходимо задействовать возможные силы для борьбы. Используемые мотивы в экстремизме зачастую апеллируют к низменным чувствам и мотивам человека. Популярными методами являются: сознательное провоцирование массовых беспорядков, призывы к гражданскому неповиновению, террористические акты, публичные заявления и угрозы. Для вовлечения в деятельность экстремистских организаций, людям обещают быстрое устранение трудностей, осуществление гарантированного порядка в стране, регионе, мире, достижения социальной обеспеченности и достойного уровня жизни. Для этого в качестве необходимые меры преподносится жесткое утверждение определенной идеологии, другой системы политических экономических идеологических ценностей. Зачастую, в качестве идеологического прикрытия, экстремисты ложно проповедуют любовь и мир во всем мире. А для достижения своих целей применяют насильственные методы, вплоть до массового убийства людей, которые сами же оправдывают

и считают приемлемыми, прикрываясь идеалами религии, свободы, скорого процветания [19].

Кибертерроризм – совокупность незаконных действий в киберпространстве, создающих угрозу обществу, личности и государству. Может привести к порче имущества, искажению информации и другим серьезным проблемам. Главной задачей кибертерроризма являться влияние на решение политических, социальных и экономических задач [20].

Кибертеррористы не закладывают бомб, не берут заложников. Они угрожают компьютерными средствами: выводом из строя крупной компьютерной сети какой-нибудь компании, уничтожением данных клиентов банков, нарушением работы заводов и электростанций и т.п. с целью получения выкупа. Для достижения поставленных целей могут использоваться различные методы:

– незаконное получение доступа к государственным и военным архивам с секретной информацией, реквизитам банковских счетов и платежных систем, личным данным;

– осуществление контроля над объектами инфраструктуры для оказания влияния на их работоспособность вплоть до вывода из строя отдельных компонентов и полного останова систем жизнеобеспечения;

– похищение или уничтожение информации, программных средств или технических ресурсов путем внедрения вредоносных программ различных типов;

– ложные угрозы совершения атак, которые могут повлечь за собой дестабилизацию экономической или социально-политической обстановки [21].

1.2 Сущность навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации

В научной литературе под «навыками кибербезопасности в социальных сетях у студентов профессиональной образовательной организации»

понимают способности обучающихся выявлять, идентифицировать и противостоять угрозам информационного воздействия в киберпространстве.

Чтобы понять сущность навыков кибербезопасности в социальных сетях и процесс их формирования у студентов профессиональной образовательной организации сделаем анализ триады «знания-умения-навыки» в современной дидактике, согласно которой овладение умениями и навыками происходит на базе усвоения знаний [22].

Знания составляют ядро содержания обучения. На основе знаний у учащихся формируются умения и навыки, умственные и практические действия. Понятие «знание» многозначно и имеет несколько определений. Оно определяется то, как часть сознания, то, как нечто общее в отражении предметного разнообразия, то, как способ упорядочения действительности, то, как некоторый продукт и результат познания, то, как способ воспроизведения в сознании познаваемого объекта. В новой «Российской педагогической энциклопедии» «знания» определяются следующим образом: «проверенный общественно-исторической практикой и удостоверенный логикой результат процесса познания действительности; адекватное ее отражение в сознании человека в виде представлений, понятий, суждений, теорий [23]. Знания фиксируются в форме знаков основе знаний вырабатываются умения и навыки. В наш век компьютеризации, век научно-технического прогресса знания необходимы каждому из нас. Еще в семнадцатом веке английский философ Ф. Бэкон утверждал: «Знание – сила».

Стремление к знанию одна из основных черт человека. Знать необходимо не для того, чтобы только знать, а для того, чтобы научиться что-то делать, чтобы получить профессию и заниматься любимым делом. Знания должны обязательно найти область применения, иначе они никакой пользы не принесут. Кто приобретает знания, но не пользуется ими, подобен тому, кто пашет, но не сеет «Мудр не тот, кто знает, а тот, чьи знания полезны», - сказал древний философ Эсхил. Всего знать никто не может. Но человек устроен так,

что он всю жизнь стремится что-то узнать, расширить свои познания. Останавливаться на достигнутом никогда нельзя [38].

Непосредственными целями любого учебного предмета являются усвоение учащимися системы знаний и овладение ими определенными умениями и навыками. При этом овладение умениями и навыками происходит на базе усвоения действенных знаний, которые определяют соответствующие умения и навыки, т.е. указывают, как следует выполнять то или иное умение или навык.

Для того чтобы разобраться в вопросе о путях и механизмах формирования у учащихся умений и навыков, надо сначала уяснить, что собой предоставляют умения и навыки.

До сих пор не уточнены соотношения между понятиями «умения» и «навыки». Большинство психологов и педагогов считают, что умение — более высокая психологическая категория, чем навыки. Педагоги-практики придерживаются обратной точки зрения: навыки представляют более высокую стадию овладения физическими упражнениями и трудовыми действиями, чем умения [39].

Одни авторы под умениями понимают возможность осуществлять на профессиональном уровне какую-либо деятельность, при этом умения формируются на базе нескольких навыков, характеризующих степень овладения действиями. Поэтому навыки предшествуют умению.

Другие авторы под умениями понимают возможность осуществлять какое-либо действие, операцию. По их понятию, умение предшествуют навыку, который рассматривается как более совершенная стадия овладения действиями.

Умение и навык есть способность совершать то или иное действие. Различаются они по степени (уровню) овладения данным действием.

Умение — это способность к действию, не достигшему наивысшего уровня сформированности, совершаемому полностью сознательно.

Навык — это способность к действию, достигшему наивысшего уровня сформированности, совершаемому автоматизировано, без осознания промежуточных шагов.

Когда человек читает книгу, контролируя смысловое и стилевое содержание ее, то считывание букв и слов происходит автоматически. Когда же он читает рукопись для выявления в ней опечаток, то контроль направлен уже на восприятие букв и слов, а смысловая сторона написанного уходит на второй план. Но в том и в другом случае человек умеет читать, и это умение у него доведено до уровня навыка [37].

Умение — это промежуточный этап овладения новым способом действия, основанным на каком-либо правиле (знании) и соответствующим правильному использованию знания в процессе решения определенного класса задач, но еще не достигшего уровня навыка. Умение обычно соотносят с уровнем, выражающимся на начальном этапе в форме усвоенного знания (правила, теоремы, определения и т.п.), которое понято учащимися и может быть произвольно воспроизведено. В последующем процессе практического использования этого знания оно приобретает некоторые операциональные характеристики, выступая в форме правильно выполняемого действия, регулируемого этим правилом. В случае каких-либо возникающих трудностей учащийся обращается к правилу с целью контроля за выполняемым действием или при работе над допущенными ошибками.

Навыки — это автоматизированные компоненты сознательного действия человека, которые вырабатываются в процессе его выполнения. Навык возникает как сознательно автоматизируемое действие и затем функционирует как автоматизированный способ его выполнения. То, что данное действие стало навыком, означает, что индивид в результате упражнения приобрел возможность осуществлять данную операцию, не делая ее выполнение своей сознательной целью [26].

Это значит, что когда мы формируем в процессе обучения у ученика способность совершать какое-то действие, то сначала он выполняет это

действие развернуто, фиксируя в сознании каждый шаг совершаемого действия. То есть способность выполнять действие формируется сначала как умение. По мере тренировки и выполнения этого действия умение совершенствуется, процесс выполнения действия свертывается, промежуточные шаги этого процесса перестают осознаваться, действие выполняется полностью автоматизировано — у ученика образуется навык в выполнении этого действия, т.е. умение переходит в навык (см. анимацию).

Но в ряде случаев, когда действие сложное, и его выполнение состоит из многих шагов, при любом совершенствовании действия оно остается умением, не превращаясь в навык. Поэтому умения и навыки различаются еще в зависимости от характера соответствующих действий.

Если действие элементарное, простое, используемое широко при выполнении более сложных действий, то его выполнение формируется обычно как навык, например, навык письма, чтения, устных арифметических действий над небольшими числами и т.д. Если же действие сложное, то выполнение этого действия, как правило, формируется как умение, в состав которого, входит один или несколько навыков [27].

Таким образом, термин «умение» имеет два значения:

1) Как первоначальный уровень овладения каким-либо простым действием. В этом случае навык рассматривается как высший уровень овладения этим действием, автоматизированное его выполнение: умение переходит в навык.

2) Как способность осознанно выполнять сложное действие с помощью ряда навыков. В этом случае навык — это автоматизированное выполнение элементарных действий, из которых состоит сложное действие, выполняемое с помощью умения [34].

На основе анализа сущности триады «знания-умения-навыки», мы сделали вывод о том, что вначале обучающийся получает и усваивает знания по дисциплине. Затем он овладевает способами управления этими знаниями и учится применять их на практике. Так формируются умения. Заключительный

этап учебного процесса – превращение связки из знаний и умений в устойчивый навык.

Большое значение в формировании всех типов умений и навыков имеют упражнения - целенаправленное систематическое повторение действий, благодаря которым происходит автоматизация навыков, совершенствование умений, деятельности в целом. Упражнения необходимы как на этапе выработки умений и навыков, так и в процессе их сохранения. Без постоянных, систематических упражнений умения и навыки обычно утрачиваются, теряют свои качества.

Важным средством формирования навыка служит речевая деятельность – словесное воспроизведение человеком наблюдаемых и выполняемых действий, а также идеальная деятельность – воспроизведение в «уме» образа действия, которое требуется совершить.

К условиям, обеспечивающим успешное формирования навыков, относится также число упражнений, их темп и распределение во времени. Важное значение имеет знание результата. Таким образом, основными *условиями* формирования навыков являются:

- четкость поставленной цели;
- планирование деятельности, осознание способа выполнения;
- контроль;
- самоконтроль;
- оценка деятельности.

Процесс формирования любого навыка складывается из нескольких этапов.

- структуризации (овладение обучающимся структурой и всеми операциями действия);
- автоматизации (доведение навыка до требуемой скорости, легкости, качеству выполнения);

– надежности («закалка» навыка усложнением условий и трудностей).

Соответственно подбираются и упражнения (кейсы): сначала — «на правильность», потом — «на правильность и скорость», наконец — «на надежность, при сохранении правильности и скорости».

Знания, умения и навыки в первую очередь помогают пользователю защитить себя и свои социальные сети, так как без них пользователи допускают ошибки, которые в дальнейшем приводят к угрозе [29].

1.3 Электронный учебно-методический комплекс как средство формирования навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации

В соответствии с требованиями стандарта профессиональной деятельности педагога возникает потребность в педагоге, способном к научно-исследовательской деятельности и научно-методической работе, обеспечивающем создание качественных учебно-методических комплексов, организацию познавательной деятельности студентов, расширение их кругозора.

В настоящее время значительно выросло требование к педагогическому обеспечению образовательного процесса. Педагогическая наука и практика убедительно доказывают, что качество образовательного процесса существенно повышаются, если его комплексное научно-методическое обеспечение осуществляется системно и на высоком уровне. В 2020 году электронно-методический комплекс стал как никогда актуальным, в связи с переводом всех учебных заведений на дистанционное обучение. Основным отличием грамотного педагога является то, что он не останавливается на достигнутом, а всегда в поиске нового: новых форм, методов и технологий. Он преобразует, модернизирует старые, хорошо зарекомендовавшие себя методы. В связи с требованием современности использует информационные технологии, повышающие уровень подготовки студентов [29].

Теоретический анализ современных исследований проблемы создания учебно-методического комплекса говорит о неоднозначности подходов к определению содержания этого понятия. Ученые освещают различные стороны и аспекты проблемы: управление самостоятельной деятельностью студентов (В. Б. Кричевский); создание модели программированного обучения (Л. С. Колмогоров); формирование положительной мотивации студентов (О. С. Гребенюк); повышение эффективности образовательного процесса (А. Ф. Щепотин); конструирование комплекса в соответствии с логикой образовательного процесса (А.И. Мищенко); функционирование совокупности средств обучения (В.М. Рябов, Б.В. Пальчевский, Л.С. Фридман); моделирование со- держания учебного материала и использование моделей на уроках (М. А. Галагузова); проектирование учебно-методического комплекса с использованием новых образовательных технологий (Т. О. Толстых).

В.М. Рябов представляет учебно-методический комплекс как совокупность средств обучения, используемых на различных этапах учебно-познавательного процесса и обеспечивающих единство педагогического воздействия.

Л.С. Фридман видит в нем фактор, необходимый для создания педагогических условий, в которых обучающий и обучающийся могли бы свободно развиваться. Он дает следующее определение:учебно-методический комплекс – это комплекс средств обучения (не набор), позволяющий преподавателю в рамках своего курса квалифицированно вести занятия.

Взгляд на учебно-методический комплекс как на педагогическую систему характерен для В. П. Беспалько, Ю. Г. Татур. Схожее представление о комплексе как системе, где все компоненты описаны в целостности, демонстрирует В. С. Ильин, основываясь при этом на системном подходе к педагогическим явлениям.

Согласно точке зрения этих ученых, учебно-методический комплекс рассматривается как определенная совокупность учебно-методических

документов, представляющих собой проект процесса обучения, который впоследствии будет реализован на практике. Необходимый же набор таких документов зависит от того, что должнобыть в нем спроектировано. Ответ на этот вопрос, по мнению В. П. Беспалько, может быть получен, если определить объект практической деятельности преподавателя. Такими объектами он называет педагогическую систему, создаваемую в ходе преподавания предмета, а также педагогическую систему учебного заведения в целом, складывающуюся из совокупности частных педагогических систем всех учебных предметов по данной специальности. Таким образом, «учебно-методический комплекс – это либо модель будущей педагогической системы изучения данной дисциплины, либо модель специальности в целом» Естественно, что составметодических документов, описывающих комплекс, зависит как от дисциплины, так и от специальности. В любом случае это должна бытьмодель принятой педагогической системы.

Вопрос конструирования учебно-методического комплекса как средства профессионального саморазвития студентов детально изучен в работах Л. Е. Солянкиной. Она определяет учебно- методический комплекс как средство учебно-методического обеспечения деятельности студента, состоящее из следующих элементов: лекции по предмету, методические рекомендации для выполнения практических работ, комплект контрольных заданий, задач, упражнений, методических рекомендаций для работы над курсовым и дипломным проектом. По ее мнению, условиями построения учебно-методического комплекса являются:

– выделение в содержании дисциплин отдельных элементов;

– проектирование матрицы взаимосвязи элементов содержания дисциплины с целью выделения ведущих знаний;

– формирование структуры наиболее общих способов познавательной деятельности, характерных для данной области знаний;

– построение системы частных задач, решаемых общими способами.

Немаловажное значение для педагогической науки имеет вопрос

классификации учебно-методических комплексов. Различают, например, методические комплексы занятия, темы, раздела, учебной дисциплины и системы дисциплин. В. М. Рябов предлагает следующую классификацию учебно-методических комплексов, разделяя их по характеру структуры формируемой профессиональнойдеятельности:

1. Формирующие практическую структуру профессиональной деятельности (практические и лабораторные работы, педагогические задачи).

2. Формирующие образные компоненты деятельности (кино- и видеофильмы, диафильмы, слайды и т. п.).

3. Формирующие понятийно-терминологические компоненты структуры деятельности (учебно-технологические и инструкционные карты, учебники, справочники, программированные материалы).

По мнению ученого, особого внимания заслуживает оценка качества разработанного комплекса. Он разрабатывается с целью системно-методического обеспечения учебного процесса. В немвоплощена принятая педагогическая система для организации образовательного процесса. О качестве комплекса можно судить теоретически и экспериментально, однако наиболее полная оценка может быть получена исходя из конечных результатов реального процесса обучения, реальных занятий.

Несмотря на различия в толковании понятия «учебно- методический комплекс», большинство авторов выделяют следующие условия его структурирования [31].

Это, во-первых, всесторонний учет характеристик педагогической среды, в пространстве которой развивается процесс обучения. Сбор материала о важнейших характеристиках педагогической среды может быть осуществлен по пяти позициям:

- уровень подготовленности студентов;
- скорость усвоения ими учебной информации;
- качество усвоения учебной информации за определенный

промежуток времени;

- особенности отношения к учебной деятельности;
- пробелы в знаниях.

Второе условие создания комплекса связано с требованиями адаптации процесса обучения к личности студента. Для этого необходимо учесть индивидуальный уровень обученности студента, мотивированность и подготовленность к познавательной деятельности [17].

Исходя из вышесказанного, формирование профессиональных знаний и умений студентов с помощью учебно-методического комплекса можно условно разделить на три этапа:

1. Формирование мотивации познавательной деятельности. Здесь осуществляется принятие целей обучения, формируется положительное отношение к процессу обучения, происходит осознание студентами важности и необходимости приобретения профессионально значимых знаний, умений.

2. Структурирование системы ориентиров для получения фундаментальных знаний и организация самостоятельной познавательной деятельности студентов с элементами самоконтроля. Правильно выбранная система ориентиров – основа для организации целенаправленного усвоения учебного материала. Она обеспечивает научно обоснованное использование комплекса, а также активность учащихся в познавательной творческой деятельности, продуктивность, творчество.

3. Самостоятельная деятельность студентов с элементами творчества, рефлексия полученных результатов. В системе профессионального образования самостоятельная познавательная деятельность субъекта образовательного процесса считается одним из основных видов деятельности, так как без нее не могут быть достигнуты общественно и личностно обусловленные цели обучения.

В структуру учебно-методического комплекса обычно включают инвариантный и вариативный компоненты. Инвариантный, общий для всех комплексов, отражает основные понятия, элементы, взаимосвязи;

вариативный учитывает особенности данного раздела, темы, его положение в матрице предмета [13].

Основные ошибки пользователей в социальных сетях:

1. Не храните информацию о паролях на компьютере, который используется для выхода в интернет. Конечно, лучше всего держать пароли в голове. Если же пароль слишком сложный, лучше запишите его отдельно на лист бумаги или в блокнот, и храните в надёжном месте. Пароли – являются основным способом защиты ваших личных данных в интернете, поэтому к ним нужно относиться с огромным вниманием.

2. Пользуйтесь двухэтапной аутентификацией — так ваши аккаунты будут надёжно защищены. Регулярно проверяйте почту и SMS-сообщения — если вам приходят подозрительные уведомления, вы всегда сможете пресечь попытки злоумышленников.

3. Не используйте для паролей информацию, которую злоумышленники могут найти самостоятельно: дату рождения, номера документов, телефонов, имена ваших друзей и родственников, адрес и так далее.

4. Придумывайте сложные пароли длиной не менее 8 символов с использованием заглавных и строчных букв, цифр, специальных значков %$#.

5. Не используйте одинаковые пароли на разных сайтах.

6. Регулярно меняйте пароли.

Несмотря на то, что в социальных сетях существует огромное количество киберугроз и мошенничества, разработчики не стоят на месте и с каждым годом улучшают работу защитных механизмов в сети. Но большинство взломов и атак происходят вовсе не по вине IT-специалистов, пользователи сами допускают ошибки в использовании социальных сетей [14].

Политика конфиденциальности — это документ, в котором декларируется IT-продукт — приложение или сайт. Его цель — информировать пользователя о том, как компания использует его данные. ПК

определяет, что относится к персональным данным пользователя, как владелец приложения или сайта их собирает, обрабатывает, хранит и кому передает.

Прежде чем установить приложение или браузерное расширение, воспользоваться онлайн-сервисом или зарегистрироваться в социальной сети, обязательно изучите политику конфиденциальности. Убедитесь, что приложение или сайт не получает права распоряжаться вашими личными данными — фотографиями, электронным адресом или номером телефона.

Разрешения для приложений. Многие приложения запрашивают данные об электронной почте или доступ к камере, фотогалерее и микрофону. Не выдавайте разрешений автоматически, следите за тем, какую информацию запрашивает приложение. В некоторых случаях разумнее вообще отказаться от его использования, чтобы не передавать личные данные о себе неизвестным лицам [19].

Настройки браузера. Не разрешайте браузеру автоматически запоминать пароли к личным сайтам и страницам, а лучше отключите эту опцию в настройках. Особенно это касается сайтов, где необходимо вводить номера документов или банковской карты. Автосохранение паролей увеличивает риск взлома личных страниц: если злоумышленник получит доступ к вашему компьютеру, ему не составит никакого труда извлечь эти данные из памяти браузера.

Отключите синхронизацию браузера на компьютере и в смартфоне. Если этого не сделать, при утере телефона все личные страницы и аккаунты станут доступны для посторонних.

Чистка cookies. Файлы cookies — это временные файлы интернета, которые хранятся на вашем устройстве и содержат информацию о сайтах, которые вы посещаете. Благодаря cookies сайты помнят ваши логины, пароли, электронную почту, историю интернет-заказов или состав корзины в интернет-магазине. С их помощью также можно отслеживать вашу активность в интернете, ваши интересы и предпочтения. Кроме того,

с помощью cookies можно взломать ваш почтовый ящик и получить доступ к личной информации. Время от времени удаляйте файлы cookies на компьютере и в смартфоне. Сделать это можно в настройках браузера.

Блокировка рекламы. Специальные программы, блокирующие рекламу, одновременно отслеживают попытки посторонних программ получить информацию с вашего компьютера, поэтому для защиты личных данных полезно скачать и установить такой блокировщик [10].

Защищённое соединение. Сайты, содержащие конфиденциальную информацию пользователей (сайты банков, государственных учреждений, онлайн-магазинов), обычно используют специальные протоколы передачи данных. При защищённом соединении данные шифруются с помощью технологии SSL, после чего информация становится недоступна для третьих лиц. Если в адресной строке браузера перед адресом сайта https:// вы видите зелёный замочек, значит, сайт использует защищённое соединение. Обращайте на это внимание, когда вводите на сайте логин, пароль, номер банковской карты или другие личные данные.

Домашний Wi-Fi. Пользоваться открытыми сетями Wi-Fi в кафе или торговом центре небезопасно, злоумышленники могут использовать их для взлома компьютера или смартфона и кражи паролей. В общественном месте не заходите на сайты, которые требуют ввода паролей и личных данных, делайте это по мобильной сети или через домашний Wi-Fi [21].

Выводы по первой главе

Изучение кибербезопасности у студентов стало предметом, требующим отдельного внимания, поскольку социальные сети стали не отъемлющей частью современного человека. Возникновение понятия кибербезопасности связано с изменением парадигмы образования; от усвоения знаний, умений, к развитию и совершенствованию навыков личной безопасности в социальных сетях у студентов.

В Российской Федерации уже сформировалась группа нормативных правовых актов, целью которых является защита детей от информации, причиняющей вред их здоровью и развитию (а именно Указ Президента РФ от 01.06.2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2012-2017 годы», Федеральный закон от29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон от27.07.2006 N 152-ФЗ (ред. от21.07.2014) «О персональных данных» (27 июля 2006 г.), Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».

Рассмотрев теоретические аспекты формирования навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации, мы изучили понятия «информационная безопасность» и «кибербезопасность». Мы выяснили какие виды угроз существуют в социальных сетях и какие ошибки допускают пользователи при использовании социальных сетей.

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ раскрывает термин «информационная безопасность детей» как «состояние защищенности 37 детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию».

Под «навыками кибербезопасности в социальных сетях у студентов профессиональной образовательной организации» понимаем способности обучающихся выявлять, идентифицировать и противостоять угрозам информационного воздействия в киберпространстве.

Мы выяснили, что электронный учебно-методический комплекс идеально подходит как средство формирования навыков кибербезопасности в социальных сетях, поскольку является совокупностью средств обучения, используемых на различных этапах учебно-познавательного процесса и обеспечивающих единство педагогического воздействия.

ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ФОРМИРОВАНИЮ НАВЫКОВ КИБЕРБЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ У СТУДЕНТОВ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ПРИ ПРЕПОДАВАНИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2.1 Проектирование и разработка электронного учебно-методического комплекса как средства формирования навыков кибербезопасности в социальных сетях

Современное общество требует от выпускников не только большой запас знаний самых разнообразных наук, но и качества свободной, творческой и ответственной личности, способной оптимально строить свою жизнь в быстроменяющемся информационном мире. А потому и современное образование должно строиться на формировании навыков саморазвития и самообразования, сотрудничества, творческого и критического мышления, самостоятельности и ответственности.

Все это требует внедрения новых педагогических технологий, лежащих в плоскости личностно ориентированного образования, для которых характерно сотрудничество участников образовательной деятельности, диалог, деятельностный и творческий характер, сотворчество учителя и ученика. Но организовать учебный процесс с максимальной эффективностью в современном профессиональном учебном заведении можно лишь с помощью современных ЭОР.

При выборе платформы для создания электронного учебно-методического комплекса был проведен анализ нескольких платформ.

Weebly.

Это бесплатный конструктор сайтов, для использования которого не нужно знание языков программирования. Интуитивно понятный сервис позволяет создавать и редактировать страницу при помощи перетаскивания и размещения элементов. Вы можете выбрать тему и оформление из

предложенных шаблонов, наиболее соответствующих вашему проекту. Их оформление отличается качеством и аккуратностью. Позволяет вести свой блог, создавать фото- и видеогалереи. Те, кто умеют пользоваться HTML, получают еще больше контроля над функционалом.

Явный плюс этого конструктора — дополнительный сервис Weebly for Education, который разработан специально для учителей и учеников. Ваш аккаунт Weebly расширяется дополнительными функциями. Преподаватель может создать страницы для себя и 40 своих учеников, которые может контролировать. Это очень удобно при работе над совместным проектом: ученики могут делиться своими наработками и идеями, обсуждать и развивать их.

Стоит отметить, что русская локализация выполнена лишь частично, но это не вызывает особых затруднений при регистрации и использовании сайта.

К сожалению, в связи со сложившимися обстоятельствами, данный сервис более не доступен на территории Российской Федерации.

Raptivity.

Raptivity это программное обеспечение для создания учебных пособий, которое можно использовать для разработки увлекательных и визуально стимулирующих онлайн-уроков. Инструмент имеет обширную библиотеку готовых интерактивных элементов, включая параллаксные дисплеи, панорамирующие слайды и интерактивные элементы 360. Даже не имея опыта в дизайне, каждый может создавать интерактивные викторины, игры, симуляции, флэшкарты и мозговые головоломки с помощью удобного интерфейса инструмента.

Вы можете максимально использовать многочисленные возможности этого инструмента, чтобы заинтересовать и мотивировать своих учеников на протяжении всего их учебного пути. Но важно отметить, что инструмент имеет некоторые ограничения по функциям, и вам может понадобиться загрузить дополнительные инструменты для разработки полноценного курса eLearning. Стоимость: 30 долларов США за пользователя в месяц [37].

MoodleCloud.

MoodleCloud бесплатная версия, действует 45 дней, она удобна тем, что ее не нужно скачивать на компьютер или устанавливать на сервер. За этот период можно опробывать абсолютно все возможности платформы, а они очень обширны.

Поддерживаемые форматы. Moodle поддерживает все современные форматы. SCORM, AICC и IMS поддерживаются по умолчанию, для xAPI нужен плагин (например, Logstore API).

Интеграция. Moodle легко интегрируется с другими системами и сервисами. Если нужно подключить CRM систему, можно воспользоваться Arlo или Edwiser Bridge (подключает все необходимое для eCommerce). WordPress также интегрируется через Edwiser Bridge. Вебинарные сервисы можно подключить через BigBlueButton или OpenMeetings.

Контент обучения. В Moodle можно загрузить любой тип контента: текстовый (включая PDF и XLS), изображения, презентации (через плагин Presentation), тесты и курсы. Видео можно загрузить просто так или для удобства подключить Medial — стриминговый видеосервис. Можно формировать планы обучения (learning plans).

Мобильное обучение. На смартфонах и планшетах Moodle можно открывать в мобильных браузерах Chrome и Safari или использовать приложение Moodle Mobile.

Отчетность. В Moodle можно выгружать любой вид отчета, но для этого нужен плагин. В данном случае плагин отвечает за дизайн отчета (график или таблица) и выгружаемую информацию (пользователи, учебные материалы, просмотры и т.п.).

Основные возможности MoodleCloud.

Создание онлайн-курсов. Текстовые документы, презентации и видео в Moodle можно объединить в обучающий курс, который будет доступен всем ученикам или отдельному классу.

Тестирование. В Moodle встроен редактор тестов. По умолчанию доступно 15 типов заданий: от выбора одного правильного ответа до перетаскивания объектов. Чтобы ученики не списывали, можно ограничить время на решение теста и число попыток.

Система автоматически проверяет ответы, показывает допущенные ошибки и указывает набранный балл.

Форум и комментарии. Чтобы связаться с преподавателем, задать вопрос или обсудить тему урока, ученики могут оставлять комментарии под курсами или заводить беседы на встроенном форуме.

База знаний — это архив учебных материалов, круглосуточно доступный всем пользователям. В любой момент ученики могут зайти в базу знаний и найти нужный доклад, видеоурок или статью.

Мобильное обучение. У сервиса есть мобильное приложение Moodle Mobil, которое позволяет проходить курсы и решать тесты с планшета или смартфона.

Статистика по обучению. Moodle отслеживает успеваемость учеников и составляет отчёты для преподавателей. Например, показывает, сколько времени ребята проходили курс, какие ошибки допустили в тесте, кому нравится учиться, а кому нет.

Школам, вузам и колледжам. Сервис поможет запустить смешанное обучение — это когда ученики изучают теорию дистанционно, а практику отрабатывают в классе. Учителя могут создавать в Moodle онлайн-курсы отдельно под каждый предмет или класс, тестировать школьников и студентов, проводить вебинары. В большинстве учебных заведений ее используют как основную.

Коммерческим компаниям. Через Moodle бизнес может дистанционно учить сотрудников продуктам компании, стандартам работы и регламентам.

Это универсальная и удобная платформа, поэтому выбор платформы для разработки пал на нее.

Переходим к процессу создания курса, так как платформа полностью переведена на множество языков, в том числе и на русский, то создавать и разрабатывать, а ней очень понятно и просто. Нам, как новым пользователям, требуется зарегистрироваться на новой платформе и создать новый аккаунт.

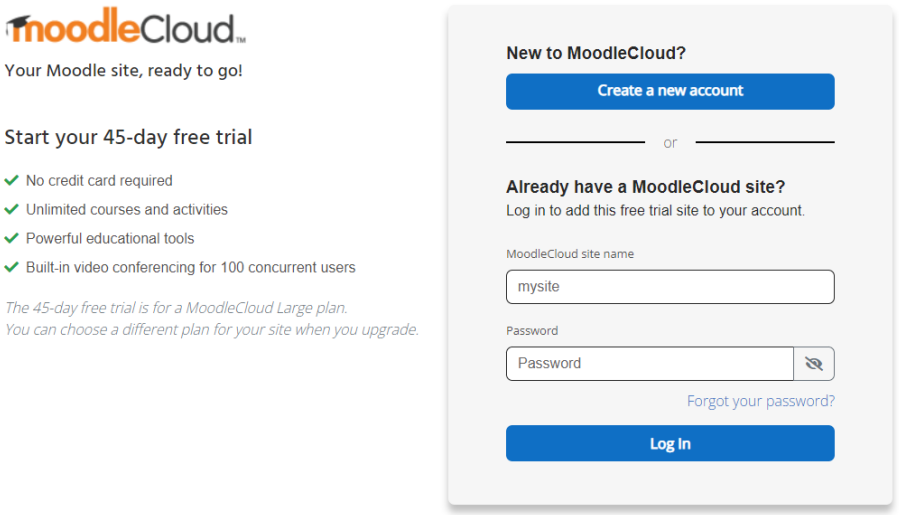


Рисунок 2.1. – Создание нового аккаунта

Далее на странице для регистрации требуется внести свое имя и фамилию, электронный почтовый адрес, страну проживания, придумываете имя сайту и пароль.

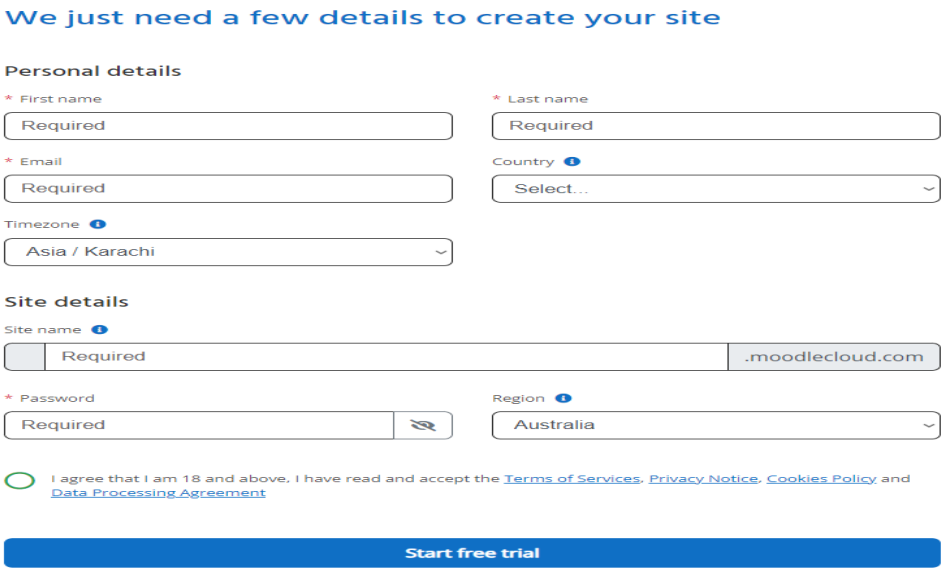


Рисунок 2.2. – Регистрация в MoodleCloud

Сайт высылает на почту вам ссылку подтверждения регистрации, после перехода по ней можно начать работу по созданию курса.

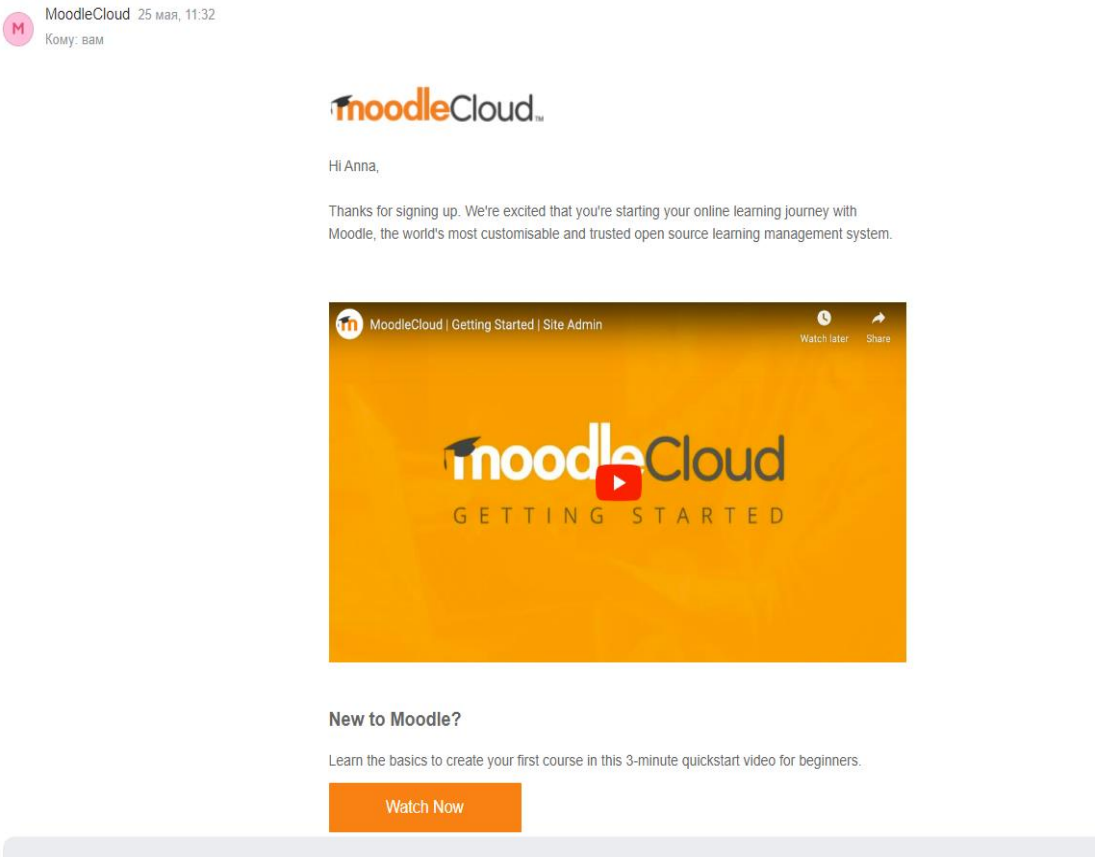


Рисунок 2.3. – Подтверждение регистрации

После того, как мы войдем в аккаунт мы оказываемся на главной странице, переходим во вкладку администрирование, раздел курсы, добавить курс.

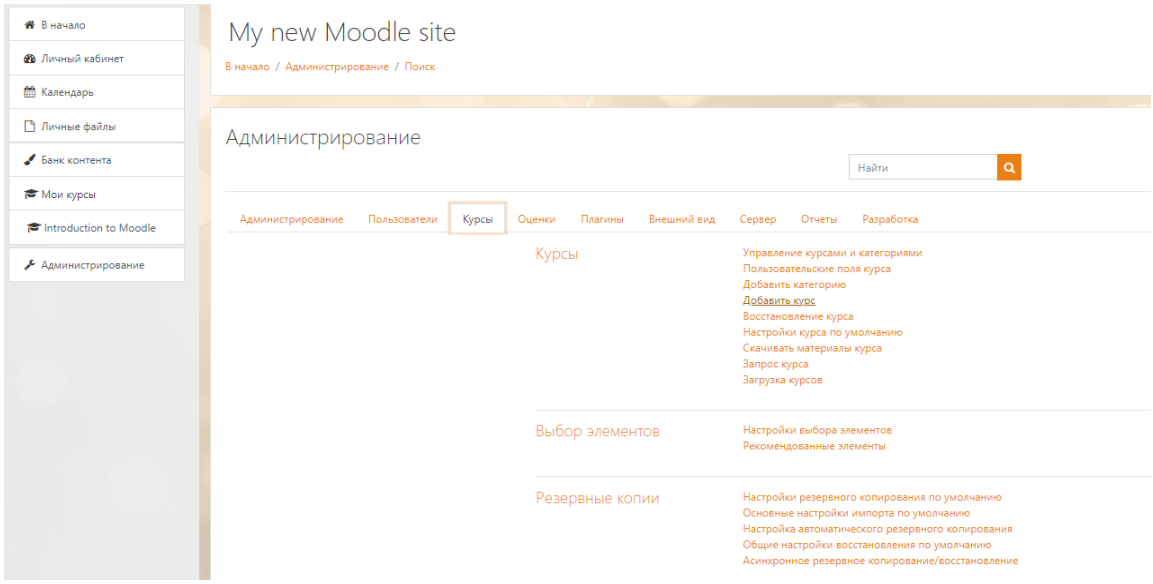


Рисунок 2.4. – Администрирование курса

Вносим название курса, номер, описание (по желанию).

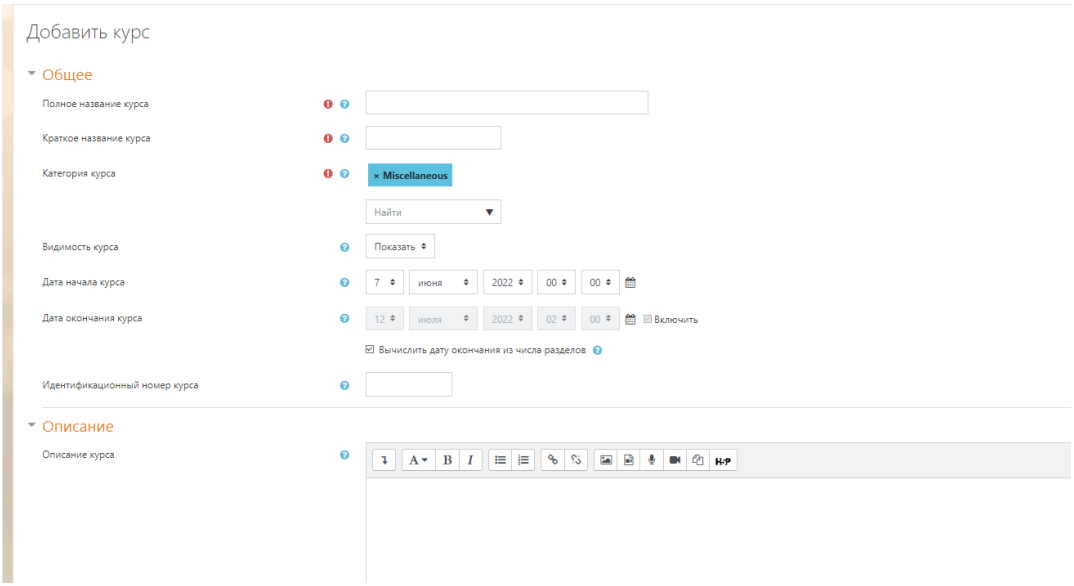


Рисунок 2.5. – Добавление курса

Далее мы можем создать в программе любой элемент или ресурс для любого раздела. Возможности MoodlCloud обширны, в дополнение возможность интеграции документов других форматов, чем мы и руководствовались при создании учебно-методического комплекса.

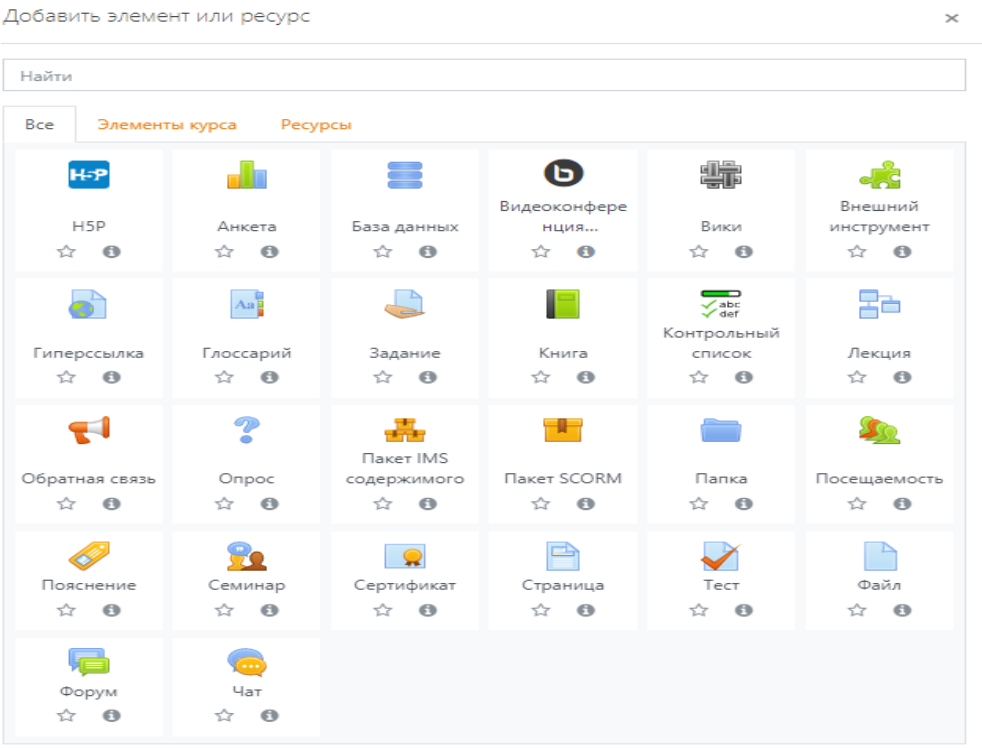


Рисунок 2.6. – Добавление в курс учебного элемента

2.2 Структура и содержание электронного учебно-методического комплекса дисциплины «Информационная Безопасность» как средство формирование навыков кибербезопасности

Для того, чтобы определить структуру и содержание учебно-методического комплекса по дисциплине ОП.13 «Информационная безопасность» по разделу «Виды угроз информационной безопасности», мы определись с нормативной базой дисциплины.

Предлагаемый учебно-методический комплекс предназначен для организации аудиторной и внеаудиторной самостоятельной работы обучающихся.

В комплексе представлен опросник для определения уровня киберграмотности у студентов, теоретический материал, словарь терминов, кейс-задания и итоговой тест для определения уровня навыков.

Предлагаемый учебно-методический комплекс предназначен для формирования навыков, для получения новых знаний, осуществления само и взаимоконтроля знаний студента

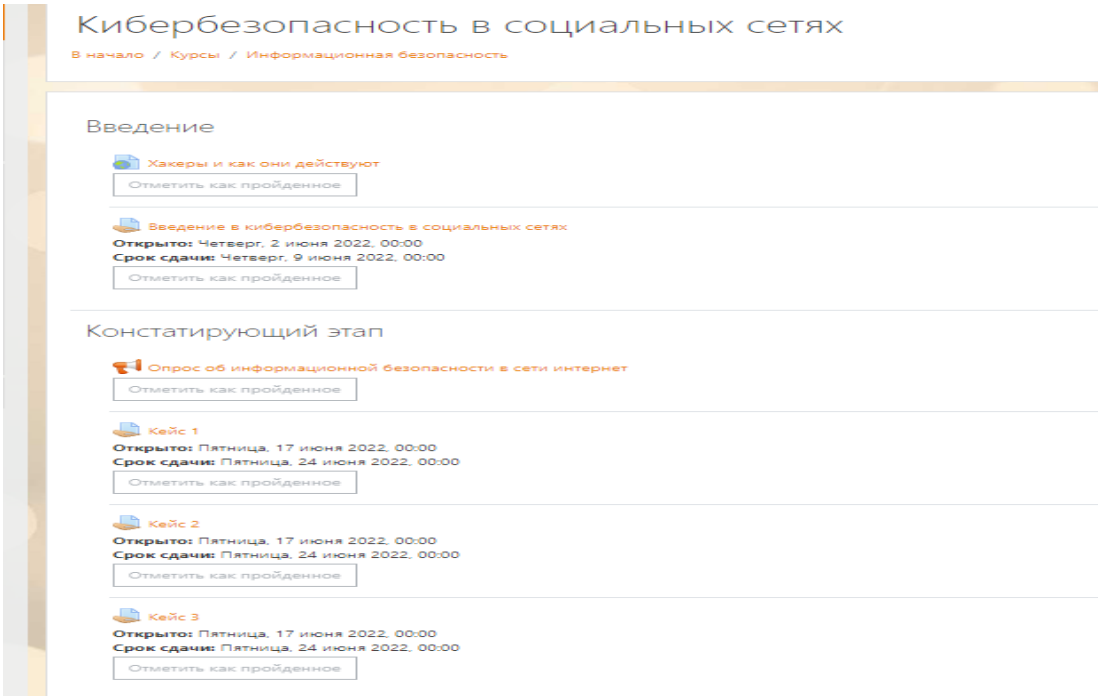


Рисунок 2.7. – Содержание курса

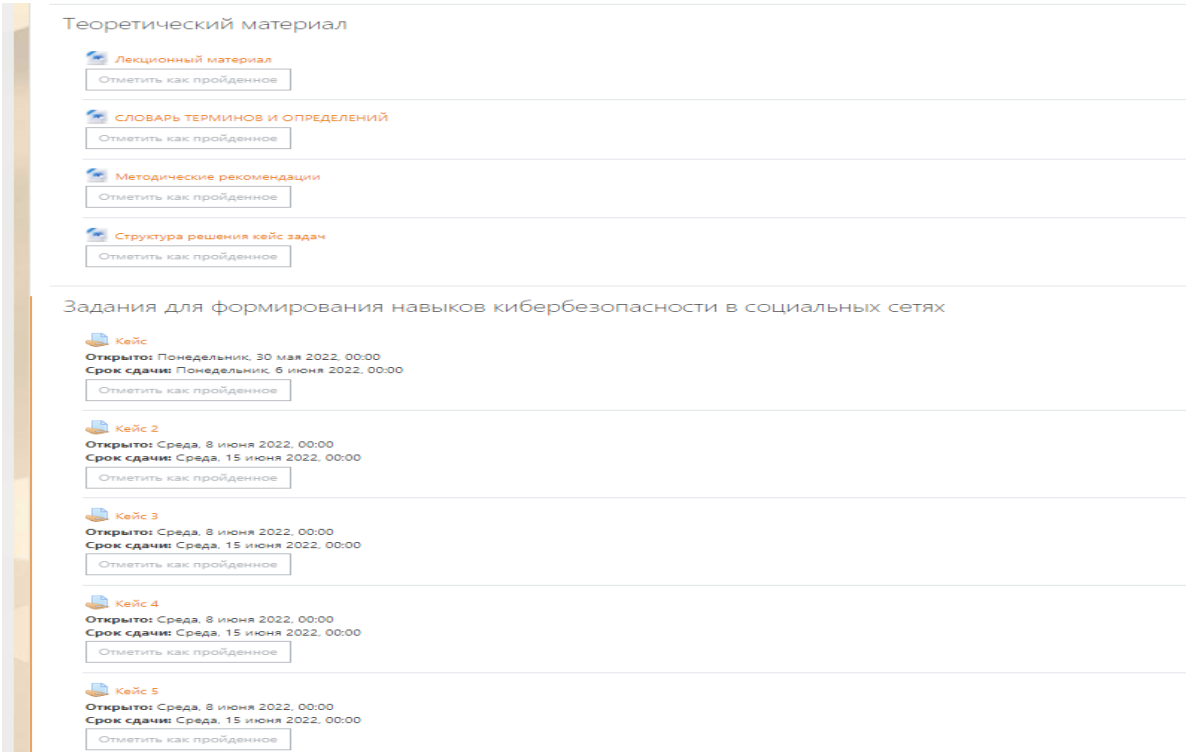


Рисунок 2.8. – Содержание курса (2)

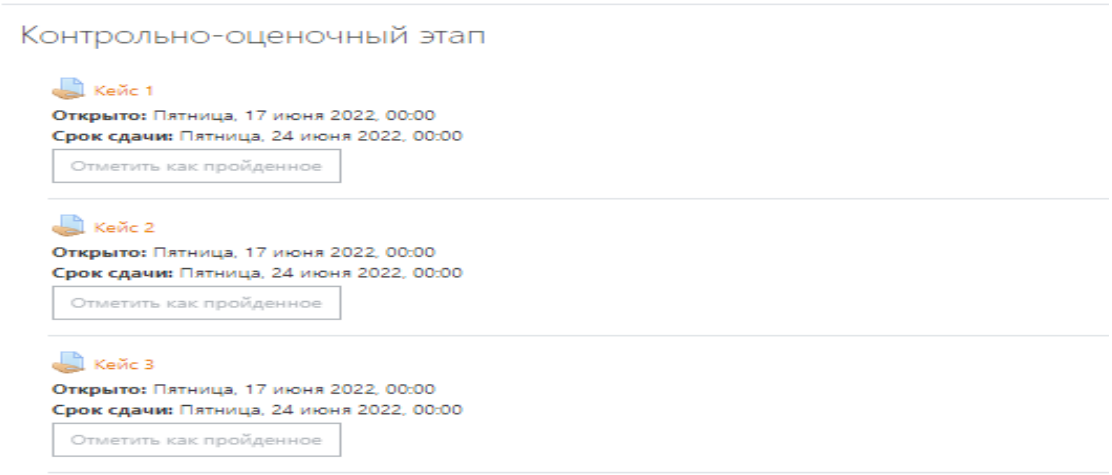


Рисунок 2.9. – Содержание курса (3)

На первой странице сайта – «Введение в кибербезопасность в социальных сетях» описано основное предназначение учебно-методического комплекса. Так же имеется дополнительно видеоматериал «Хакеры Killnet», в котором можно узнать о современных хакерских группировках и их методы информационных атак.

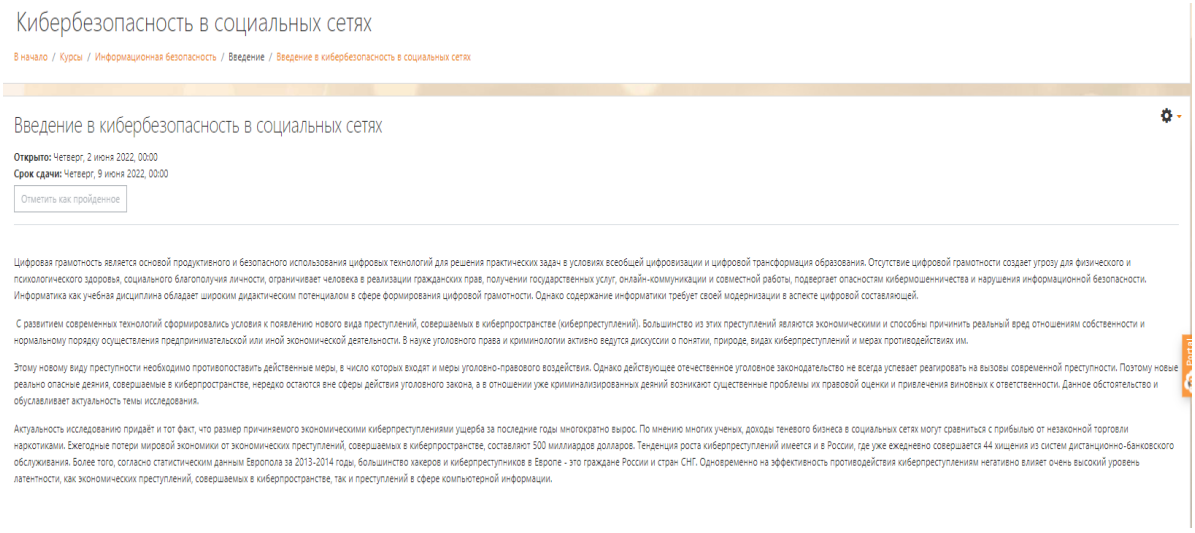


Рисунок 2.10. – Введение

После введения мы переходим к опроснику, чтобы определить уровень имеющихся знаний у студентов колледжа. Опрос состоит из 11 вопросов.

Данный опрос внесен в электронный учебно-методический комплекс для отслеживания поведения студентов в социальных сетях. Студенты проходят его не на оценку, таким образом мы получаем максимально реальные и честные результаты и в дальнейшем можем проанализировать их.

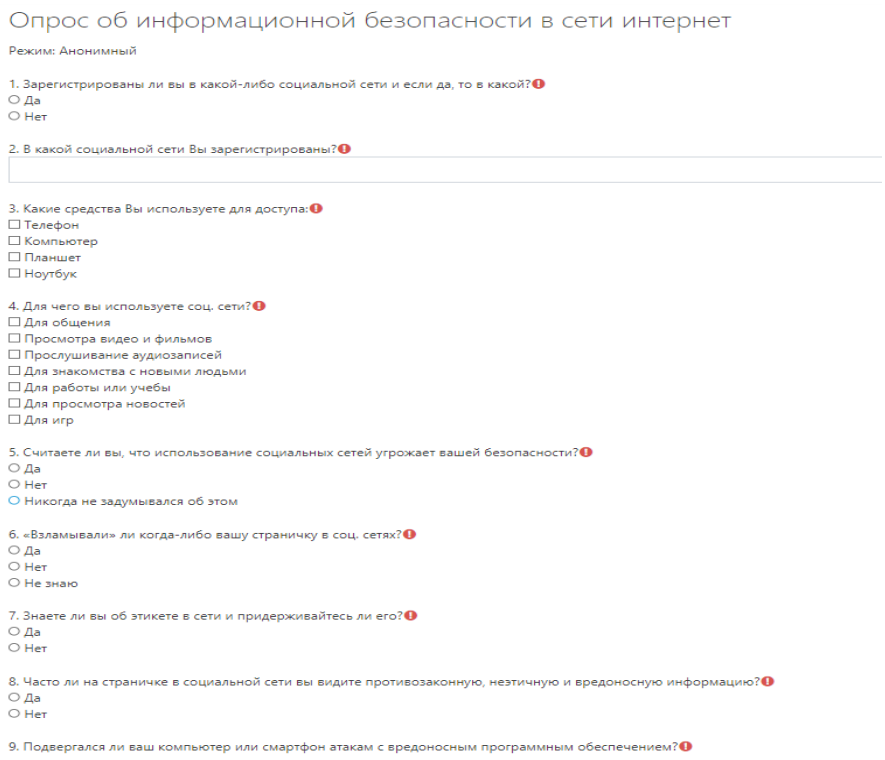


Рисунок 2.11. – Опросник

После опроса идет анализ результатов отвечающих, опрос полностью анонимный, поэтому мы может только отследить сколько человек ответили на

тот или иной вопрос и что они выбрали, тем самым отслеживаем статистику знаний по кибербезопасности у студентов двух групп. Сайт для удобства позволяет результаты опроса экспортировать в Excel.

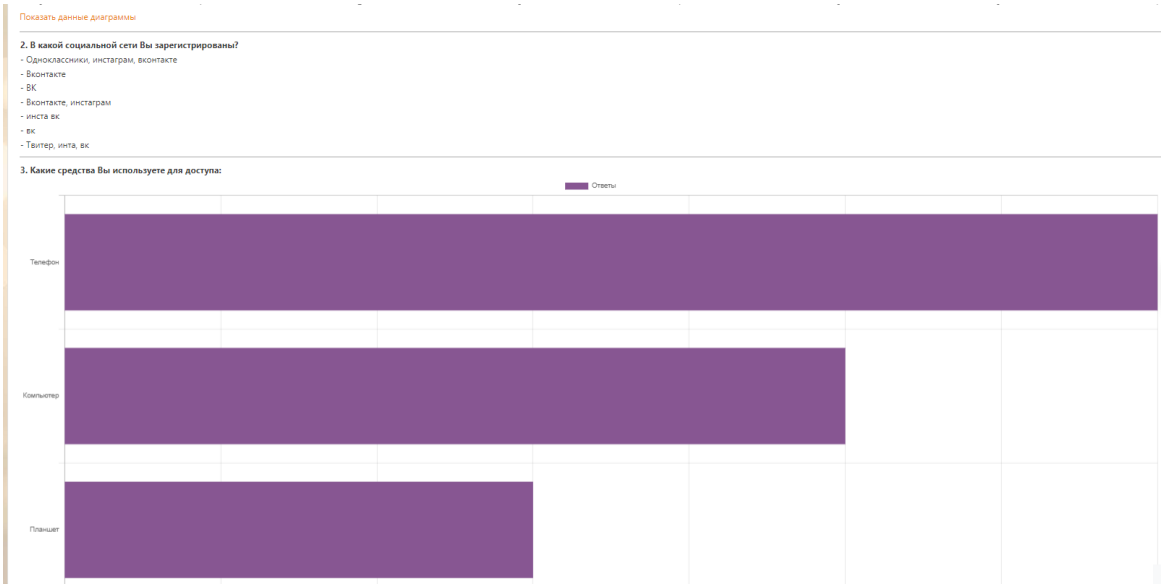


Рисунок 2.12. – Результаты ответов

Пятница, 18 март 2022, 14:15								
Отправлено ответов: 15								
Вопросов: 11								
Метка	**Вопрос**	**Ответы**						
	Зарегистрированы ли вы в какой	**Да**	**Нет**					
		15	0					
	В какой социальной сети Вы заре	**ВК**						
		вк						
		Вконтакте, инстаграм						
		инста вк						
		Одноклассники, инстаграм, вконтакте						
		Твитер, инта, вк						
		Вконтакте						
	Какие средства Вы используете д	**Телефон**	**Компьютер**	**Планшет**	**Ноутбук**			
		15	15	6	10			
	Для чего вы используете соц. сети	**Для общения**	**Просмотра виде**	**Прослушивание**	**Для знакомства**	**Для работы или**	**Для просмотра н**	**Для игр**
		15	10	12	8	13	8	3
	Считаете ли вы, что использовани	**Да**	**Нет**	**Никогда не задумывался об этом**				
		5	3	7				
	«Взламывали» ли когда-либо ваш	**Да**	**Нет**	**Не знаю**				
		13	1	1				
	Знаете ли вы об этикете в сети и	**Да**	**Нет**					
		12	3					
	Часто ли на страничке в социалы	**Да**	**Нет**					
		5	10					
	Подвергался ли ваш компьютер и	**Да**	**Нет**					
		13	2					
	Знаете ли вы о правилах безопасн	**Да**	**Нет**					
		13	2					
	Проводятся ли в вашей образоват	**Да**	**Иногда**	**Нет**	**Никогда**			
		7	8	0	0			

Рисунок 2.13. – Результаты в таблице Excel

Далее мы проверяем сформированность навыков кибербезопасности в социальных сетях у студентов двух групп на констатирующем этапе. Для этого студенты выполняют кейс-задания.

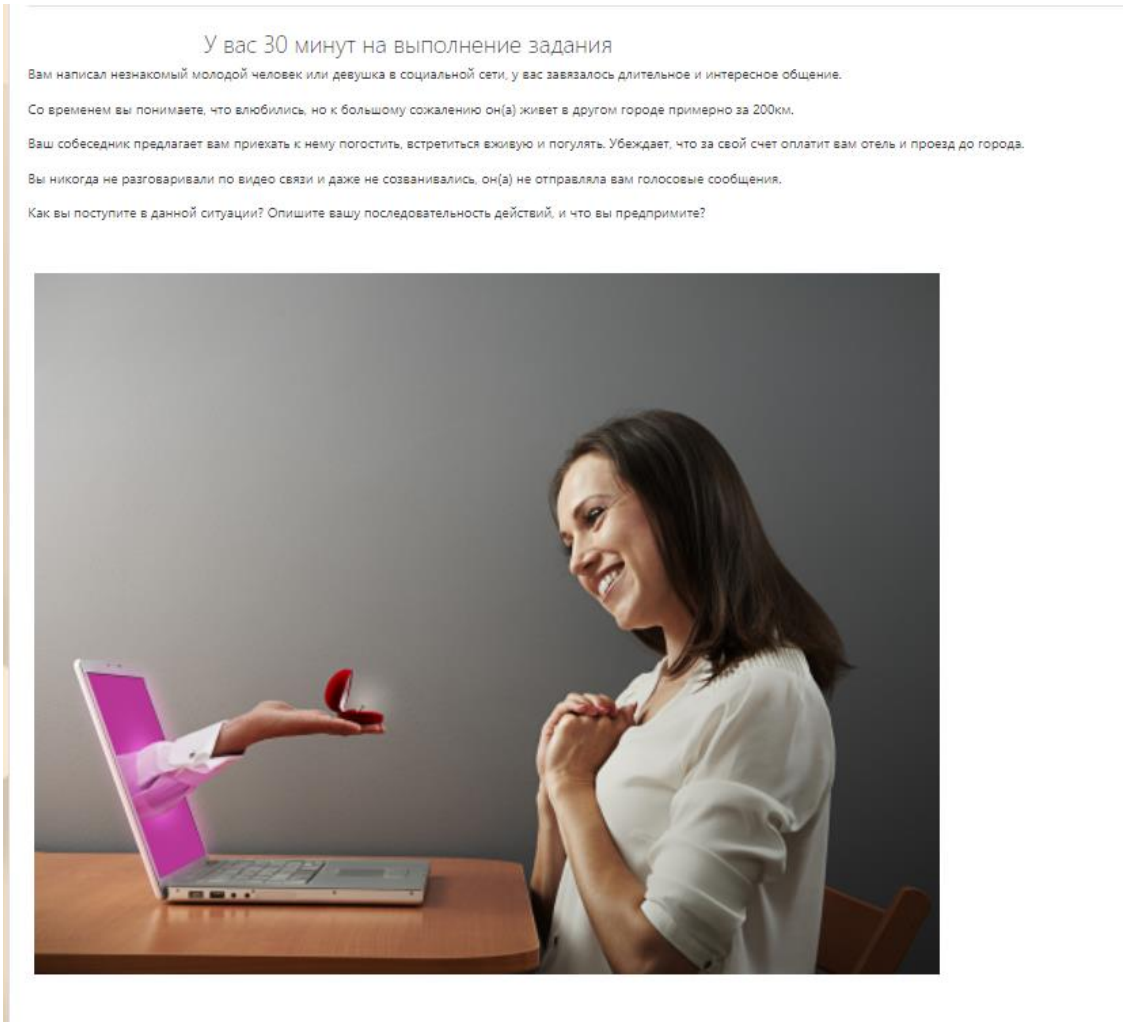


Рисунок 2.14. – Кейс 1. Констатирующий этап

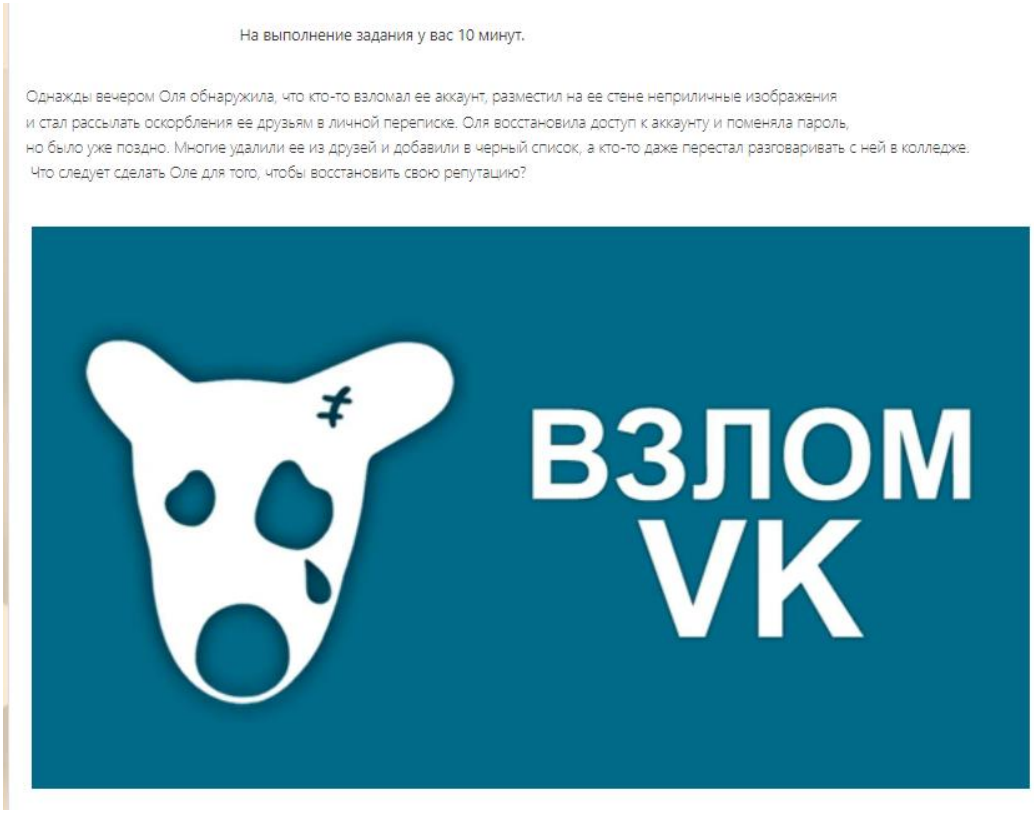


Рисунок 2.15. – Кейс 2. Констатирующий этап

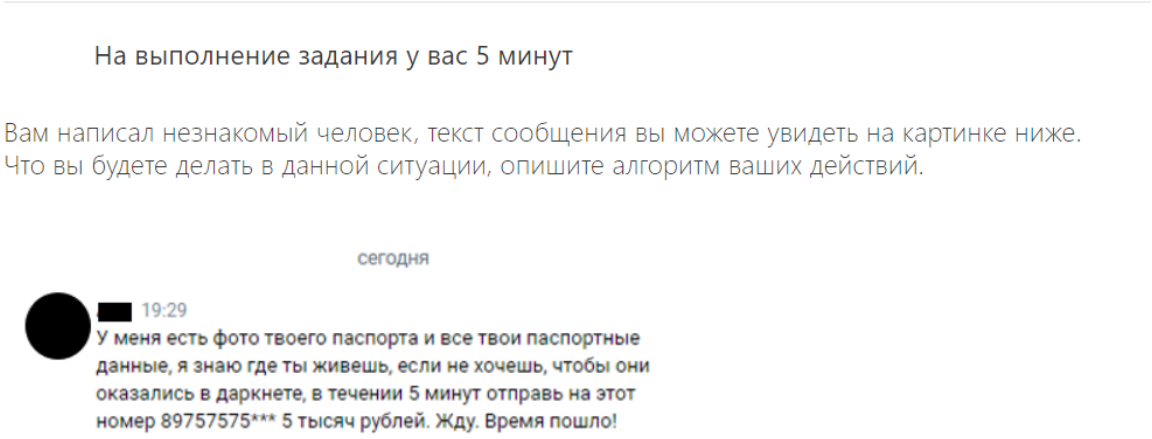
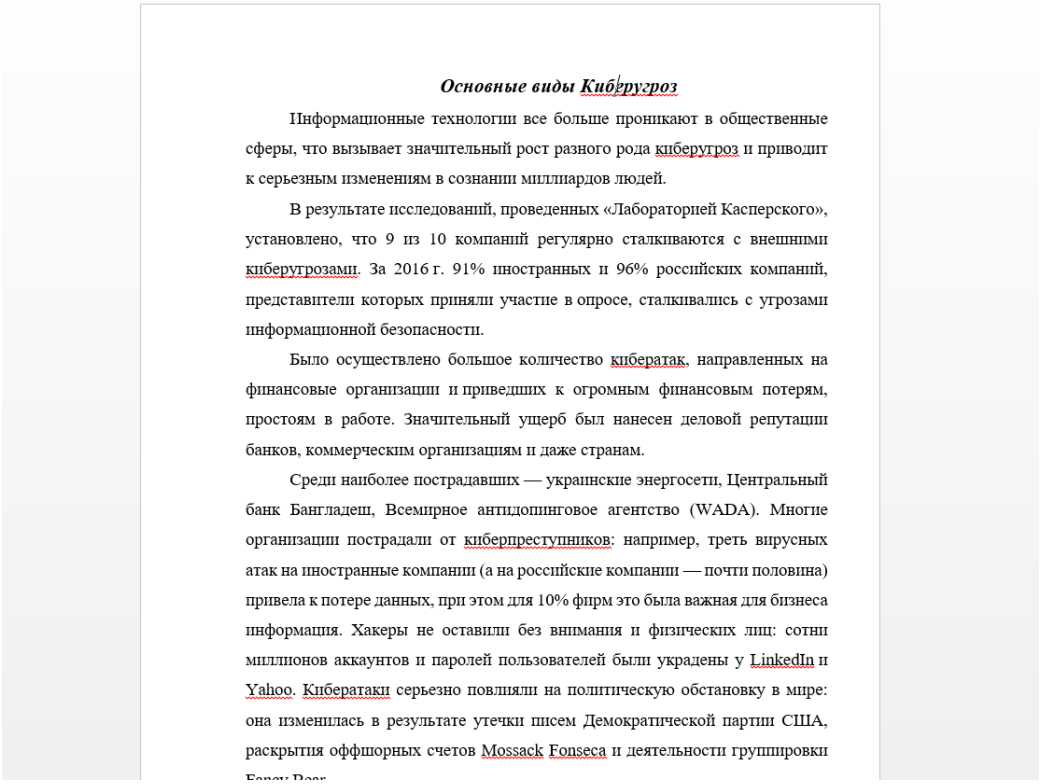


Рисунок 2.16. – Кейс 3. Констатирующий этап

Далее мы переходим к теоретическому материалу. В данном разделе располагается лекционный материал и также словарь терминов, и методические рекомендации, которые используются в теоретической части. В этом разделе так же находится документ Сайт MoodleCloud позволяет

интегрировать файлы в систему, поэтому этот раздел представлен на сайте в формате Word. Данный формат был выбран для того, чтобы студенты могли скачать себе нужные документы для самостоятельного повторения.



***Основные виды Кибе*ругроз**

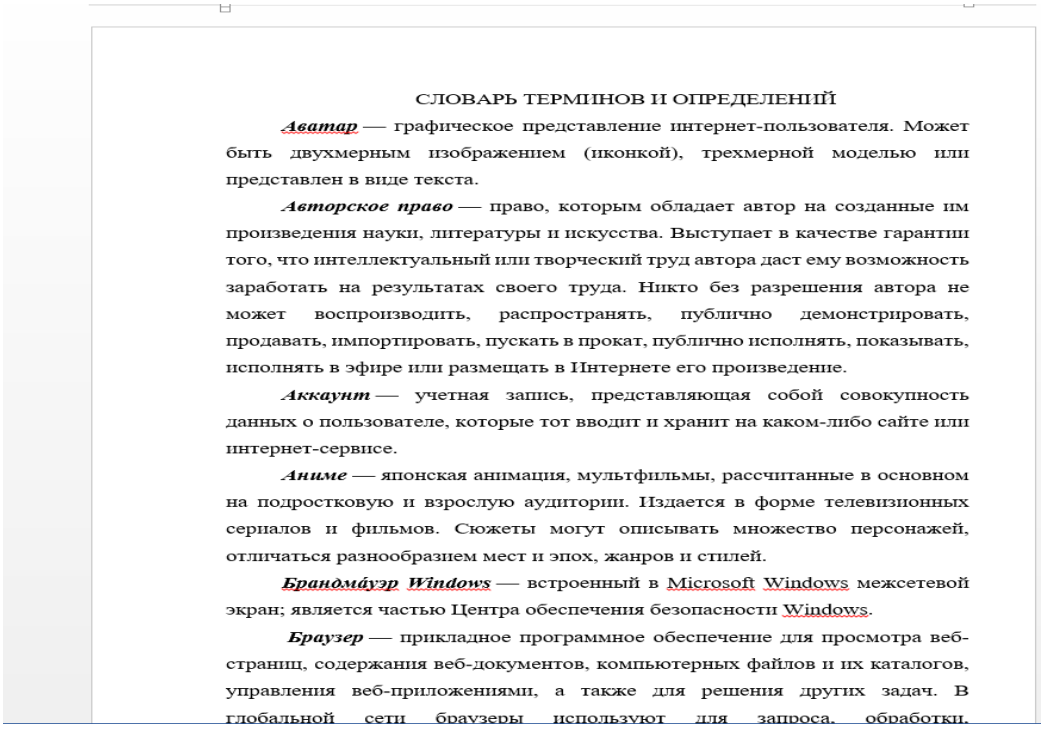
Информационные технологии все больше проникают в общественные сферы, что вызывает значительный рост разного рода киберугроз и приводит к серьезным изменениям в сознании миллиардов людей.

В результате исследований, проведенных «Лабораторией Касперского», установлено, что 9 из 10 компаний регулярно сталкиваются с внешними киберугрозами. За 2016 г. 91% иностранных и 96% российских компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности.

Было осуществлено большое количество кибератак, направленных на финансовые организации и приведших к огромным финансовым потерям, простоям в работе. Значительный ущерб был нанесен деловой репутации банков, коммерческим организациям и даже странам.

Среди наиболее пострадавших — украинские энергосети, Центральный банк Бангладеш, Всемирное антидопинговое агентство (WADA). Многие организации пострадали от киберпреступников: например, треть вирусных атак на иностранные компании (а на российские компании — почти половина) привела к потере данных, при этом для 10% фирм это была важная для бизнеса информация. Хакеры не оставили без внимания и физических лиц: сотни миллионов аккаунтов и паролей пользователей были украдены у LinkedIn и Yahoo. Кибератаки серьезно повлияли на политическую обстановку в мире: она изменилась в результате утечки писем Демократической партии США, раскрытия оффшорных счетов Mossack Fonseca и деятельности группировки

Рисунок 2.17. – Лекционный раздел



СЛОВАРЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Аватар — графическое представление интернет-пользователя. Может быть двухмерным изображением (иконкой), трехмерной моделью или представлен в виде текста.

Авторское право — право, которым обладает автор на созданные им произведения науки, литературы и искусства. Выступает в качестве гарантии того, что интеллектуальный или творческий труд автора даст ему возможность заработать на результатах своего труда. Никто без разрешения автора не может воспроизводить, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать, исполнять в эфире или размещать в Интернете его произведение.

Аккаунт — учетная запись, представляющая собой совокупность данных о пользователе, которые тот вводит и хранит на каком-либо сайте или интернет-сервисе.

Аниме — японская анимация, мультфильмы, рассчитанные в основном на подростковую и взрослую аудитории. Издается в форме телевизионных сериалов и фильмов. Сюжеты могут описывать множество персонажей, отличаться разнообразием мест и эпох, жанров и стилей.

Брандма́уэр Windows — встроенный в Microsoft Windows межсетевой экран; является частью Центра обеспечения безопасности Windows.

Браузер — прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач. В глобальной сети браузеры используют для запроса, обработки,

Рисунок 2.18. – Словарь

Методические рекомендации для обучающихся

Как вести себя в социальных сетях

Социальные сети так прочно вошли в нашу жизнь, что многие люди работают и общаются там постоянно. Например, в Facebook уже зарегистрирована седьмая часть жителей планеты, а это около 1 млрд человек. Помните, что информация, размещенная в социальных сетях, может быть найдена и использована кем угодно, в том числе с недобрыми намерениями.

• Следует ограничить список друзей, среди них не должно быть случайных и незнакомых людей.

• Не указывать в социальных сетях пароли, телефоны, адреса, дату рождения, другую личную информацию и информацию о своей семье.

• Прежде чем что-то опубликовать, написать и загрузить, необходимо подумать, нужно ли, чтобы это видели другие пользователи.

• При общении с незнакомыми людьми не использовать свое реальное имя и другую личную информацию, не называть место жительства, место учебы или работы.

• Не размещать в Интернете фотографии, по которым можно определить ваше местоположение.

• При регистрации в социальной сети использовать только сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

• Для социальной сети, почты и других сайтов использовать разные

Рисунок 2.19. – Методические рекомендации для обучающихся

Констатирующий этап

Кейс 1

Вам написал незнакомый молодой человек или девушка в социальной сети, у вас завязалось длительное и интересное общение. Со временем вы понимаете, что влюбились, но к большому сожалению он(а) живет в другом городе примерно за 200км.

Ваш собеседник предлагает вам приехать к нему погостить, встретиться вживую и погулять. Убеждает, что за свой счет оплатит вам отель и проезд до города. Вы никогда не разговаривали по видео связи и даже не созванивались, он(а) не отправляла вам голосовые сообщения. Как вы поступите в данной ситуации? Опишите вашу последовательность действий, и что вы предпримите?

Структура решения:

1. Предложить собеседнику созвониться по видео связи
2. Объяснить, что вы не готовы ехать в другой город к малознакомому человеку
3. Предложить в качестве альтернативы, чтобы собеседник сам приехал к вам
4. В случае отказа от вышеперечисленных действий, заблокировать собеседника в социальной сети
5. Закрыть социальную страницу, для того, чтобы вам не писали незнакомые люди

Кейс 2

Однажды вечером Оля обнаружила, что кто-то взломал ее аккаунт, разместил на ее стене неприличные изображения и стал рассылать оскорбления ее друзьям в личной переписке. Оля восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили ее из друзей и добавили в черный список, а кто-то даже перестал разговаривать с ней в колледже. Что

Рисунок 2.20. – Структура решения кейс-задач

Далее мы переходим в раздел «Задания для формирования навыков кибербезопасности в социальных сетях», где представлены кейс-задания. В данном разделе представлено 5 разных заданий. Все задания взяты из реальных ситуаций и опыта разных людей.

Ситуация, которая представлена на рисунке 2.21, ее можно разыграть в паре на занятии или же предложить разобрать ситуацию со студентами.

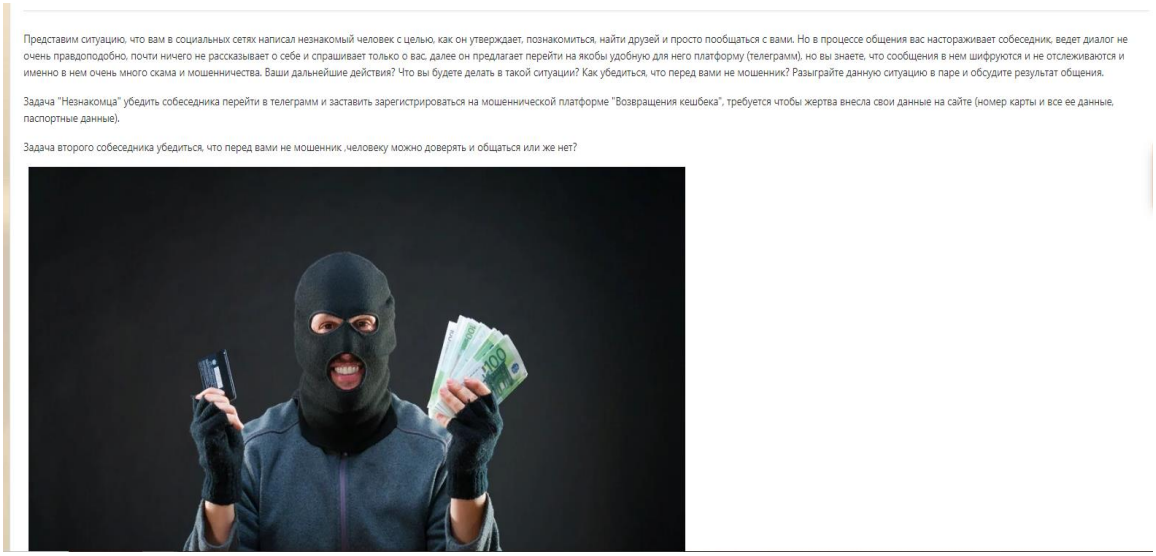
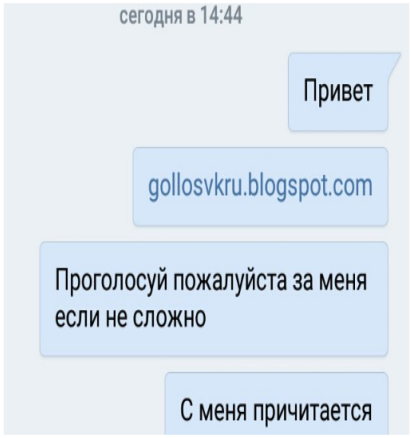


Рисунок 2.21. – Кейс 1



Вам приходит сообщение от вашего близкого друга в социальной сети, он просит вас перейти по ссылке и проголосовать за него в конкурсе на самое креативное фото. Вы внимательно изучаете ссылку и не понимаете, на какой сайт ведет данная ссылка, она отличается от ссылки социальной сети в которой вы ведёте переписку, но вы очень хотите помочь другу в его достижениях. Что же вы будете делать? Как вам убедиться в безопасности данной операции?

Рисунок 2.22. – Кейс 2

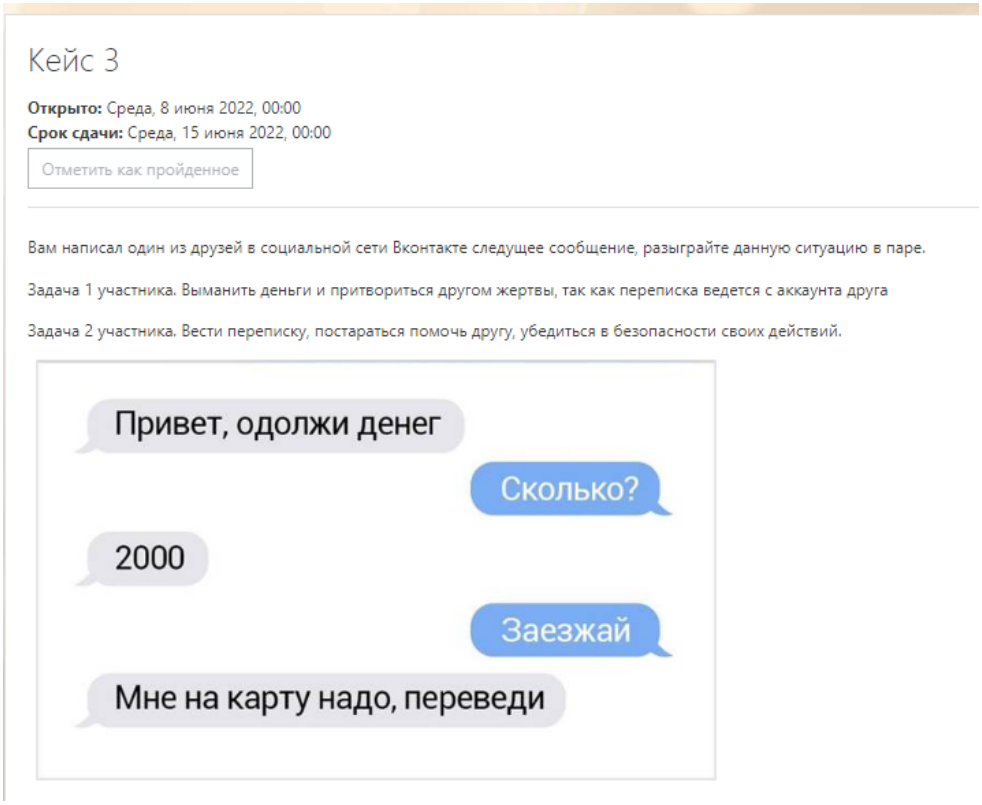


Рисунок 2.23. – Кейс 3

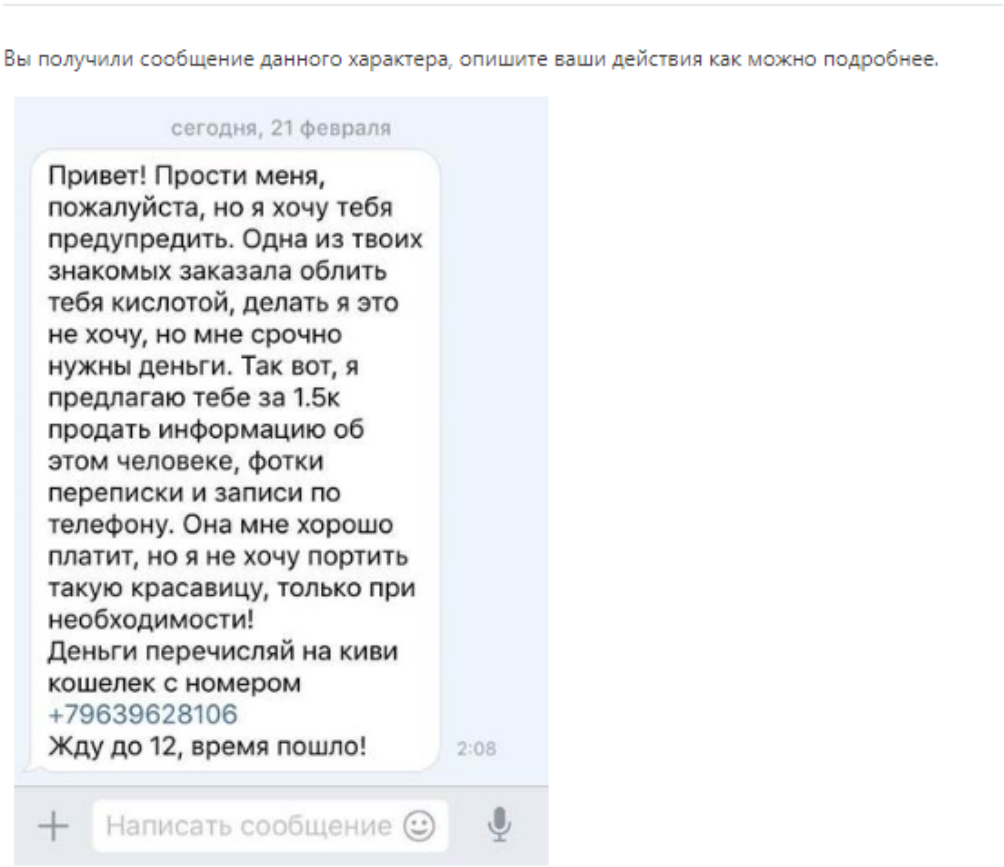


Рисунок 2.24. – Кейс 4

Ваш аккаунт в социальной сети взломали, какими способами вы будете восстанавливать доступ?

Что следует предпринять в следующий раз при регистрации и настройки аккаунта, что бы снизить риск до минимума?

Что не следует делать, чтобы не подвергать себя риску взлома социальной сети?

Рисунок 2.25. – Кейс 5

Последний раздел нашего электронного учебно-методический комплекса является контрольно-оценочный этап. В данном разделе представлены три кейс-задания, по результатам которых мы выявляем сформированность навыков кибербезопасности в социальных сетях.

На решение задачи дано 30 минут

Вам приходит сообщение в социальной сети с официальной страницы, пишет вам один из администраторов сайта, о том, что на вашем аккаунте успешно сменен пароль, но вы точно не меняли его. Через 30 минут будет заменена привязка номера телефона к странице в социальной сети, если вы хотите отменить данную операцию по смене номера перейдите по указанной ссылке "cancellation/fanktion840_283838.com".

Как следует поступить в данной ситуации? Опишите порядок ваших действий.

Рисунок 2.26. – Кейс 1. Контрольно-оценочный этап

На решение задачи дано 10 минут

Ваш друг присылает вам сообщение в социальной сети, вы общаетесь, он хвастается вам своими новыми стикерами, которые получил бесплатно. Вам эти стикеры тоже понравились и вы спрашиваете у друга где их можно получить? Он говорит, что выиграл их на сайте и прилагает в сообщении ссылку на розыгрыш. Вы переходите по данной ссылке, открываете подарок с призом. Вам выпадают стикеры, даже лучше чем у друга, вам они очень понравились, сайт для получения стикеров переводит вас на страницу социальной сети для авторизации. Вы вводите свой логин и пароль, вам выскакивает сообщение о том что стикеры получены на страницу. Вы закрываете браузер и переходите в приложение социальной сети. Заходите в свой набор стикеров и не обнаруживаете их в коллекции. Вы решаете, что стикеры придут вам позже и со спокойной душой ложитесь спать. На следующий день вы не можете зайти на свою страницу. Опишите в чем может заключаться данная проблема, если ваш аккаунт взломали, то каким образом, вы же все делали по инструкции?

Рисунок 2.27. – Кейс 2. Контрольно-оценочный этап

На выполнение задания дано 5 минут

На основании отработанных навыков кибербезопасности в социальных сетях, опишите любую мошенническую схему и метод борьбы с ней.

Нельзя использовать задачи из контрольно-оценочного блока.

У вас все получится!
Удачи вам!

Рисунок 2.28. – Кейс 3. Контрольно-оценочный этап

Разработанный нами электронный учебно-методический комплекс является одним из инструментов формирования навыков и получения

дополнительных знаний по кибербезопасности в социальных сетях у студентов по дисциплине «Информационная безопасность». Опрос, который проходит каждый студент, позволяет отслеживать уровень знаний о кибербезопасности до начала прохождения курса, кейс-задания выявляют и формируют навыки кибербезопасности в социальных сетях, а теоретический материал дает знания для дальнейших действий в случае киберугроз в социальных сетях.

2.3 Диагностика навыков кибербезопасности в социальных сетях у студентов с использованием электронного учебно-методического комплекса по дисциплине «Информационная безопасность»

Процесс формирования любого навыка складывается из нескольких этапов.

– структуризации (овладение обучающимся структурой и всеми операциями действия);

– автоматизации (доведение навыка до требуемой скорости, легкости, качеству выполнения);

– надежности («закалка» навыка усложнением условий и трудностей).

Упражнения (кейсы) помогают в формировании навыков будущих специалистов, развивают творческое мышление, логику и последовательность действий при угрозах в социальных сетях, студенты при прохождении кейсов перенимают опыт ситуаций и примеряют роль жертвы или злоумышника на себя, тем самым оттачивая навыки кибербезопасности в социальных сетях.

Соответственно подбираются и упражнения (кейсы): сначала — «на правильность», потом — «на правильность и скорость», наконец — «на надежность, при сохранении правильности и скорости» [42].

На основе анализа теоретических работ по данной проблеме мы выделили показатели, а также подобрали методы изучения сформированности навыков информационной безопасности в социальных сетях и представили их

в таблице 1.

Таблица 1 – Показатели и методы исследования

Показатели	Методы изучения
Овладение обучающимся структурой и всеми операциями действия	Решение кейс заданий на правильность
Доведение навыка до требуемой скорости, легкости, качеству выполнения	Решение кейс заданий на правильность и скорость
Оттачивание навыка усложнением условий и трудностей	Решение кейс заданий на надежность, при сохранении правильности и скорости

Таблица 2 –Таблица формирования оценок

Оценка	Методы оценивая
Отлично	Полностью отражена структура кейса, сохранением скорости и правильности
Хорошо	Правильно отражена структура кейса с сохранением скорости
Удовлетворительно	Структура кейса отражена
Неудовлетворительно	Структура кейса не отражена, задача не выполнена

Методы исследования подбирались на основе рекомендаций Юрьев, В. Н. [42], Н.С. Дерендяевой [21], Щепотин, А. Ф. [37], Семененко, В.А. [25], Ярочкин, В.И [43]. Базой исследования определены 2 группы первокурсников: ИС117Д и ИС120Д колледжа ГБПОУ «Южно-Уральский государственный колледж» города Челябинска. Учащиеся в обоих группах обучаются по программе ОП.13 Информационная безопасность по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование. Имеют одну возрастную категорию от 16 до 17 лет. По уровню освоения учебных дисциплин группы примерно одинаковы: около 45% учащихся успевают на «4» и «5», остальные 55% учащихся имеют разное количество хороших и удовлетворительных оценок (от 1 до 8). Не справляющихся с освоением программного материала в обоих группах нет.

Исследование проводилось в 3 этапа:

− констатирующий этап. Цель - выявить уровень сформированности навыков информационной безопасности, обучающихся ИС117Д и ИС120Д

групп, сделать анализ полученных результатов, разделить группы на экспериментальную и контрольную;

− формирующий этап. Цель - разработать электронный учебно-методический комплекс, опрос, лекцию, практические работы, систему кейсов по формированию навыков информационной безопасности в социальных сетях и реализовать его в экспериментальной группе. Контрольная группа занимается по обычному планированию педагога;

− контрольный этап. Цель – выявить достигнутый уровень сформированности навыков информационной безопасности в социальных сетях после реализации цикла занятий в экспериментальной и контрольной группах. Сделать анализ полученных результатов. Разработать рекомендации для студентов по использованию социальных сетей.

Исследование проводилось в обычных условиях в течение учебного времени на занятиях по дисциплине «Информационная безопасность» в течение восьми академических часов. Жесткий регламент времени не устанавливался. Всем испытуемым были предъявлен опрос с вопросами, тексты ситуационных задач (кейсов).

По результатам опроса мы выяснили, что студенты обеих групп зарегистрированы в 3-4 социальных сетях (Вконтакте, Инстаграм, Твитер, Одноклассники). В качестве средства доступа в социальные сети все студенты выбрали телефон – 50 опрошенных, следом идут компьютер и ноутбук – 25 студентов, меньшинство используют планшет – 11 опрошенных студентов. В вопросе для чего используют студенты социальные сети, 50 человек ответили, что используют их для общения, прослушивания аудиозаписей, для учебы или работы и для просмотра новостей.

25 студентов в социальных сетях смотрят видео и фильмы, 18 знакомятся с людьми, и лишь 3 человек играют в игры в социальных сетях. На вопрос про взлом страницы в социальных сетях 40 человек ответили, что их взламывали, 2 ответили – «нет» и 8 отметили, что не знают. Об этикете в социальных сетях не знает 37 человек, остальные ответили, что знают и

придерживаются его. С вредоносной информацией в социальных сетях сталкивались 41 студент и 9 никогда не встречали или не обращали внимания. 48 студентов сталкивались с вредоносным программным обеспечением на телефоне или на компьютере и 2 ответили, что не сталкивались. Все 50 человек сказали, что знакомы с правилами безопасности в интернете. На вопрос о мероприятиях по информационной безопасности 45 человека ответили, что они проводятся часто и 5 ответили, что они проводятся иногда.

Анализ результатов исследования по кейс-заданиям представлены в таблице 3.

Таблица 3 – Результаты ИС117Д группы (констатирующий этап исследования)

Показатели	Оценки			
	Отлично	Хорошо	Удовл	Неудовл
	Проценты	Проценты	Проценты	Проценты
1) Овладение обучающимся структурой и всеми операциями действия	20	40	28	12
2) Доведение навыка до требуемой скорости, легкости, качеству выполнения	12	20	40	28
3) Оттачивание навыка усложнением условий и трудностей	8	16	24	52

При суммировании оценок по всем критериям, мы получили данные о сформированности навыков информационной безопасности в социальных сетях**.** Получены следующие результаты: количество отличных оценок по первому показателю навыков информационной безопасности у 20% студентов; хорошо получили 40% обучающихся, удовлетворительно 28% и

неудовлетворительно выявлено у 12% студентов. У второго и третьего показателя, как мы можем наблюдать в таблице 2, оценки заметно снижаются, поскольку данные показатели требуют более высокого уровня сформированности навыков информационной безопасности в социальных сетях.

Представим графически результаты исследования по кейс заданиям на рисунке 2.21.

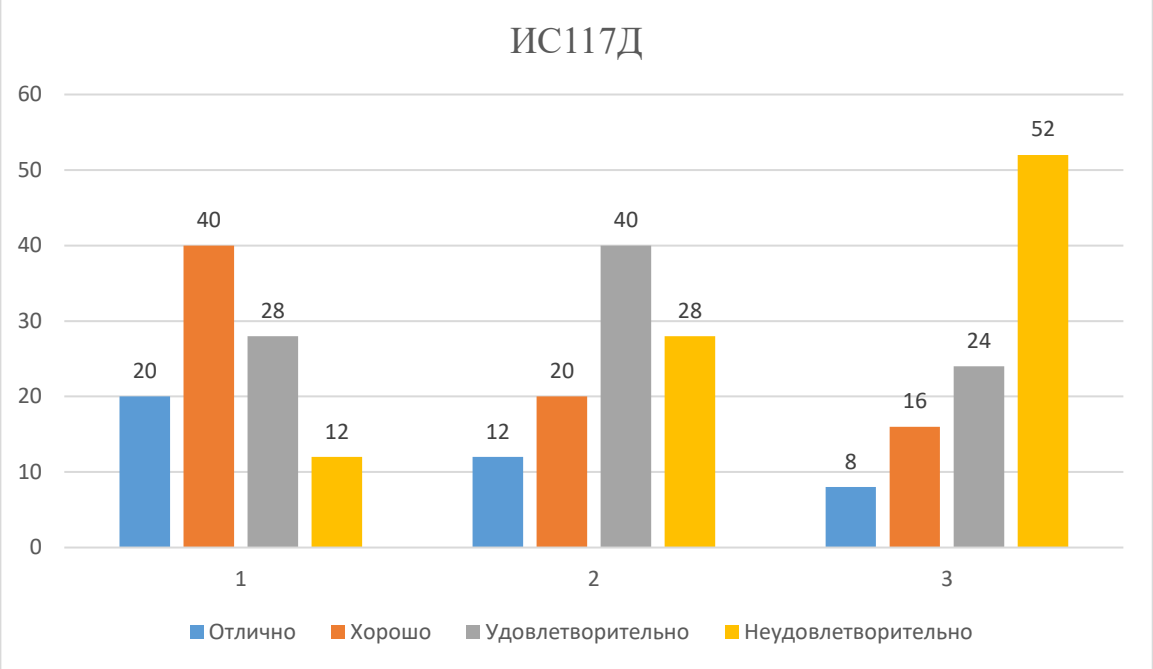


Рисунок 2.29. – Результаты сформированности навыков кибербезопасности в социальных сетях в группе ИС117Д на этапе констатирующего исследования

Графический рисунок дает представление о преимущественно развитых показателях информационной безопасности в социальных сетях. Небольшая часть группы умеет работать в социальных сетях, на констатирующем этапе 14% студентов получили оценки отлично, хорошо – 26%, удовлетворительно – 30% и неудовлетворительно – 30%. Они умеют пользоваться социальными сетями, большинство имеет около 3 активных социальных страниц, но, к сожалению, большая часть студентов не знает об угрозах в социальных сетях.

Выявление сформированности навыков кибербезопасности безопасности в социальных сетях проводилось на основе диагностического задания – решение ситуаций (кейсов). При решении ситуационных задач по

кибербезопасности безопасности оказалось, что большинство учащихся имеют низкий уровень информационной безопасности при работе с социальными сетями и ресурсами Интернета. Часть учащихся просто не задумывалась над этой проблемой и не считает, что это может угрожать безопасности личности, никогда не задумывались, что виртуальные знакомства опасны и могут пойти на встречу без друзей, в одиночку.

Результаты исследования навыков информационной безопасности в группе ИС120Д.

Анализ результатов исследования по кейс заданиям. Все результаты по каждому показателю представлены в таблице 4.

Таблица 4 – Результаты ИС120Д группы (констатирующий этап исследования)

Показатели	Оценки			
	Отлично	Хорошо	Удовл	Неудовл
	Проценты	Проценты	Проценты	Проценты
1) Овладение обучающимся структурой и всеми операциями действия	24	32	28	16
2) Доведение навыка до требуемой скорости, легкости, качеству выполнения	4	28	32	36
3) Оттачивание навыка усложнением условий и трудностей	4	12	28	56

При суммировании баллов по всем критериям, мы получили уровень информационной безопасности в социальных сетях. Получены следующие результаты: количество отличных оценок, по первому показателю навыков информационной безопасности, у 24% студентов; хорошо получили 32% обучающихся, удовлетворительно 28% и неудовлетворительно выявлено у 16% студентов. У второго и третьего показателя, как мы можем наблюдать в

таблице 2, оценки заметно снижаются, поскольку данные показатели требуют более высокого уровня сформированности навыков информационной безопасности в социальных сетях. Полученные данные в ИС120Д группе мы сравнили с результатами, полученными в ИС117Д, и нами выявлено, что полученные результаты практически совпадают.

Представим графически результаты исследования по кейс заданиям на рисунке 2.22.

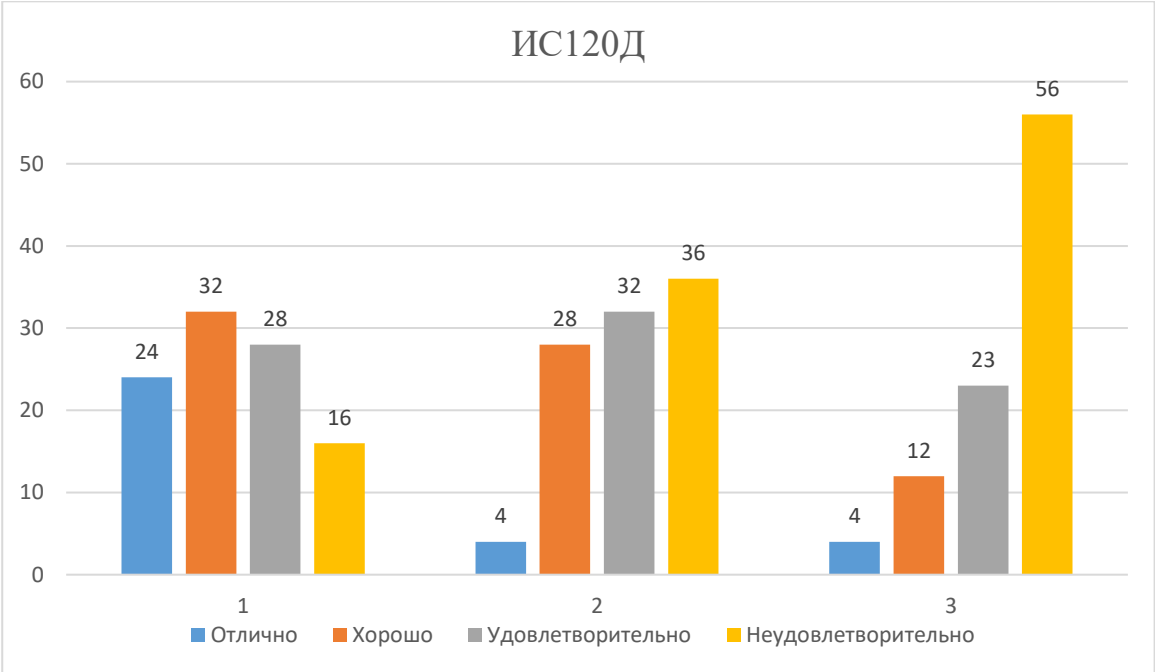


Рисунок 2.30. – Результаты сформированности навыков кибербезопасности в социальных сетях в группе ИС120Д на этапе констатирующего исследования

Графический рисунок дает представление о преимущественно развитых показателях информационной безопасности в социальных сетях в группе ИС120Д. Как и в группе ИС117Д не большая часть группы умеет работать с социальными сетями, на констатирующем этапе данный студенты получили оценки отлично 11% или хорошо 24%, остальные же показали удовлетворительно 29%и неудовлетворительно 36%. Они умеют пользоваться социальными сетями, большинство имеет около 3-4 активных социальных страниц, но, к сожалению, большая часть студентов не знает о угрозах социальных сетей, в этой группе половина студентов тоже не знает о угрозах социальных сетей. Стоит обратить внимание на то,что показатели обеих групп

практически одинаковы, соответственно сформированность навыков у них примерно на одно уровне.

Выявление уровня информационной безопасности проводилось на основе диагностического задания – решение кейс-ситуаций. Студенты в основном знают об угрозах вирусного заражения компьютера, знают, что предпринимается в этом случае, однако проявляют беспечность при знакомстве в социальных сетях. Так большинство учащихся двух групп не опасаются пойти на встречу в одиночку после виртуального знакомства или легко поддаться панике, в случае кибер угрозы и не могут правильно распределить свой прядок действий. Анализ результатов и их сравнение показало, что уровень развития информационной культуры в ИС117Д и ИС120Д находится примерно на одинаковом уровне.

На основании данного вывода для продолжения экспериментального исследования ИС117Д группу определяем, как экспериментальную, а ИС120Д группу– как контрольную.

Итак, в результате проведенного исследования мы выяснили, что сформированность навыков кибербезопасности безопасности в социальных сетях в экспериментальной группе и контрольной группе примерно равен. Большая часть учащихся обеих групп получили на этом этапе четверки, тройки и двойки.

В теоретических исследованиях проводится параллель между формированием навыков информационной безопасности в социальных сетях и компетенций информационной безопасности.

Действительно, можно выделить общее:

– развитие умения критически осмысливать любую информацию, а затем конструктивно ее преобразовывать и анализировать;

– формирование устойчивых нравственных черт личности студента;

– формирование навыков избирательности к внешним влияниям.

– необходимо формировать умение сопоставлять собственные намерения и поступки с существующими в обществе нормами и правилами.

Для достижения цели формирования навыков информационной безопасности в социальных сетях на занятиях информационной безопасности мы выбрали формы работы:

– формирование на занятиях информационной безопасности в процессе изучения программного материала;

– формирование на специально проводимых уроках, посвященных проблеме формирования информационной безопасности.

Определили следующие средства формирования:

– учебные тексты;

– интернет источники;

– формирование через разработанные методические рекомендации

– формирование навыков специально разработанными лекциями и кейсами.

Методы обучения: необходимые традиционные методы, а также моделирование ситуаций и исследовательские методы.

На основе рабочей программы мы проводим более детальное планирование с целью формирования именно навыков информационной безопасности в социальных сетях.

Рассмотрим на примере изучения раздела: «Виды угроз информационной безопасности». В данном разделе изучаются следующие темы:

1. Понятие угрозы.
2. Угрозы нарушения конфиденциальности.
3. Угрозы нарушения целостности.
4. Угрозы нарушения доступности.

Из резервного в этот раздел ввели изучение таких тем:

1. Угрозы интернета и безопасное использование социальных сетей.

2. Практическое занятие. Решение кейсов по кибербезопасности в социальных сетях.

При изучении тем данного раздела на учебном материале мы

формировали такие компоненты информационной безопасности в социальных сетях:

– когнитивный. Учащиеся получают большой объем новой информации по обеспечению личной безопасности в социальных сетях. Причем у них уже есть практика наблюдения, участия в ситуациях, связанных с реальными опасностями в социальных сетях. В процессе изучения учебного материала они анализируют ее, проводят сравнения событий и потенциальных угроз, выделяют главное и существенное. В результате у них происходит синтез новых знаний с уже имеющимися знаниями. При рассмотрении знакомых опасных ситуаций всех названных тем выделяется обязательно причины возникновения опасных ситуаций в сети. В дальнейшем это дает возможность прогнозировать события на основе имеющейся информации, предвидеть наступлений определенных последствий.

– деятельностный компонент реализуем в процессе занятия при рассмотрении конкретных ситуаций, обращаемся к учащимся с вопросами: Как надо поступить? Что необходимо предпринять? Твои действия в данной ситуации?

– коммуникативный компонент обеспечиваем за счет использования групповой формы работы, проектной, частично – поисковой, практической.

Оценка и анализ эффективности внедрения методов по формированию навыков информационной безопасности в социальных сетях у студентов ИС117Д и ИС120Д на занятиях по информационной безопасности.

Для установления сформированности навыков кибербезопасности в социальных сетях после реализации цикла занятий, мы провели контрольное исследование в экспериментальной и контрольной группе. Контрольная группа занималась по обычной программе.

Для исследования использовали те же методы, что и на этапе констатирующего исследования. В экспериментальном классе были получены следующие результаты, представленные в таблице 5.

Таблица 5 – Результаты контрольного исследования экспериментальной ИС117Д группы

Показатели	Оценки			
	Отлично	Хорошо	Удовл	Неудовл
	Проценты	Проценты	Проценты	Проценты
1) Овладение обучающимся структурой и всеми операциями действия	64	28	8	0
2) Доведение навыка до требуемой скорости, легкости, качеству выполнения	56	36	8	0
3) Оттачивание навыка усложнением условий и трудностей	44	32	16	8

При суммировании баллов по всем критериям, мы получили данные о сформированности навыков информационной безопасности в социальных сетях.

Получены следующие результаты: отличных оценок по трем показателям в сумме получилось 55%, оценок хорошо 32%, остальные же показали удовлетворительно 10% и неудовлетворительно 3%. При сравнении с предыдущим результатом, сформированность навыков значительно выросла.

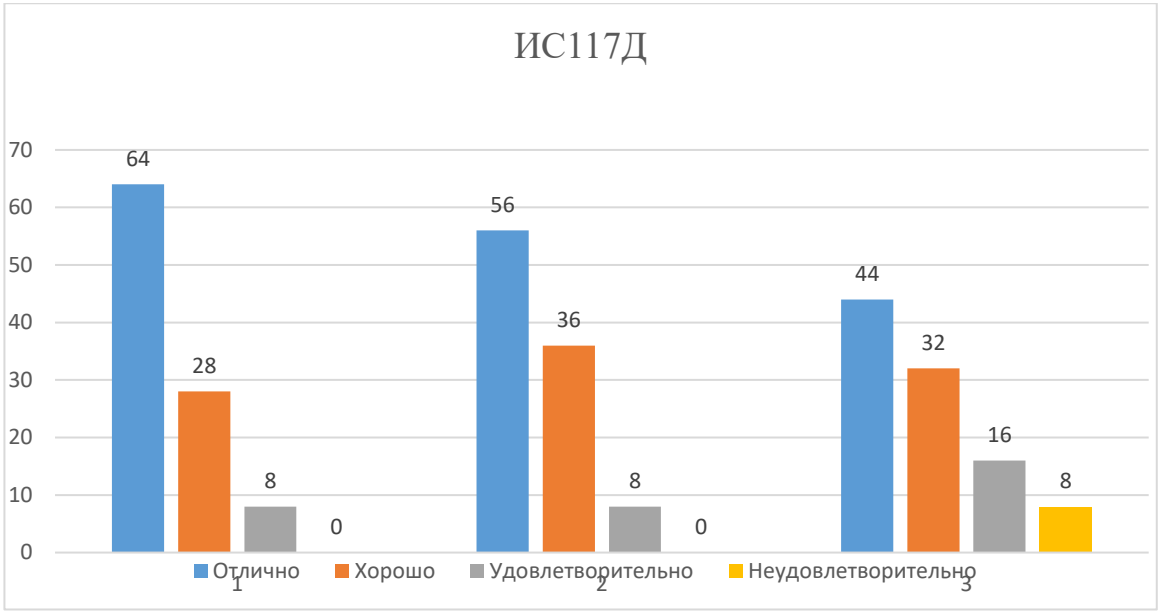


Рисунок 2.31. – Результаты сформированности навыков кибербезопасности в социальных сетях в экспериментальной группе на контрольно-оценочном этапе

Анализ результатов, представленный графически, показал, что большинство студентов имеют более высокие показатели сформированности навыков по информационной безопасности в социальных сетях. Все студенты группы умеют работать с социальными сетями, и лишь 8% студентов получили оценку 2 по третьему показателю навыков информации. Они умеют пользоваться социальными сетями и теперь владеют навыками информационной безопасности в социальных сетях.

Во время формирующего этапа студенты контрольный группы занимались по обычной программе дисциплины «Информационная безопасность», в отличии от экспериментальный группы, где использовался разработанный нами электронный учебно-методический комплекс. После завершения формирующего этапа эксперимента, в контрольной группе было проведен анализ достигнутого уровня сформированности навыков по информационной безопасности в социальных сетях по тем же методикам, что и в экспериментальной группе. Все результаты по каждому критерию представлены в таблице 6.

Таблица 6 – Результаты контрольного исследования контрольной группы ИС120Д

Показатели	Оценки			
	Отлично	Хорошо	Удовл	Неудовл
	Проценты	Проценты	Проценты	Проценты
1) Овладение обучающимся структурой и всеми операциями действия	52	28	12	8
2) Доведение навыка до требуемой скорости, легкости, качеству выполнения	40	20	28	12
3) Оттачивание навыка усложнением условий и трудностей	32	12	36	20

При суммировании баллов по всем критериям, мы получили уровень сформированных навыков информационной безопасности в социальных сетях. Получены следующие результаты: отличных оценок по трем показателям получилось 41%, оценок хорошо 20%, остальные же показали удовлетворительно 26% и неудовлетворительно 13%. Полученные данные в контрольной группе мы сравнили с результатами, полученными в экспериментальной группе, и нами выявлено, что полученные результаты по всем показателям отличаются.

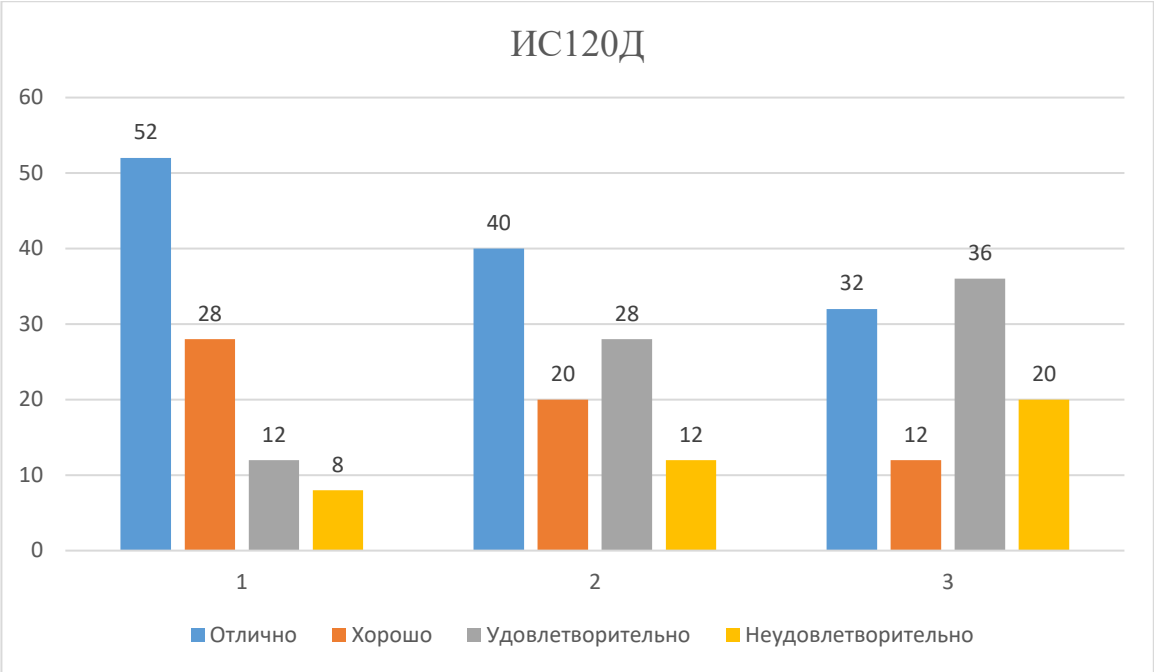


Рисунок 2.32. – Результаты сформированности навыков кибербезопасности в социальных сетях в контрольной группе на контрольно-оценочном этапе

Более высокие результаты сформированности навыков кибербезопасности в социальных сетях по всем указанным показателям показала экспериментальная группа – 55% пятерок, в контрольной группе 41% пятерок 41%. В экспериментальной группе 32% четверок, контрольная группа получила 20% четверок. Больше всего оценок удовлетворительно 26% и неудовлетворительно 13% получили в контрольной группе. У экспериментальной группы оценку удовлетворительно получили 11% студентов и неудовлетворительно 2%. Более низкими результаты оказались в контрольной группе.

Представим графически результаты сравнения на рисунке 2.24

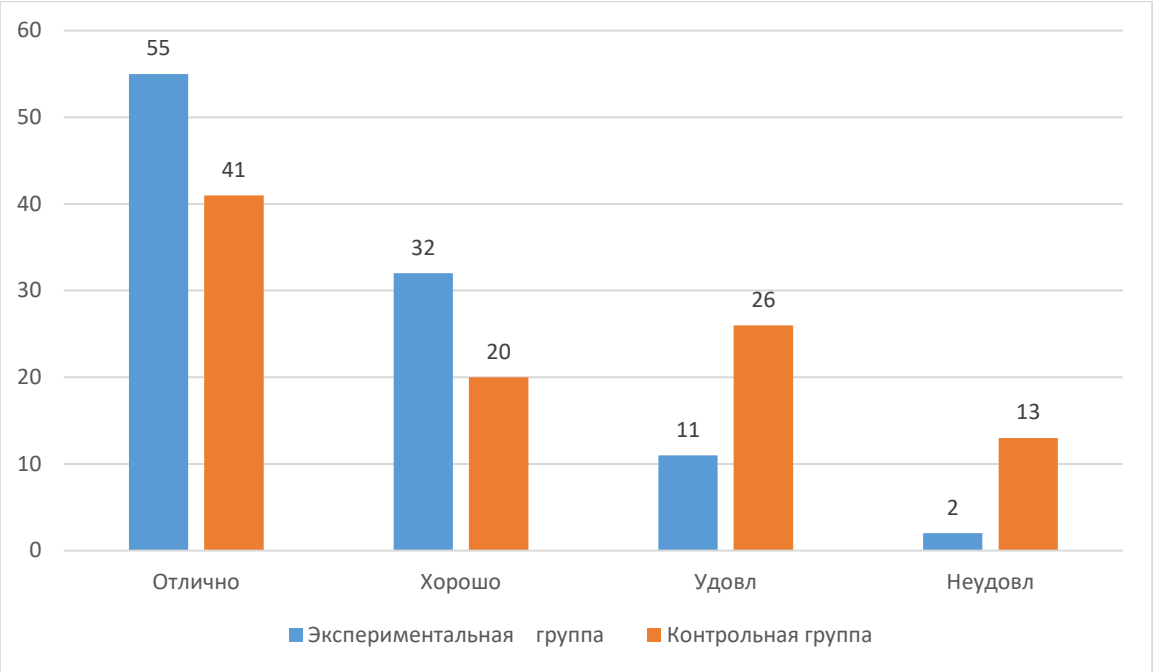


Рисунок 2.33. – Результаты сформированности навыков кибербезопасности в социальных сетях в экспериментальной и контрольной группе на контрольно-оценочном этапе

Графический рисунок дает представление о преимущественно более сформированных навыках кибербезопасности в социальных сетях в экспериментальной группе по сравнению с контрольной группой. Они имеют практически одинаковые значения, но все же экспериментальная группа превосходит контрольную.

Итак, в результате проведенного исследования мы выяснили, что сформированность навыков кибербезопасности в социальных сетях в экспериментальной группе, по сравнению с контрольной группой, является более высокой.

Выводы по второй главе

На основе теоретических положений, изложенных в первой главе, во второй главе представлены результаты проведенной экспериментальной работы по формированию навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации.

Результаты констатирующего этапа эксперимента свидетельствуют о том, что навыки кибербезопасности в социальных сетях сформированы недостаточно, в связи с чем необходимо использование дополнительных педагогических средств, а именно электронного учебно-методического комплекса.

Использованные показатели и методы исследования позволили нам определить уровень сформированности навыков кибербезопасности в социальных сетях.

Результаты формирующего этапа эксперимента показали, что формирование навыков кибербезопасности в социальных сетях происходит эффективнее в экспериментальной группе, где был реализован электронный учебно-методический комплекс, который включает наряду с лекционным, практическим материалом, систему кейс-заданий. Студенты осведомлены о том, как нужно себя обезопасить в социальных сетях и что нужно предпринять в случае информационной угрозы. У студентов контрольной группы в процессе обучения в колледже навыки кибербезопасности в социальных сетях формируются, но медленнее, чем в ЭГ.

ЗАКЛЮЧЕНИЕ

Подводя итоги данной работы, важно отметить, что формирование навыков кибербезопасности будет более эффективным, если внедрить данный электронный учебно-методический комплекс в программу среднего профессионального образования.

Проблема информационной безопасности и кибербезопасности в социальных сетях действительно существует, нарушая состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, отсюда появляется необходимость активной разработки проблематики кибербезопасности.

Для эффективного и полноценного развития обучающегося не нужно создавать соответствующую информационную среду, необходимо научить жить в информационной среде, видеть опасности, исходящие от информации, уметь предвидеть и реагировать на информационную угрозу.

Рассмотрев теоретические аспекты формирования навыков кибербезопасности в социальных сетях у студентов профессиональной образовательной организации, нами были решены следующие задачи:

1. Проанализировать угрозы и способы защиты персональной информации в социальных сетях.

Мы выяснили, что кибербезопасность – это часть такого понятия как информационная безопасность и они неразрывно связаны друг с другом. Изучили современные угрозы и способы противодействия им. Двадцать первый век стал самым прогрессируем по утечки данных из социальных сетей и сети интернет в целом. Конечно этому поспособствовало быстрое развитие технологий и общедоступность гаджетов. Государство разрабатывает законы для защиты детей в социальных сетях и сети интернет, один из рассмотренных нами законов - Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ раскрывает термин «информационная безопасность детей» как «состояние

защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью или физическому, психическому, духовному, нравственному развитию». Поскольку студенты первых кусов среднего профессионального образования по закону еще остаются детьми, поэтому их психическое и физическое здоровье в социальных сетях охраняется государственными законами. Рассмотрели такие понятия как кибертерроризм, киберэкстремизм и киберпреступления, как взаимосвязаны данные понятия и в чем их кардинальное отличие друг от друга.

2. Исследовать сущность навыков кибербезопасности в социальных сетях.

Под навыками кибербезопасности в социальных сетях у студентов профессиональной образовательной организации понимают способности обучающихся выявлять, идентифицировать и противостоять угрозам информационного воздействия в киберпространстве.

Сущность навыков кибербезопасности в социальных сетях и процесс их формирования у студентов профессиональной образовательной организации определяется триадой «знания-умения-навыки» в современной дидактике, согласно которой овладение умениями и навыками происходит на базе усвоения знаний.

Знания составляют ядро содержания обучения. На основе знаний у учащихся формируются умения и навыки, умственные и практические действия. До сих пор не уточнены соотношения между понятиями "умения" и "навыки". Большинство психологов и педагогов считают, что умение — более высокая психологическая категория, чем навыки. Мы пришли к выводу, что термин "умение" имеет два значения:

Как первоначальный уровень овладения каким-либо простым действием. В этом случае навык рассматривается как высший уровень овладения этим действием, автоматизированное его выполнение: умение переходит в навык.

Как способность осознанно выполнять сложное действие с помощью ряда навыков. В этом случае навык — это автоматизированное выполнение элементарных действий, из которых состоит сложное действие, выполняемое с помощью умения.

3. Разработать электронный учебно-методический комплекс как средство формирования готовности к кибербезопасности в социальных сетях.

Нами был разработан электронный учебно-методический комплекс для формирования навыков в социальных сетях в системе MoodleCloud, который включает в себя систему кейсов, позволяющую формировать навыки кибербезопасности в социальных сетях, лекционный материал для теоретического обучения, словарь терминов и определений, тестовые задания с кейсами на контроль формирования навыков кибербезопасности, опрос для определения теоретических знаний кибербезопасности в социальных сетях на этапе контрольного исследования.

4. Разработать методические рекомендации по кибербезопасности в социальных сетях для обучающихся.

Нами были разработаны методические рекомендации для студентов среднего профессионального образования. Методические рекомендации включают в себя дополнительный теоретический и практический материал, который поможет студентам выявлять, идентифицировать и противостоять угрозам информационного воздействия в киберпространстве.

В методических рекомендациях прописано все начиная с регистрации в социальных сетях и правильностью общения, заканчивая возможными угрозами и методами их ликвидации.

5. Провести проверку сформированности навыков и проанализировать полученные результаты.

Проверка сфомированности навыков и анализ результатов разработки проводились в двух группах первого курса в учебном учреждении среднего профессионального образования ГБПОУ «Южно-Уральский государственный колледж». Обе группы по результатам проверки констатирующего этапа

исследования имели примерно одинаковые показатели сформированности навыков кибербезопасности в социальной сети. В дальнейшем группы разделили на экспериментальную, в которой помимо основной учебной программы коллежа, по дисциплине «Информационная безопасность», проводились занятия по разработанному электронному учебно-методическому пособию и контрольную группу, которая обучалась только по учебной программе. После изучения учебного материала обеими группами, провели контрольный тест с практическими кейс-заданиями, для выявления уровня знаний, умений и навыков. По результатам исследования выяснилось, что более высокий уровень показала экспериментальная группа, контрольная группа тоже улучшила свои результаты и лишь немного отставала от экспериментальной. Тем самым результат эффективности электронного учебно-методического пособия оказался выше стандартной программы по дисциплине информационная безопасность.

Таким образом, цель работы достигнута, поставленные задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аверченков, В. И. Аудит информационной безопасности органов исполнительной власти. Учебное пособие / В.И. Аверченков. - М.: Флинта**,** 2020**. -** 355 с.

2. Алпеев, А. С. Терминология безопасности: кибербезопасность, информационная безопасность [Текст] / А. С. Алпеев. – Москва, 2018. – № 5. – С. 39–42.

3. Анурьева М.С. Влияние интернета на социализацию молодежи — Санкт-Петербург: Питер. – 2019. – 164 с.

4. Беспалько, В. П. Слагаемые педагогической технологии / В. П. Беспалько. – М.: Педагогика, 2017. – 190 с.

5. Беспалько, В. П. Основы теории педагогических систем / В. П. Беспалько. – Воронеж: Издательство ВГУ, 2017. – 34 с.

6. Беспалько, В. П. Системно-методическое обеспечение учебно-воспитательного процесса подготовки специалистов / В. П. Беспалько,Ю. Г. Татур. – М.: Высшая школа, 2018. – 144 с.

7. Галагузова, М. А. Профессиональная подготовка социальных работников / М. А. Галагузова. – М.: Союз, 2020. – 220 с.

8. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.

9. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

10. Ищенко, А. Н., Прокопенко, А. Н., Страхов, А. А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России информационной сфере / А. Н. Ищенко, А. Н.Прокопенко, А. А. Страхов // Проблемы правоохранительной деятельности, Москва, 2017. – № 2. – С. 55–62.

11. Колмогоров, Л. С. Опыт создания электронных УМК по психологии для студентов / Л. С. Колмогоров // Организационно-управленческие инновации в системе педагогического образования. – Барнаул, 2019. – С. 36-38.

12. Концепция стратегии кибербезопасности Российской Федерации. Проект [Электронный ресурс] // Проект [сайт] [2020]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf.

13.Кричевский, В. Б. Комплексная методика профессиональной подготовки преподавателя музыки: автореф. дисс. … канд. пед. наук: В. Б. Кричевский. – М., 2020. – 22 с.

14. Магдилов, М. М., Магдилова, Л. В. Особенности формирования образовательного курса по интернетбезопасности несовершеннолетних [Текст] / EUROPEAN RESEARCH. Сборник статей XVIII Международной научно-практической конференции; Под общ.ред. к.э.н. Г.Ю. Гуляева. – Москва: Наука и просвещение. – 2019. – 199 с

15. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. N 646 / Собрание законодательства РФ, 12.12.2016, N 50, ст. 7074.

16. Обухова, Л. Ф. Возрастная психология: учебник для бакалавров / Л. Ф. Обухова. – Москва: Юрайт. – 2018. – 460 с.

17.Пальчевский, Б. В. Учебно-методический комплекс средств обучения / Б. В. Пальчевский, Л. С. Фридман // Советская педагогика. –2021. – № 6. – С. 26-32.

18. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2021. - 432 с.

19. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2020. - 368 с.

20. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: ИНФРА-М, 2021. - 368 с.

21. Петров, Сергей Викторович; Кисляков Павел Александрович Информационная Безопасность / Александрович Петров Сергей Викторович; Кисляков Павел. - Москва: Машиностроение**,** 2018. - 329 с.

22. Пидкасистый, П. И. Педагогика: учебник для студентов высших учебных заведений, обучающихся [Текст] / П. И. Пидкасистый, В. А. Мижериков, Т. А. Юзефавичус; под ред. П.И. Пидкасистого. - 2-е изд., перераб. и доп. – Москва: Академия. – 2020. – 619 с.

23. Родичев, Ю. А. Информационная безопасность: нормативноправовые аспекты: учебное пособие [Текст] / под ред. Ю.А. Родичев. — Санкт-Петербург: Питер. – 2018. – 272 с.

24. Российская педагогическая энциклопедия: В 2 т. / Гл. ред. В. Г. Панов. - М.: Большая Рос. энцикл., 1993-1999. - 27 см.

25. Сальная, Л.К. Английский язык для специалистов в области информационной безопасности / Л.К. Сальная. - М.: Гелиос АРВ, 2019. - 733 с.

26. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2021. — 277 с.

27. Синицын, Д. С. Психолого-педагогические условия обучения информационно-психологической безопасности подростков. Дис. канд. пед. наук [Текст] / Д. С. Синицын: 13.00.01 / Рос.гос. пед. ун-т им. А. И. Герцена. – Санкт-Петербург. – 2021. – 19 с.

28. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2020. - 304 с.

29. Стрельцов, А. А. Обеспечение информационной безопасности России [Текст] / А.А. Стрельцов // Теоретические и методологические основы под ред. В. А. Садовничего и В. П. Шерстюка. – Москва: МЦНМО. – 2020. – 86 с.

30. Татур. Библер, В. С. Нравственность. Культура. Современность: философские размышления о жизненных проблемах / В. С. Библер. – М.: Знание, 2019. – 62 с.

31. Толстых, Т. О. Проектирование учебно-методическихкомплексов с использованием новых образовательных технологий/ Т. О. Толстых // Проблемы практической подготовки студентов: материалы 2 Всероссийской научно-методической конференции. – Воронеж, 2018. – С. 239-248.

32. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Текст] / Собрание законодательства РФ. – 2020. – № 1. – Ст. 48.

33. Федоров, А. В. Информационная безопасность в мировом политическом процессе / А.В. Федоров. - М.: МГИМО-Университет, 2021. - 220 с.

34. Фридман, Л. М. Изучение личности учащегося и ученических коллективов: книга для учителя/ Л. М. Фридман, Т. А. Пушкина, И. Я. Каплунович. – М.: Просвещение, 2019. – 207 с.: ил.

35. Фридман, Л. М. Психологическая наука учителю/ Л. М. Фридман, К. Н. Волков. – М.: Просвещение, 2018. – 205 с.

36. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2019. - 336 с.

37. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2020. — 702 с.

38. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. — 416 с.

39. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. Гриф МО РФ / В.Ф. Шаньгин. - М.: Форум, 2022**.** - 172 с.

40. Шаньгин, Владимир Федорович Информационная безопасность и защита информации / Шаньгин Владимир Федорович. - М.: ДМК Пресс, 2022**.** - 648 с.

41.Щепотин, А. Ф. Комплексное учебно-методическое обеспечение образовательного процесса в средних профессиональных учебных заведениях: методическое пособие / А. Ф. Щепотин,М. А. Чекулаев. –

М.: НМЦ СПО, 2019. – 50 с.

42. Юрьев, В. Н. Игровой подход к оценке риска и формированию бюджета информационной безопасности предприятия / В.Н. Юрьев. - М.: Синергия, 2018**.** - 504 с.

43. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.