МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

Государственное бюджетное профессиональное образовательное учреждение Краснодарского края «Краснодарский политехнический техникум»

РАБОЧАЯ ПРОГРАММА

ЭК. 03 Правовая, социальная, информационная безопасность

для специальности:
43.02.13 «Технология парикмахерского искусства»

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа элективного курса ЭК 03. «Правовая, социальная, информационная безопасность» предназначена для изучения в профессиональных образовательных организациях СПО, реализующих образовательную программу среднего общего образования в пределах освоения основной профессиональной образовательной программы СПО (ОПОП СПО) на базе основного общего образования при подготовке квалифицированных рабочих. Содержание, последовательность изучения тем, объём рабочей программы полностью является авторской программой.

В программу включено содержание, направленное на формирование у студентов компетенций, необходимых для качественного освоения основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования; программы подготовки специалистов среднего звена (ППССЗ):

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОБЩАЯ ХАРАКТЕРИСТИКА ЭЛЕКТИВНОГО КУРСА ЭК 03. «Правовая, социальная, информационная безопасность»

Курс ориентирован на проведение занятий по информационной безопасности обучающихся и безопасному поведению в сети Интернет. Отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ компаний и операторов мобильной связи Российской Федерации. Важную часть курса составляет изучение правовой информации об основных законодательных актах в сфере информационной безопасности, а также материалов, размещенных на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, на основании которых рекомендуется практическая работа, например составление информационной листовки, буклета по темам: персональные данные http://rkn.gov.ru/personal-data/ protection-

of-the-innocent/; контроль и надзор в сфере информационных технологий http://rkn.gov.ru/it/control/; контроль и надзор в сфере связи http://rkn.gov.ru/communication/control/; контроль и надзор в сфере массовых коммуникаций http://rkn.gov.ru/mass-communications/

Главная цель курса - обеспечить социальные аспекты информационной безопасности в воспитании подростков в условиях цифрового мира, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формирование у обучающихся правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания.

Задачи курса:

– формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;

– создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

– формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

– мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально правовых регуляторов жизни общества и государства в условиях цифрового мира;

– научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Планируемые результаты освоения курса:

В соответствии с ФГОС общего образования необходимо сформировать у обучающихся такие *личностные результаты*, которые позволят подростку ориентироваться в информационном мире с учетом имеющихся в нем угроз:

- Принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества.
- Быть социально активным, уважающим закон и правопорядок, соизмеряющим свои поступки с нравственными ценностями, осознающим свои обязанности перед семьей, обществом, Отечеством.

- Уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов.
- Осознанно выполнять правила здорового и экологически целесообразного образа жизни, безопасного для человека и окружающей его среды.

В результате обучения по модулям курса акцентируется внимание на такие *метапредметные* результаты освоения основной образовательной программы основного общего образования, как:

- освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества;
- участие в самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;
- формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, подростками старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебноисследовательской, творческой и других видов деятельности;
- умение использовать средства информационных и коммуникационных технологий (далее - ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Также планируется достижение некоторых предметных результатов, актуальных для данного курса в интеграции с предметами: «Информатика» (раздел «Социальная информатика»), «Безопасность жизнедеятельности», «Обществознание» (разделы «Социальные отношения», «Право»), «Право» (разделы «Административное право», «Уголовное право», «Гражданское право») для СПО, например:

- формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;
- освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;
- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

Планируется достижение некоторых предметных результатов, актуальных для данного курса в предметах.

В результате освоения курса учащиеся будут

знать и понимать:

– источники угроз, поступающих на мобильный телефон, планшет, компьютер

– виды угроз
– проблемные ситуации в сетевом взаимодействии
– правила поведения для защиты от угроз
– правила поведения в проблемных ситуациях
– этикет сетевого взаимодействия
– роль близких людей, семьи для устранения проблем и угроз в сети Интернет и мобильной телефонной связи
– телефоны экстренных служб
– личные данные
– позитивный Интернет;

уметь:

– правильно использовать аватар с учетом защиты личных данных
– регистрироваться на сайтах без распространения личных данных
– вести общение в социальной сети или в мессенджере сообщений
– правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.)
– отключиться от нежелательных контактов
– использовать позитивный Интернет.

СОДЕРЖАНИЕ ПРОГРАММЫ КУРСА

1. Правовые основы информационной безопасности

Понятия юридической ответственности за правонарушения в области информационной безопасности.

2. Законодательство Российской Федерации о гражданско - правовой ответственности в сфере инфобезопасности.

Законодательство Российской Федерации о гражданско правовой ответственности. Гражданско правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации).

3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности.

Понятие административной ответственности. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).

4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности.

Понятие уголовной ответственности. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации).

5. Безопасность общения и безопасность информации.

Соблюдения норм инфобезопасности в личном информационном пространстве.

ТЕМАТИЧЕСКИЙ ПЛАН КУРСА

Курс рассчитан на 39 часов обучения, ориентирован на работу обучающихся с документами в области законодательства Российской Федерации в сфере информационной безопасности.

В конце каждого раздела предусмотрено контрольное занятие. Аттестация учащихся проводится по системе **зачет/незачет.**

Программа элективного курса рассчитана на 39 учебных часов, из них 19 часов – теоретического обучения, 20 часов – практические занятия.

№ темы	Наименование разделов и тем	Количество часов аудиторной нагрузки			Самостоятельная работа
		Всего	Теоретического обучения	В том числе, практические занятия	
1	**Раздел 1. Правовые основы информационной безопасности**	**4**	**2**	**2**	**-**
1.1	Понятия юридической ответственности за правонарушения в области информационной безопасности	4	2	2	-
2	**Раздел 2. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности**	**4**	**2**	**2**	-
2.1	Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	4	2	2	-
3	**Раздел 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности**	**4**	**2**	**2**	-
3.1	Административная ответственность за проступки в области информационной безопасности (защиты информации)	4	2	2	-
4	**Раздел 4. Законодательство Российской Федерации об**	**5**	**3**	**2**	**-**

	уголовной ответственности в сфере инфобезопасности				
4.1	Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)	5	3	2	-
5	**Раздел 5. Безопасность общения и безопасность информации**	**22**	**10**	**12**	-
5.1	Мир виртуальный и реальный. Интернет зависимость.	2	2	-	-
5.2	Кибербуллинг	2	-	2	-
5.3	Правила сетевого этикета	2	-	2	-
5.4	Мошеннические действия в Интернете. Киберпреступления	2	-	2	-
5.5	Фишинг	2	2	-	-
5.6	Потребительские опасности в Интернете	2	-	2	-
5.7	Безопасность при использовании платежных карт в Интернете	2	-	2	-
5.8	Россия на пути к информационному обществу	2	2	-	-
5.9	Ложная информация в Интернете	2	2	-	-
5.10	Государственная политика в области защиты информации.	2	-	2	-
	Дифференцированный зачет	2	2	-	-
	Итого	**39**	**19**	**20**	-

ХАРАКТЕРИСТИКА ОСНОВНЫХ ВИДОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

№ п/п	Содержание обучения	Основное содержание	Характеристика основных видов деятельности студентов (на уровне учебных действий)
1	**Раздел 1. Правовые основы информационной безопасности**		
1.1	Понятия юридической ответственности за правонарушения в области информационной безопасности	1.Понятия юридической ответственности за правонарушения в области информационной безопасности. 2.Основные документы в области ин формационной безопасности Российской Федерации 3. Информация как объект правовых отношений 4. Функции, принципы и виды юридической ответственности. 5.Субъективная и объективная стороны юридической ответственности	Подготовка презентации по теме в группах учащихся.
2	**Раздел 2. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности**		
2.1	Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	1.Общие положения законодательства Российской Федерации о гражданско правовой ответственности. 2.Порядок привлечения несовершеннолетних к гражданско правовой ответственности за проступки в облати информационной безопасности (защиты информации) 3.Ответственность за проступок в области присвоение авторства (плагиат) 4. Ответственность за проступок за оскорбления, в том числе в социальных сетях	Решать ситуации предполагающие гражданско-правовую ответственность за преступления в сфере информационной безопасности.
3	**Раздел 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности**		
3.1	Административная ответственность за проступки в области информационной безопасности (защиты информации)	1.Административное правонарушение. 2.Основные понятия административного правонарушения. 3.Особенности административной ответственности несовершеннолетних. 4.Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение	Решать ситуации предполагающие административную ответственность за преступления в сфере информационной безопасности.

		5. Ответственность за проступок — за оскорбления, в том числе в социальных сетях 6. Ответственность за проступок — ложный вызов экстренных служб 7. Ответственность за проступок — пропаганду в Интернете наркотических и психотропных веществ 8. Ответственность за проступок — нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные) 9. Ответственность за проступок — нарушение правил защиты информации 10. Ответственность за проступок — представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство 11. Ответственность за проступок — за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт 12. Ответственность за проступок — нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации	

4	**Раздел 4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности**		
4.1	Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)	Основные направления государственной политики в области формирования культуры информационной безопасности.	Решать ситуации предполагающие уголовную ответственность за преступления в сфере информационной безопасности.
5	**Раздел 5. Безопасность общения и безопасность информации**		
5.1	Мир виртуальный и реальный. Интернет зависимость.	Правильное использование компьютера и сотовых телефонов, чтобы не быть затянутым в виртуальный мир.	Активизировать размышления о негативных и позитивных сторонах виртуальной жизни.
5.2	Кибербуллинг	Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
5.3	Правила сетевого этикета	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальныхсетях. Профиль пользователя. Анонимные социальные сети. Общение.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
5.4	Мошеннические действия в Интернете. Киберпреступления	Определение Интернет-ресурсов, несущих потенциальную угрозу финансовому благополучию пользователей	Решение ситуаций (памятка МВД - https://xn--b1aew.xn--p1ai/document/1910260)
5.5	Фишинг	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.
5.6	Потребительские опасности в Интернете	Безопасность потребителей в сети Интернет	Умеет определить источник риска, разрабатывает возможные варианты решения ситуаций, связанных с рисками.
5.7	Безопасность при использовании платежных карт в Интернете	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.

5.8	Россия на пути к информационному обществу	Процесс перехода к информационному обществу, а так же информационный кризис и пути его решения.	Дает понятие информационного общества, информационный кризис и предлагает пути его решения.
5.9	Ложная информация в Интернете	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
5.10	Государственная политика в области защиты информации	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.

УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ КУРСА

ЭК. 03 Правовая, социальная, информационная безопасность

Освоение программы элективного курса ЭК.03 «Правовая, социальная, информационная безопасность» предполагает наличие в профессиональной образовательной организации, реализующей образовательную программу среднего общего образования в пределах освоения ОПОП СПО на базе основного общего образования, учебного кабинета, в котором имеется возможность обеспечить свободный доступ в Интернет во время учебного занятия и период внеучебной деятельности обучающихся.

Помещение кабинета должно удовлетворять требованиям Санитарно-эпидемиологических правил и нормативов (СанПиН 2.4.2 № 178-02) и быть оснащено типовым оборудованием, указанным в настоящих требованиях, в том числе специализированной учебной мебелью и средствами обучения, достаточными для выполнения требований к уровню подготовки обучающихся.

В кабинете должно быть мультимедийное оборудование, посредством которого участники образовательного процесса могут просматривать визуальную информацию по праву, создавать презентации, видеоматериалы, иные документы.

В состав учебно-методического и материально-технического обеспечения про-

граммы ЭК.03 «Правовая, социальная, информационная безопасность» входят:

- многофункциональный комплекс преподавателя;
- наглядные пособия (памятки, Федеральные законы в сфере информационной безопасности и др.);
- информационно-коммуникационные средства;
- экранно-звуковые пособия;
- комплект технической документации, в том числе паспорта на средства обучения, инструкции по их использованию и технике безопасности;

Библиотечный фонд дополнен энциклопедиями, справочниками, научной и научно-популярной литературой по информатике, социологии, праву и т. п. в электронном формате.

В процессе освоения ЭК. 03 «Правовая, социальная, информационная безопасность» студенты должны иметь возможность доступа к электронным учебным материалам по обществознанию, информатике, БЖД, праву, имеющимся в свободном доступе в сети Интернет (электронным книгам, практикумам, тестам и др.), сайтам государственных, муниципальных органов власти.

№ темы	Наименование разделов и тем	Количество часов аудиторной нагрузки			Материалы ЭК
		Всего	Теоретического обучения	В том числе, практические занятия ПЗ	
1	**Раздел 1. Правовые основы информационной безопасности**	**4**	**2**	**2**	1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» http://www.consultant.ru/document/cons_doc_LAW_61798/ 2. Указ Президента Российской Федерации №203/2017 г. «О стратегии развития информационного общества в Российской Федерации до 2030 года» 3. Указ №646/2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» 4. Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р «Концепция информационной безопасности детей» 5. ДОКУМЕНТЫ, РЕГУЛИРУЮЩИЕ РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В
1.1	Понятия юридической ответственности за правонарушения в области информационной безопасности	4	2	2	

					РОССИИ 6. Конституция Российской Федерации http://www.constitution.ru/ 7. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (ред. от 01.05.2019) https://fzrf.su/zakon/o-zashchite-detej-ot-informacii-436-fz/ 8. https://resh.edu.ru/subject/lesson/3350/main/ - видео 9. https://resh.edu.ru/subject/lesson/7323/conspect/250819/ - конспект 10. https://resh.edu.ru/subject/lesson/7323/main/250824/ - видео
2	**Раздел 2. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности**	**4**	**2**	**2**	1. Федеральный закон от 30 ноября 1994 года № 51-ФЗ «Гражданский кодекс Российской Федерации (ГК РФ). http://www.consultant.ru/document/cons_doc_LAW_5142/ 2. https://resh.edu.ru/page/cyber-project - КИБЕР БЕЗОПАСНОСТЬ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ (ВИДЕОПОДБОРКА) 3. https://resh.edu.ru/subject/lesson/7323/train/250832/ - Задание
2.1	Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	4	2	2	
3	**Раздел 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности**	**4**	**2**	**2**	1. Федеральный закон от 30 декабря 2001 года № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (КоАП РФ) 2. http://www.consultant.ru/document/cons_doc_LAW_34661/ - Изменения КоАП 2021 года 3. https://resh.edu.ru/page/cyber-project - КИБЕР БЕЗОПАСНОСТЬ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ (ВИДЕОПОДБОРКА)
3.1	Административная ответственность за проступки в области информационной безопасности (защиты информации)	4	2	2	
4	**Раздел 4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности**	**5**	**3**	**2**	1. Федеральный закон от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс Российской Федерации» (УГ РФ) http://www.consultant.ru/document/cons_doc_LAW_10699/ 2. Федеральный закон от 18 декабря 2001 года № 174-ФЗ «Уголовно-процессуальный кодекс Российской Федерации» (УПГ РФ). http://www.consultant.ru/document/cons_doc_LAW_34481/
4.1	Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)	5	3	2	

5	**Раздел 5. Безопасность общения и безопасность информации**	**22**	**10**	**12**	1. Онлайн-интервью с заслуженным юристом Российской Федерации, доктором юридических наук, профессором В.В. Черниковым | КонсультантПлюс - студенту и преподавателю http://www.consultant.ru/edu/news/interview/v_pomosh_studentu/studencheskiye_voprosy/chernikov/ 2. Видеоролик https://yandex.ru/video/preview/16188790155859638934 3. https://resh.edu.ru/page/cyber-project - КИБЕР БЕЗОПАСНОСТЬ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ (ВИДЕОПОДБОРКА)
5.1	Мир виртуальный и реальный. Интернет зависимость.	2	2	-	
5.2	Кибербуллинг	2	-	2	1. https://www.9111.ru/questions/7777777772033338/ - советы юриста 2. https://resh.edu.ru/page/cyberproject-4 - видео РЭШ
5.3	Правила сетевого этикета	2	-	2	1. https://resh.edu.ru/subject/lesson/3350/train/#193801 –практическая часть с рэш 2. https://www.kaspersky.ru/resource-center/preemptive-safety/what-is-netiquette 3. http://school497.ru/download/u/01/urok7/les7.html
5.4	Мошеннические действия в Интернете. Киберпреступления	2	-	2	1. Пираты XXI века и как им противостоять 2. Денис Давид, инженер по информационной безопасности группы внедрения ОБИС, ООО “ИНФОРИОН” https://www.itweek.ru/security/article/detail.php?ID=218525 3. https://yandex.ru/video/preview/10563354142526510568 - видео Фишинг 4. https://101poisk.ru/slovar-internet-i-seo-terminov-dlya-chajnikov.html 5. https://resh.edu.ru/page/cyberproject-5 - видео РЭШ 6. https://resh.edu.ru/page/cyberproject-1 -видео РЭШ
5.5	Фишинг	2	2	-	
5.6	Потребительские опасности в Интернете	2	-	2	1. https://101poisk.ru/slovar-internet-i-seo-terminov-dlya-chajnikov.html 2. https://resh.edu.ru/page/cyberproject-6 - видео РЭШ 3.
5.7	Безопасность при использовании платежных карт в Интернете	2	-	2	1. https://yandex.ru/video/preview/10563354142526510568 - видео 2. https://resh.edu.ru/page/cyber-project - КИБЕР БЕЗОПАСНОСТЬ ДЛЯ ДЕТЕЙ И ВЗРОС-

					ЛЫХ (ВИДЕОПОДБОРКА)
5.8	Россия на пути к информационному обществу	2	2	-	1. https://resh.edu.ru/subject/lesson/5495/conspect/166747/ - РЭШ 2. https://resh.edu.ru/subject/lesson/5495/main/166752/ - видео 3. https://resh.edu.ru/subject/lesson/5495/train/166755/ - задание
5.9	Ложная информация в Интернете	2	2	-	1. https://resh.edu.ru/subject/lesson/5495/conspect/166747/ - РЭШ 2. https://resh.edu.ru/subject/lesson/5495/main/166752/ - видео 3. https://resh.edu.ru/subject/lesson/5495/train/166755/ - задание 4. https://resh.edu.ru/page/cyberproject-3 - видео РЭШ 5. https://resh.edu.ru/page/cyberproject-2 - видео РЭШ
5.10	Государственная политика в области защиты информации.	2	-	2	1. https://intuit.ru/studies/courses/3601/843/lecture/31531?page=3 – лекция ИНТУИТ Национальный открытый университет 2. https://mcs.mail.ru/blog/zakonodatelstvo-ob-informatsionnoy-bezopasnosti
	Дифференцированный зачет	2	2	-	-
	Итого	**39**	**19**	**20**	

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Для студентов

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
4. Прохорова О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова.— 2_е изд., стер. — Санкт_Петербург : Лань, 2021.— 124 с. : ил.— Текст : непосредственный.
   ISBN 978_5_8114_7338_0
5. Нестеров, С. А. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессиональное образование).
   ISBN 978-5-534-07979-1

Электронный учебник

1. Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://rkn.gov.ru/
2. Цветкова М. С., Голубчиков С. В., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10–11 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
3. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/ authors/ib/
4. «Безопасный Билайн», компания Билайн, URL: http:// moskva.beeline.ru/customers/help/safebeeline/
5. «Безопасность», компания МТС, URL: http://www.safety. mts.ru/ru/
6. «Безопасное общение», компания Мегафон, URL: http:// moscow.megafon.ru/bezopasnoe_obschenie/
7. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/ stopfraud/brochure.pdf
8. Открытый онлайнкурс «Безопасность в Интернете», «Академия Яндекс», компания Яндекс, URL: https:// academy.yandex.ru/events/onlinecourses/internet_security/
9. Дети в информационном обществе // http://detionline.com/journal/about
10. Защита детей by Kaspersky // https://kids.kaspersky.ru/
11. Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
12. http://lbz.ru/metodist/authors/ib/10-11.php
13. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций https://rkn.gov.ru/

Ресурсы для выполнения практических заданий к занятиям из открытых электронных документов и ресурсов

1. «ИНТУИТ» Национальный открытый университет https://intuit.ru/studies/courses/10/10/lecture/296; http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Указ Президента Российской Федерации №203/2017 г. «О стратегии развития информационного общества в Российской Федерации до 2030 года»

4. Указ №646/2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации»
5. Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р «Концепция информационной безопасности детей»
6. ДОКУМЕНТЫ, РЕГУЛИРУЮЩИЕ РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИИ
7. Конституция Российской Федерации http://www.constitution.ru/
8. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (ред. от 01.05.2019) https://fzrf.su/zakon/o-zashchite-detej-ot-informacii-436-fz/
9. Курсы Цифровая грамотность
10. Федеральный закон от 30 ноября 1994 года № 51-ФЗ «Гражданский кодекс Российской Федерации (ГК РФ). http://www.consultant.ru/document/cons_doc_LAW_5142/
11. Федеральный закон от 30 декабря 2001 года № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (КоАП РФ) http://www.consultant.ru/document/cons_doc_LAW_34661/;
12. Изменения КоАП 2021 года
13. Федеральный закон от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс Российской Федерации» (УК РФ) http://www.consultant.ru/document/cons_doc_LAW_10699/
14. Федеральный закон от 18 декабря 2001 года № 174-ФЗ «Уголовно-процессуальный кодекс Российской Федерации» (УПК РФ) http://www.consultant.ru/document/cons_doc_LAW_34481/