МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования Самарской области
Кинельское управление министерства образования Самарской области
ГБОУ СОШ с. Георгиевка

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании МО "Точных наук" Руководитель МО	заместителем директора по УВР	и.о. директора ГБОУ СОШ с. Георгиевка
Цыганова Э.В. Протокол №1 от 28.08.2024 г.	Климова Е.Ф. 29.08.2024 г.	Шафигулина О.С. Приказ № 85-ОД от 30.08.2024 г.

Шафигулина О.С.
C=RU, O=ГБОУ СОШ с. Георгиевка, CN=Шафигулина О.С., E=so_knl_georg_sch@samara.edu.ru
0090b6f41e18d0dc73
2024.08.30 14:54:39+03'00'

Рабочая программа
курса внеурочной деятельности

Информационная безопасность

основного общего образования
Педагогическое сопровождение (воспитательная направленность)

9 класс

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа курса внеурочной деятельности «Информационная безопасность» (далее — курс) для 9 класса составлена на основе требований Федерального государственного образовательного стандарта основного общего образования к результатам освоения основной программы основного общего образования (приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования») с учётом Программы воспитания (протокол Федерального учебно-методического объединения по общему образованию № 3/22 от 23.06.2022) и Основной образовательной программы основного общего образования (протокол Федерального учебно-методического объединения по общему образованию № 1/22 от 18.03.2022).

Рабочая программа курса даёт представление о цели, задачах, общей стратегии обучения, воспитания и развития обучающихся средствами курса внеурочной деятельности, устанавливает содержание курса, предусматривает его структурирование по разделам и темам; предлагает распределение учебных часов по разделам и темам и последовательность их изучения с учётом межпредметных и внутрипредметных связей, логики учебного процесса и возрастных особенностей обучающихся, включает описание форм организации занятий и учебно-методического обеспечения образовательного процесса.

Рабочая программа курса определяет количественные и качественные характеристики учебного материала, в том числе планируемые результаты освоения обучающимися программы курса внеурочной деятельности на уровне основного общего образования и систему оценки достижения планируемых результатов.

Общая характеристика учебного курса «Информационная безопасность»

Начинать обучение по курсу информационной безопасности крайне актуально по острым проблемным ситуациям в условиях присутствия в жизни детей персональных устройств работы в сети Интернет и мобильных сетях связи, а также для содействия при использовании детьми Интернета для обучения, творческого и развивающего досуга, познавательной деятельности. Программа направлена на решение вопросов массового формирования культуры информационной безопасности школьников, которые живут в современном информационном обществе, стремительно расширяющем общедоступные коммуникации в Интернете.

Проникновение мобильных устройств с доступом к Интернету в быт и досуг детей обострило проблему интернет-зависимости, игромании, зависимости от социальных сетей, необоснованного доверия посторонним людям в сети и, как следствие, незащищенности детей от атак мошенников, преступников, агрессивно настроенных людей, включая вовлечение детей в теневые, закрытые субкультуры, несущие угрозу здоровью и даже жизни ребенка.

Курс «Информационная безопасность» структурирован по модульному принципу. Он включает в себя 7 модулей:

- Общие сведения о безопасности ПК и Интернета
- Техника безопасности и экология
- Проблемы Интернет-зависимости
- Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
- Мошеннические действия в Интернете. Киберпреступления
- Сетевой этикет. Психология и сеть
- Правовые аспекты защиты киберпространства

Цели изучения учебного курса «Информационная безопасность»

Безопасность в сети Интернет в свете быстрого развития информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, а также в связи с массовым использованием детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Программа учебного курса информационной безопасности имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

При реализации требований безопасности в сети Интернет для любого пользователя, будь то школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к противоправной негативной информации. Но включение детей в интернет-взаимодействие наиболее активно осуществляется вне школы без надлежащего надзора со стороны взрослых.

В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у детей *культуры информационной безопасности* при работе в сети Интернет вне школы с участием родителей. Для этого следует проводить непрерывную образовательно-просветительскую работу с детьми, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет — важная задача для вовлечения детей в современную

цифровую образовательную среду, отвлечения их от бесполезного контента и игромании, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения детей, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения детей:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта 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 последствия 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, 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.

Место учебного курса «Информационная безопасность» в учебном плане

Особенностью программы курса является ее поэтапное развитие для разных возрастных групп обучающихся основного общего образования с учетом из возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им.

Данный курс реализуется в рамках социального направления внеурочной деятельности и рассчитан на 17 часов 9 классе.

Программа учебного курса поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. 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.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРОГРАММЕ

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

Патриотическое воспитание:

- ценностное отношение к отечественному культурному, историческому и научному наследию;

- понимание значения информатики как науки в жизни современного общества.

Духовно-нравственное воспитание:

- ориентация на моральные ценности и нормы в ситуациях нравственного выбора;
- готовность оценивать своё поведение и поступки, а также поведение и поступки других людей с позиции нравственных и правовых норм, с учётом осознания последствий поступков;
- активное неприятие асоциальных поступков, в том числе в Интернете.

Гражданское воспитание:

- представление о социальных нормах и правилах межличностных отношений в коллективе, в том числе в социальных сообществах;
- соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде;
- ориентация на совместную деятельность при выполнении учебных и познавательных задач, создании учебных проектов;
- стремление оценивать своё поведение и поступки своих товарищей с позиции нравственных и правовых норм, с учётом осознания последствий поступков.

Ценность научного познания:

- наличие представлений об информации, информационных процессах и информационных технологиях, соответствующих современному уровню развития науки и общественной практики;
- интерес к обучению и познанию;
- любознательность;
- стремление к самообразованию;
- овладение начальными навыками исследовательской деятельности, установка на осмысление опыта, наблюдений, поступков и стремление совершенствовать пути достижения индивидуального и коллективного благополучия;
- наличие базовых навыков самостоятельной работы с учебными текстами, справочной литературой, разнообразными средствами информационных технологий, а также умения
- самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности.

Формирование культуры здоровья:

- установка на здоровый образ жизни, в том числе и за счёт освоения и соблюдения требований безопасной эксплуатации средств ИКТ.

Трудовое воспитание:

- интерес к практическому изучению профессий в сферах деятельности, связанных с информатикой, программированием и информационными технологиями, основанными на достижениях науки информатики и научно-технического прогресса.

Экологическое воспитание:

- наличие представлений о глобальном характере экологических проблем и путей их решения, в том числе с учётом возможностей ИКТ.

Адаптация обучающегося к изменяющимся условиям социальной среды:

- освоение обучающимися социального опыта, основных социальных ролей, соответствующих ведущей деятельности возраста, норм и правил общественного поведения, форм социальной жизни в группах и сообществах, в том числе в виртуальном пространстве.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Универсальные познавательные действия

***Базовые логические действия*:**

- умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логические рассуждения, делать умозаключения (индуктивные, дедуктивные и по аналогии) и выводы;
- умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;
- самостоятельно выбирать способ решения учебной задачи (сравнивать несколько вариантов решения, выбирать наиболее подходящий с учётом самостоятельно выделенных критериев).

***Базовые исследовательские действия*:**

- формулировать вопросы, фиксирующие разрыв между реальным и желательным состоянием ситуации, объекта, и самостоятельно устанавливать искомое и данное;
- оценивать применимость и достоверность информации, полученной в ходе исследования;
- прогнозировать возможное дальнейшее развитие процессов, событий и их последствия в аналогичных или сходных ситуациях, а также выдвигать предположения об их развитии
- в новых условиях и контекстах.

***Работа с информацией*:**

- выявлять дефицит информации, данных, необходимых для решения поставленной задачи;
- применять основные методы и инструменты при поиске и отборе информации из источников с учётом предложенной учебной задачи и заданных критериев;
- выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;
- выбирать оптимальную форму представления информации и иллюстрировать решаемые задачи несложными схемами, диаграммами, иными графическими объектами и их комбинациями;
- оценивать достоверность информации по критериям, предложенным учителем или сформулированным самостоятельно;
- запоминать и систематизировать информацию.

Универсальные коммуникативные действия

***Общение*:**

- сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;
- публично представлять результаты выполненного опыта (исследования, проекта);
- выбирать формат выступления с учётом задач презентации и особенностей аудитории и в соответствии с ним составлять устные и письменные тексты с использованием иллюстративных материалов.

***Совместная деятельность (сотрудничество)*:**

- понимать и использовать преимущества командной и индивидуальной работы при решении конкретной проблемы, в том числе при создании информационного продукта;
- принимать цель совместной информационной деятельности по сбору, обработке, передаче и формализации информации, коллективно строить действия по её достижению: распределять роли, договариваться, обсуждать процесс и результат совместной работы;
- выполнять свою часть работы с информацией или информационным продуктом, достигая качественного результата по своему направлению и координируя свои действия с другими членами команды;

- оценивать качество своего вклада в общий информационный продукт по критериям, самостоятельно сформулированным участниками взаимодействия;
- сравнивать результаты с исходной задачей и вклад каждого члена команды в достижение результатов, разделять сферу ответственности и проявлять готовность к предоставлению отчёта перед группой.

Универсальные регулятивные действия

***Самоорганизация*:**

- выявлять в жизненных и учебных ситуациях проблемы, требующие решения;
- составлять алгоритм решения задачи (или его часть), выбирать способ решения учебной задачи с учётом имеющихся ресурсов и собственных возможностей, аргументировать выбор варианта решения задачи;
- составлять план действий (план реализации намеченного алгоритма решения), корректировать предложенный алгоритм с учётом получения новых знаний об изучаемом объекте.

***Самоконтроль (рефлексия)*:**

- владеть способами самоконтроля, самомотивации и рефлексии;
- учитывать контекст и предвидеть трудности, которые могут возникнуть при решении учебной задачи, адаптировать решение к меняющимся обстоятельствам;
- вносить коррективы в деятельность на основе новых обстоятельств, изменившихся ситуаций, установленных ошибок, возникших трудностей;
- оценивать соответствие результата цели и условиям.

***Эмоциональный интеллект*:**

- ставить себя на место другого человека, понимать мотивы и намерения другого.

***Принятие себя и других*:**

осознавать невозможность контролировать всё вокруг даже в условиях открытого доступа к любым объёмам информации.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

- понимание личной и общественной значимости современной культуры безопасности жизнедеятельности;
- знание основных опасных и чрезвычайных ситуаций социального характера, включая экстремизм и терроризм, и их последствий для личности, общества и государства; формирование антиэкстремистской и антитеррористической личностной позиции;
- знание и умение применять меры безопасности и правила поведения в условиях опасных и чрезвычайных ситуаций.
- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики;
- умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

В результате освоения программы курса ученик освоит жизненно важные практические компетенции.

Выпускник научится понимать:

- источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;
- роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;
- виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;
- проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

- этикет сетевого взаимодействия, правовые нормы в сфере информационной безопасности;
- правила защиты персональных данных;
- назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

Выпускник научится применять на практике:

- правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);
- компетенции медиаинформационной грамотности при работе с информацией в сети Интернет, критическое и избирательное отношение к источникам информации;
- компетенции компьютерной грамотности по защите персональных устройств от вредоносных программ, использованию антивирусных программных средств, лицензионного программного обеспечения;
- информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.

Для выявления достижения планируемых результатов обучения используются диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

9 класс

Модуль 1. Общие сведения о безопасности ПК и Интернета (7 часов).

Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.

Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации.

Что такое защищенная информационная среда. Защита каналов передачи данных, средства предотвращения утечки информации, защита информации от НСД (антивирусная защита, средства контроля защищенности, средства обнаружения и предупреждения атак), средства аутентификации.

Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.

Требования к безопасности информации: сохранение целостности, конфиденциальности и доступности. Определения по ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения».

Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.

Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).

Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.

Угрозы информации (техногенные, случайные и преднамеренные; природные). Неосторожность пользователя как одна из угроз для информационной безопасности.

Меры кибербезопасности для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО.

Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности).

Модуль 2. Техника безопасности и экология (1 час).

Кибератаки на инфраструктуру.

Компьютер в режиме труда и отдыха. Информационная перегрузка.

Влияние компьютера на репродуктивную систему.

Модуль 3. Проблемы Интернет-зависимости (1 час).

Интернет- и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость.

Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

Модуль 4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (3 часа).

Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Методы защиты.

Проверка подлинности (аутентификация) в Интернете.

Меры безопасности для пользователя WiFi. Настройка безопасности.

Вирусы для мобильных устройств (мобильные банкеры и др.).

Настройка компьютера для безопасной работы.

Ошибки пользователя (установка нескольких антивирусов, установка слишком большого числа программ, отсутствие резервного копирования и т.п.).

Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.

Модуль 5. Мошеннические действия в Интернете. Киберпреступления (3 часа).

Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.

Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.

Мошеннические действия в сети. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды.

Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег.

Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.

Платные предложения работы. Платный просмотр видеоматериалов.
Технологии манипулирования в Интернете.

Модуль 6. Сетевой этикет. Психология и сеть (1 час).

Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Сетевой этикет. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.

Модуль 7. Правовые аспекты защиты киберпространства (1 часа).

Как расследуются преступления в сети.
Ответственность за интернет-мошенничество.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

№ п/п	Наименование модулей	Кол-во часов
1	Общие сведения о безопасности ПК и Интернета	7
2	Техника безопасности и экология.	1
3	Проблемы Интернет-зависимости	1
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	3
5	Мошеннические действия в Интернете. Киберпреступления	3
6	Сетевой этикет. Психология и сеть	1
7	Правовые аспекты защиты киберпространства	1
	Всего часов:	**17**

Поурочное планирование

9 класс (17 часа)

№ урока	Тема	Кол-во часов
	Общие сведения о безопасности ПК и Интернета.	**7**
1	Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности.	1
2	Компьютерная и информационная безопасность. Что такое защищенная информационная среда.	1
3	Организационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средства резервного копирования и восстановления.	1
4	Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации.	1
5	Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты).	1
6	Угрозы безопасности в сетях WiFi. Методы защиты сетей WiFi.	1
7	Меры кибербезопасности для конечных пользователей. Киберугрозы Интернета (кибервойны, манипулирование людьми,	1

	зависимость, вирусные атаки, отсутствие приватности).	
	Техника безопасности и экология.	**1**
8	Кибератаки на инфраструктуру. Компьютер в режиме труда и отдыха. Информационная перегрузка. Влияние компьютера на репродуктивную систему.	1
	Проблемы Интернет-зависимости.	**1**
9	Интернет- и компьютерная зависимость (аддикция). Типы интернет-зависимости.	1
	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	**3**
10	Проблемы безопасности инфраструктуры Интернета. Методы защиты. Меры безопасности для пользователя Wi-Fi. Настройка безопасности.	1
11	Настройка компьютера и телефона для безопасной работы. Ошибки пользователя.	1
12	Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях.	1
	Мошеннические действия в Интернете. Киберпреступления.	**3**
13	Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса.	1
14	Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники. Платные предложения работы. Платный просмотр видеоматериалов.	1
15	Что такое электронный кошелек – удобства и проблемы безопасности. «Обменники» для электронных денег. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Технологии манипулирования в Интернете.	1
	Сетевой этикет. Психология и сеть.	**1**
16	Безопасная работа в сети в процессе сетевой коммуникации. Сетевой этикет.	1
	Правовые аспекты защиты киберпространства.	**1**
17	Как расследуются преступления в сети. Ответственность за интернет-мошенничество.	1