**Федеральная рабочая программа**

**Основы безопасности и защиты Родины**

**8–9 классы**

Программа ОБЗР обеспечивает:

* ясное понимание обучающимися современных проблем безопасности и формирование у подрастающего поколения базового уровня культуры безопасного поведения;
* прочное усвоение обучающимися основных ключевых понятий, обеспечивающих преемственность изучения основ комплексной безопасности личности на следующем уровне образования;
* возможность выработки и закрепления у обучающихся умений и навыков, необходимых для последующей жизни;
* выработку практико-ориентированных компетенций, соответствующих потребностям современности;
* реализацию оптимального баланса межпредметных связей и их разумное взаимодополнение, способствующее формированию практических умений и навыков.

**Темы программы, рекомендуемые для включения в обучение**

**по кибербезопасности**

**Модуль № 1 «Безопасное и устойчивое развитие личности, общества, государства»**

*Предметные результаты обучающихся:*

* раскрывать понятия «национальные интересы» и «угрозы национальной безопасности», приводить примеры;
* раскрывать классификацию чрезвычайных ситуаций по масштабам и источникам возникновения, приводить примеры;
* раскрывать способы информирования и оповещения населения о чрезвычайных ситуациях.

**Тема 1.1. Роль безопасности в жизни человека, общества, государства**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Фундаментальные ценности и принципы, формирующие основы российского общества, безопасности страны, закрепленные в Конституции Российской Федерации.  Стратегия национальной безопасности.  Национальные интересы и угрозы национальной безопасности | 1. Карта-схема стратегии национальной безопасности с включением элементов информационной (кибер)безопасности |

**Модуль № 3 «Культура безопасности жизнедеятельности в современном обществе»:**

*Предметные результаты обучающихся:*

* классифицировать и характеризовать источники опасности.

**Тема 3.1. Основы безопасности жизнедеятельности**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Безопасность жизнедеятельности: ключевые понятия и значение для человека.  Смысл понятий «опасность», «безопасность», «риск», «культура безопасности жизнедеятельности».  Источники и факторы опасности, их классификация.  Общие принципы безопасного поведения | 1. Карта–схема источников опасности для жизнедеятельности с включением источников цифровой природы (информационные, киберопасности)  2. Ситуационные задачи (модели реальных ситуаций, требующих поиска решений воздействия на источники и факторы опасности комбинированного характера (материального, реального и цифрового, виртуального) |

**Модуль № 10 «Безопасность в информационном пространстве».**

*Предметные результаты обучающихся:*

* раскрывать понятие «цифровая среда», её характеристики и приводить примеры информационных и компьютерных угроз;
* объяснять положительные возможности цифровой среды;
* характеризовать риски и угрозы при использовании Интернета;
* знать общие принципы безопасного поведения, необходимые для предупреждения возникновения опасных ситуаций в личном цифровом пространстве;
* характеризовать опасные явления цифровой среды;
* классифицировать и оценивать риски вредоносных программ и приложений, их разновидностей;
* иметь навыки соблюдения правил кибергигиены для предупреждения возникновения опасных ситуаций в цифровой среде;
* характеризовать основные виды опасного и запрещённого контента в Интернете и характеризовать его признаки;
* раскрывать приёмы распознавания опасностей при использовании Интернета;
* характеризовать противоправные действия в Интернете;
* иметь навыки соблюдения правил цифрового поведения, необходимых для снижения рисков и угроз при использовании Интернета (кибербуллинга, вербовки в различные организации и группы);
* характеризовать деструктивные течения в Интернете, их признаки и опасности;
* иметь навыки соблюдения правил безопасного использования Интернета, необходимых для снижения рисков и угроз вовлечения в различную деструктивную деятельность.

**Тема 10.1. Общие принципы безопасности в цифровой среде.**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Понятие «цифровая среда», её характеристики и примеры информационных и компьютерных угроз, положительные возможности цифровой среды | 1. Понятие «цифровая среда» и его компонентов с описанием характеристик.  2. Виды интернет-рисков  3. Чек-лист положительных возможностей цифровой среды  4. Тест на проверку знаний о компонентах цифровой среды, информационных угрозах, позитивной значимости цифровых технологий |
| Риски и угрозы при использовании Интернета | 1. Алгоритм выявления признаков угроз и рисков при использовании Интернета  2. Карта рисков и угроз для личности  3. Карта рисков и угроз для общества |
| Общие принципы безопасного поведения, необходимые для предупреждения возникновения опасных ситуаций в личном цифровом пространстве | Ситуационные задачи (модели реальных ситуаций, требующих поиска решений предупреждения возникновения опасных ситуаций в личном цифровом пространстве) |

**Тема10.2. Опасные программы и явления цифровой среды**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Опасные явления цифровой среды: вредоносные программы и приложения и их разновидности | 1. Карта-схема опасных явлений цифровой среды  2. Тест на проверку знаний о классификации вредоносных программ и приложений и их разновидностей |
| Правила кибергигиены, необходимые для предупреждения возникновения опасных ситуаций в цифровой среде | Ситуационные задачи (модели реальных ситуаций, требующих поиска решений предупреждения возникновения опасных ситуаций в общественном цифровом пространстве) |

**Тема 10.3.** **Безопасные правила цифрового поведения**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Основные виды опасного и запрещённого контента в Интернете и его признаки, приёмы распознавания опасностей при использовании Интернета | 1. Карта-схема видов опасного и запрещённого контента в Интернете  2. Тест на проверку знаний приёмов распознавания опасностей при использовании Интернета |
| Противоправные действия в Интернете | Ситуационные задачи (модели реальных ситуаций, требующих определения действий в Интернете правового характера) |
| Правила цифрового поведения, необходимого для снижения рисков и угроз при использовании Интернета (кибербуллинга, вербовки в различные организации и группы) | 1. Игра «Цифровые правила» (быстрые ответы «да-нет», ответы «одним словом» и т.д.), направленные на профилактику кибербуллинга, вербовки в различные организации и группы  2. Ситуационные задачи (модели реальных ситуаций, требующих поиска решений, направленных на профилактику кибербуллинга, вербовки в различные организации и группы) |

**Федеральная рабочая программа**

**Основы безопасности и защиты Родины**

**10–11 классы**

Программа ОБЗР обеспечивает:

* формирование личности выпускника с высоким уровнем культуры и мотивации ведения безопасного, здорового и экологически целесообразного образа жизни;
* достижение выпускниками базового уровня культуры безопасности жизнедеятельности, соответствующего интересам обучающихся и потребностям общества в формировании полноценной личности безопасного типа;
* взаимосвязь личностных, метапредметных и предметных результатов освоения учебного предмета ОБЗР на уровнях основного общего и среднего общего образования;
* подготовку выпускников к решению актуальных практических задач безопасности жизнедеятельности в повседневной жизни.

**Темы программы, рекомендуемые для включения в обучение**

**по кибербезопасности**

**МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ**

**Работа с информацией:**

* владеть навыками самостоятельного поиска, сбора, обобщения и анализа различных видов информации из источников разных типов при обеспечении условий информационной безопасности личности;
* создавать информационные блоки в различных форматах с учетом характера решаемой учебной задачи;
* самостоятельно выбирать оптимальную форму их представления. оценивать достоверность, легитимность информации, ее соответствие правовым и морально-этическим нормам;
* владеть навыками по предотвращению рисков, профилактике угроз и защите от опасностей цифровой среды;
* использовать средства информационных и коммуникационных технологий в учебном процессе с соблюдением требований эргономики, техники безопасности и гигиены.

**Модуль № 1 «Безопасное и устойчивое развитие личности, общества, государства»**

*Предметные результаты:*

* раскрывать правовые основы и принципы обеспечения национальной безопасности Российской Федерации;
* характеризовать роль личности, общества и государства в достижении стратегических национальных приоритетов, объяснять значение их реализации в обеспечении комплексной безопасности и устойчивого развития Российской Федерации, приводить примеры;
* характеризовать роль правоохранительных органов и специальных служб в обеспечении национальной безопасности;
* объяснять роль личности, общества и государства в предупреждении противоправной деятельности.

**Тема 1.1. Взаимодействие личности, общества и государства в обеспечении национальной безопасности**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Российская Федерация в современном мире.  Правовая основа обеспечения национальной безопасности.  Принципы обеспечения национальной безопасности.  Реализация национальных приоритетов как условие обеспечения национальной безопасности и устойчивого развития Российской Федерации.  Взаимодействие личности, государства и общества в реализации национальных приоритетов | 1. Блок-схема «Правовые основы и принципы обеспечения национальной безопасности РФ (на примере информационной безопасности).  2. Ситуационные задачи на определение роли личности, общества и государства в достижении стратегических национальных приоритетов в информационной безопасности. |

**Тема 1.2. Государственная и общественная безопасность**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Роль правоохранительных органов и специальных служб в обеспечении национальной безопасности.  Роль личности, общества и государства в предупреждении противоправной деятельности | 1. Тест на проверку знаний правового характера о действиях Министерства внутренних дел Российской Федерации, Федеральной службы безопасности Российской Федерации, Службы внешней разведки Российской Федерации, Росгвардии России и общественных институтов в обеспечении информационной безопасности на основе стратегии национальной безопасности. |

**Тема 1.4. Оборона страны как обязательное условие благополучного развития страны**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Россия в современном мире. Оборона страны как обязательное условие мирного социально-экономического развития Российской Федерации и обеспечение ее военной безопасности.  Роль Вооруженных Сил Российской Федерации в обеспечении национальной безопасности | 1. Таблица с элементами инфографики «Угрозы военной безопасности Российской Федерации цифрового характера»  2. Блок-схема «Примеры цифровых решений (приборы, техническое оборудование, программное обеспечение и т.п.) обеспечения военной безопасности» |

**Модуль № 3 «Культура безопасности жизнедеятельности в современном обществе»**

*Предметные результаты*

объяснять смысл понятий «опасность», «безопасность», «риск (угроза)», «культура безопасности», «опасная ситуация», «чрезвычайная ситуация», объяснять их взаимосвязь;

приводить примеры решения задач по обеспечению безопасности в повседневной жизни (индивидуальный, групповой и общественно-государственный уровни);

знать общие принципы безопасного поведения, приводить примеры.

**Тема 3.1. Современные представления о культуре безопасности**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Понятие «культура безопасности», его значение в жизни человека, общества, государства.  Соотношение понятий «опасность», «безопасность», «риск» (угроза).  Соотношение понятий «опасная ситуация», «чрезвычайная ситуация».  Общие принципы (правила) безопасного поведения.  Индивидуальный, групповой, общественно-государственный уровни решения задачи обеспечения безопасности | 1. Видеоролики с примерами решения задач по обеспечению информационной безопасности в повседневной жизни (индивидуальный, групповой и общественно-государственный уровни). |

**Модуль № 9 «Безопасность в социуме»**

*Предметные результаты:*

* приводить примеры межличностного общения и общения в группе; иметь навыки конструктивного общения в информационном пространстве;
* понимать влияние групповых норм и ценностей на комфортное и безопасное взаимодействие в группе в информационном пространстве, приводить примеры;
* раскрывать способы противодействия буллингу, проявлениям насилия;
* называть характеристики манипулятивного воздействия в информационном пространстве, приводить примеры;
* иметь представления о способах противодействия манипуляции в информационном пространстве;
* раскрывать механизмы воздействия на большую группу (заражение, убеждение, внушение, подражание и другие), приводить примеры.

**Тема 9.1. Общение в жизни человека. Межличностное общение, общение в группе**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Определение понятия «общение».  Навыки конструктивного общения.  Общие представления о понятиях «социальная группа», «большая группа», «малая группа».  Межличностное общение, общение в группе, межгрупповое общение  (взаимодействие). Особенности общения в группе. Психологические характеристики группы и особенности взаимодействия в группе.  Групповые нормы и ценности. Коллектив как социальная группа.  Психологические закономерности в группе | Ситуационные задачи с примерами влияния групповых норм и ценностей на взаимодействие в группе, межличностного общения и общения в группе с использованием цифровых технологий для выработки навыков конструктивного общения в социальных сетях и Интернет-сообществах (технология «Социальный театр» с использованием видеоматериалов) |

**Тема 9.3. Конструктивные и деструктивные способы психологического воздействия**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Способы психологического воздействия.  Психологическое влияние в малой группе. Положительные и отрицательные стороны конформизма.  Эмпатия и уважение к партнеру (партнерам) по общению как основа коммуникации.  Убеждающая коммуникация. Манипуляция в общении.  Цели, технологии и способы противодействия | 1. Карта-схема способов психологического воздействия в информационном пространстве (реклама, подписки, маркеты, посты, личные сообщения и т.п.).  2. Ситуационные задачи (аудиоформат, письмо по электронной почте, сообщение в мессенджерах) с примерами манипулятивного воздействия для формирования навыков противодействия манипуляции в цифровой среде |

**Модуль № 10 «Безопасность в информационном пространстве»:**

*Предметные результаты:*

* характеризовать цифровую среду, ее влияние на жизнь человека;
* объяснять смысл понятий «цифровая среда», «цифровой след», «персональные данные»;
* анализировать угрозы цифровой среды (цифровая зависимость, вредоносное программное обеспечение, сетевое мошенничество и травля, вовлечение в деструктивные сообщества, запрещенный контент и другие), раскрывать их характерные признаки;
* иметь навыки безопасных действий по снижению рисков, и защите от опасностей цифровой среды;
* объяснять смысл понятий «программное обеспечение», «вредоносное программное обеспечение»;
* характеризовать и классифицировать опасности, анализировать риски, источником которых является вредоносное программное обеспечение;
* иметь навыки безопасного использования устройств и программ;
* перечислять и классифицировать опасности, связанные с поведением людей в цифровой среде;
* характеризовать риски, связанные с коммуникацией в цифровой среде (имитация близких социальных отношений; травля; шантаж разглашением сведений; вовлечение в деструктивную, противоправную деятельность), способы их выявления и противодействия им;
* иметь навыки безопасной коммуникации в цифровой среде;
* объяснять смысл и взаимосвязь понятий «достоверность информации», «информационный пузырь», «фейк»;
* иметь представление о способах проверки достоверности, легитимности информации, ее соответствия правовым и морально-этическим нормам;
* раскрывать правовые основы взаимодействия с цифровой средой, выработать навыки безопасных действий по защите прав в цифровой среде;
* объяснять права, обязанности и иметь представление об ответственности граждан и юридических лиц в информационном пространстве.

**Тема 10.1. Безопасность в цифровой среде**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Понятия «цифровая среда», «цифровой след».  Влияние цифровой среды на жизнь человека. Приватность, персональные данные.  «Цифровая зависимость», ее признаки и последствия.  Опасности и риски цифровой среды, их источники.  Правила безопасного поведения в цифровой среде | 1. Тест на проверку знаний понятий «цифровая среда», «цифровой след», «цифровая зависимость»  2. Ситуационные задачи по защите персональных данных в цифровой среде.  3. Чек-лист «Правила безопасного поведения в цифровой среде» |

**Тема 10.2. Опасности, связанные с использованием программного обеспечения**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Вредоносное программное обеспечение.  Виды вредоносного программного обеспечения, его цели, принципы работы. Правила защиты от вредоносного программного обеспечения.  Кража персональных данных, паролей.  Мошенничество, фишинг, правила защиты от мошенников.  Правила безопасного использования устройств и программ | 1. Тест на проверку знаний понятий «программное обеспечение», «вредоносное программное обеспечение».  2. Карта-схема «Классификация опасностей и рисков, источником которых является вредоносное программное обеспечение».  3. Имитационные задачи с использованием скриншотов с экрана диалогов при установке программного обеспечения для вырабатывают навыки безопасного использования устройств и программ |

**Тема 10.3. Опасности, связанные с коммуникацией в цифровой среде**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Поведенческие опасности в цифровой среде и их причины.  Опасные персоны, имитация близких социальных отношений. Неосмотрительное поведение  и коммуникация в Сети как угроза для будущей жизни и карьеры.  Травля в Сети, методы защиты от травли.  Деструктивные сообщества и деструктивный контент в цифровой среде, их признаки. Механизмы вовлечения в деструктивные сообщества. Вербовка, манипуляция, воронки вовлечения.  Радикализация деструктива. Профилактика и противодействие вовлечению в деструктивные сообщества.  Правила коммуникации в цифровой среде | 1. Карта-схема «Классификация опасностей, связанные с поведением людей в цифровой среде».  2. Ситуационные задачи, связанные с коммуникацией в цифровой среде (имитация близких социальных отношений; травля; шантаж разглашением сведений; вовлечение в деструктивную, противоправную деятельность), для поиска способов выявления и противодействия рискам и угрозам информационной безопасности.  3. Чек-лист «Правила коммуникации в цифровой среде» |

**Тема 10.4. Достоверность информации в цифровой среде**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Достоверность информации в цифровой среде.  Источники информации. Проверка на достоверность.  «Информационный пузырь», манипуляция сознанием, пропаганда. Фальшивые аккаунты, вредные  советчики, манипуляторы. Понятие «фейк», цели и виды, распространение фейков.  Правила и инструменты для распознавания фейковых текстов и изображений | 1. Карта признаков и методов распознавания фальшивых аккаунтов.  2. Чек-лист по проверке достоверности информации  3. Чек-лист по распознаванию фейковых текстов и изображений |

**Тема 10.5. Защита прав в цифровом пространстве**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Понятие прав человека в цифровой среде, их защита.  Ответственность за действия в Интернете.  Запрещенный контент.  Защита прав в цифровом пространстве | 1. Чек-лист «Правовые основы взаимодействия с цифровой средой»  2. Тест на проверку знаний по правам и обязанностям граждан в цифровой среде» |

**Модуль № 11 «Основы противодействия экстремизму и терроризму»**

*Предметные результаты:*

характеризовать признаки вовлечения в экстремистскую и террористическую деятельность в информационном пространстве, выработать навыки безопасных действий при их обнаружении;

объяснять права, обязанности и иметь представление об ответственности граждан и юридических лиц в области противодействия экстремизму и терроризму.

**Тема 11.1. Экстремизм и терроризм как угроза устойчивого развития общества**

|  |  |
| --- | --- |
| Содержание занятий | Методические материалы |
| Экстремизм и терроризм как угроза устойчивого развития общества.  Понятия «экстремизм» и «терроризм», их взаимосвязь. Варианты проявления экстремизма, возможные последствия.  Преступления террористической направленности, их цель, причины, последствия. Опасность вовлечения в экстремистскую и террористическую деятельность: способы и признаки.  Предупреждение и противодействие вовлечению в экстремистскую и террористическую деятельность | 1. Алгоритм анализа проявления экстремизма и терроризма в информационном пространстве и возможных последствий.  2. Ситуационные задачи с признаками вовлечения в информационном пространстве в экстремистскую и террористическую деятельность с целью поиска решений безопасных действий при их обнаружении. |