Реализация модуля «Безопасность в информационном пространстве»

современная школа

Спикеры
Захаров Вячеслав Владимирович,
директор ЦНППМ ПР г.Истра
Куторго Наталья Анатольевна,
кпн
заместитель начальника ГКУ ДПО «УМЦ ГО и ЧС»

ОСНОВЫ БЕЗОПАСНОСТИ И ЗАЩИТЫ РОДИНЫ
Модуль № 10 «Безопасность в информационном пространстве»

№ п/п	Наименование разделов и тем учебного предмета	Количество часов
10.1.	Безопасность в цифровой среде	1
10.2.	Опасности, связанные с использованием программного обеспечения	1
10.3.	Опасности, связанные с коммуникацией в цифровой среде	2
10.4.	Достоверность информации в цифровой среде	2
10.5.	Защита прав в цифровом пространстве	1
	Итого по модулю:	**7**

Модуль № 10 «Безопасность в информационном пространстве»
Раздел 10.1. Безопасность в цифровой среде

Программное содержание	Основные виды деятельности обучающихся
✓ Понятия «цифровая среда», «цифровой след». ✓ Влияние цифровой среды на жизнь человека. ✓ Приватность, персональные данные. ✓ «Цифровая зависимость», её признаки и последствия. ✓ Опасности и риски цифровой среды, их источники. ✓ Правила безопасного поведения в цифровой среде	✓ Характеризуют цифровую среду, её влияние на жизнь человека. ✓ Объясняют смысл понятий «цифровая среда», «цифровой след», «персональные данные». ✓ Анализируют угрозы цифровой среды (цифровая зависимость; вредоносное программное обеспечение; сетевое мошенничество и травля; вовлечение в деструктивные сообщества; запрещённый контент), раскрывают их характерные признаки. ✓ Вырабатывают навыки безопасных действий по предотвращению рисков, профилактике угроз и защите от опасностей цифровой среды

Модуль № 10 «Безопасность в информационном пространстве» Раздел 10.2. Опасности, связанные с использованием программного обеспечения

Программное содержание	Основные виды деятельности обучающихся
✓ 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	✓ Объясняют смысл понятий «программное обеспечение», «вредоносное программное обеспечение». ✓ Характеризуют и классифицируют опасности, анализируют риски, источником которых является вредоносное программное обеспечение. ✓ Вырабатывают навыки безопасного использования устройств и программ

современная школа

Модуль № 10 «Безопасность в информационном пространстве»
Раздел 10.3. Опасности, связанные с коммуникацией в цифровой среде

Программное содержание	Основные виды деятельности обучающихся
✓ Поведенческие риски 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	✓ Перечисляют и классифицируют риски, связанные с поведением людей в цифровой среде. ✓ Раскрывают опасности, 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. ✓ Вырабатывают навыки безопасной коммуникации в цифровой среде

Модуль № 10 «Безопасность в информационном пространстве»
Раздел 10.4. Достоверность информации в цифровой среде

Программное содержание	Основные виды деятельности обучающихся
✓ 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	✓ Объясняют смысл и взаимосвязь понятий «достоверность информации», «информационный пузырь», «фейк». ✓ Вырабатывают навыки проверки достоверности, легитимности информации, её соответствия правовым и морально-этическим нормам

Модуль № 10 «Безопасность в информационном пространстве»
Раздел 10.5. Защита прав в цифровом пространстве

Программное содержание	Основные виды деятельности обучающихся
✓ Понятие прав человека в цифровой среде, их защита. ✓ Ответственность за действия в Интернете. ✓ Запрещённый контент. ✓ Защита прав в цифровом пространстве	✓ Раскрывают правовые основы взаимодействия с цифровой средой, вырабатывают навыки безопасных действий по защите прав в цифровой среде. ✓ Объясняют права, обязанности и ответственность граждан и организаций в информационном пространстве

современная школа

Модуль № 10 «Безопасность в информационном пространстве»
Предметные результаты

- ✓ Характеризовать цифровую среду, её 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; запрещённый контент), раскрывать их характерные признаки
- ✓ Выработать навыки безопасных действий по предотвращению рисков, профилактике угроз 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
- ✓ Выработать навыки безопасного использования устройств и программ

современная школа

Модуль № 10 «Безопасность в информационном пространстве»
Предметные результаты

- ✓ Перечислять и классифицировать риски, связанные с поведением людей в цифровой среде
- ✓ Раскрывать опасности, 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
- ✓ Выработать навыки безопасной коммуникации в цифровой среде
- ✓ Объяснять смысл и взаимосвязь понятий «достоверность информации», «информационный пузырь», «фейк»
- ✓ Выработать навыки проверки достоверности, легитимности информации, её 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 ответственность граждан и организаций в информационном пространстве

Элементы системы безопасности

- ✓ Средства защиты
- ✓ Культура безопасного поведения
- ✓ Знания закономерностей среды и опасных факторов
- ✓ Умение человека предвидеть, выявлять и правильно оценивать опасные факторы и адекватно реагировать на них

современная школа

Практическое задание:

Установите соответствие предметных результатов освоения модуля элементам системы безопасности

Элементы системы безопасности	Предметные результаты
А. Средства защиты	1. Характеризовать цифровую среду, её влияние на жизнь человека 2. Анализировать угрозы цифровой среды (цифровая зависимость; вредоносное программное обеспечение; сетевое мошенничество …), раскрывать их характерные признаки 3. Выработать навыки безопасных действий по предотвращению рисков, профилактике угроз и защите от опасностей цифровой среды 4. Объяснять смысл понятий «программное обеспечение», «вредоносное программное обеспечение» 5. Характеризовать и классифицировать опасности, анализировать риски, источником которых является вредоносное программное обеспечение 6. Выработать навыки безопасного использования устройств и программ 7. Перечислять и классифицировать риски, связанные с поведением людей в цифровой среде 8. Раскрывать опасности, связанные с коммуникацией в цифровой среде (имитация близких социальных отношений; травля; шантаж разглашением сведений …), способы их выявления и противодействия им 9. Выработать навыки безопасной коммуникации в цифровой среде 10. Объяснять смысл и взаимосвязь понятий «достоверность информации», «информационный пузырь», «фейк» 11. Выработать навыки проверки достоверности, легитимности информации, её соответствия правовым и морально-этическим нормам 12. Раскрывать правовые основы взаимодействия с цифровой средой, выработать навыки безопасных действий по защите прав в цифровой среде 13. Объяснять права, обязанности и ответственность граждан и организаций в информационном пространстве
Б. Культура безопасного поведения	
В. Знания закономерностей среды и опасных факторов	
Г. Умение человека предвидеть, выявлять и правильно оценивать опасные факторы и адекватно реагировать на них	

современная школа

Практическое задание:
Установите соответствие предметных результатов освоения модуля элементам системы безопасности

современная школа

Правовые основы обеспечения информационной безопасности

Наименование документа	
Конституция Российской Федерации	Содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности
Федеральный закон от 28.12.2010 г. N 390-ФЗ «О безопасности»	Закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции
Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности
Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»	Определяет виды информации, причиняющей вред здоровью и (или) развитию детей, категории информационной продукции, дополнительные требования к ее распространению посредством теле- и радиовещания, сети Интернет
Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	Представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации
Концепция информационной безопасности детей в Российской Федерации, утв. Распоряжением Правительства РФ от 28.04.2023 N 1105-р	Определены мероприятия, направленные на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции

Информационная безопасность. Основные понятия

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Доступ к информации - возможность получения информации и ее использования;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

Информационная безопасность – состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Безопасность информации — защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

современная школа

Элементы системы безопасности - культура безопасного поведения

Культура безопасности в информационном пространстве — это совокупность сформированных знаний, умений и навыков по вопросам информационной безопасности, обеспечивающая безопасное пребывание гражданина Российской Федерации в информационном пространстве.

(Распоряжение Правительства РФ от 22 декабря 2022 г. № 4088-р О Концепции формирования и развития культуры информационной безопасности граждан РФ)

Основные принципы повышения уровня культуры информационной безопасности граждан

- ✓ ответственность государства за соблюдение законных интересов граждан Российской Федерации в информационной сфере;
- ✓ консолидация усилий органов государственной власти, неправительственных и коммерческих организаций в работе по повышению грамотности граждан Российской Федерации в вопросах информационной безопасности;
- ✓ проведение работы органами государственной власти по совершенствованию законодательства Российской Федерации, позволяющего на регулярной основе осуществлять реализацию мероприятий по повышению грамотности по вопросам информационной безопасности, в том числе для лиц, замещающих должности государственной гражданской и муниципальной службы Российской Федерации;
- ✓ проведение адаптированной под разные категории граждан Российской Федерации информационной кампании как основного способа повышения культуры информационной безопасности;
- ✓ проведение на регулярной основе иных мероприятий, направленных на повышение грамотности граждан Российской Федерации по вопросам информационной безопасности;
- ✓ формирование у граждан Российской Федерации ответственного отношения к личной информационной безопасности в цифровом пространстве.

современная школа

Элементы системы безопасности - культура безопасного поведения

Стратегическая цель государственной политики в области повышения культуры информационной безопасности граждан Российской Федерации — формирование у них навыков противодействия угрозам информационной безопасности, в том числе информационно-психологическим угрозам, и, как следствие, повышение общего уровня грамотности по вопросам информационной безопасности граждан Российской Федерации.

Приоритетные задачи в области повышения уровня культуры информационной безопасности граждан

- ✓ проведение на регулярной основе мониторинга уровня грамотности граждан Российской Федерации по вопросам информационной безопасности, в том числе путем проведения ежегодного тестирования;
- ✓ донесение на регулярной основе до граждан Российской Федерации значимости проблемы и последствий несоблюдения правил личной информационной безопасности;
- ✓ формирование у граждан Российской Федерации, не интересующихся вопросами личной информационной безопасности, интереса к указанной теме;
- ✓ повышение доверия к цифровым сервисам, в том числе к государственным;
- ✓ обучение граждан Российской Федерации новым образцам поведения, основанным на правилах личной информационной безопасности;
- ✓ выработка мероприятий по регулярному повышению грамотности по вопросам информационной безопасности лиц, замещающих должности государственной гражданской и муниципальной службы Российской Федерации;
- ✓ снижение актуальности угроз информационной безопасности, а также повышение эффективности противодействия их реализации;
- ✓ выстраивание взаимодействия органов государственной власти, неправительственных и коммерческих организаций, направленного на повышение грамотности граждан Российской Федерации по вопросам информационной безопасности;
- ✓ создание дополнительных точек взаимодействия с каждой отдельной категорией граждан Российской Федерации в целях эффективного донесения до них информации о важности соблюдения правил личной информационной безопасности посредством выбора неформальных каналов коммуникации и актуальных интересов

Элементы системы безопасности - культура безопасного поведения

Критерии информационной культуры человека

- ✓ умение адекватно формулировать свою потребность в информации;
- ✓ эффективно осуществлять поиск нужной информации во всей совокупности информационных ресурсов;
- ✓ перерабатывать информацию и создавать качественно новую;
- ✓ адекватно отбирать и оценивать информацию;
- ✓ способность к информационному общению и компьютерная грамотность

Элементы системы безопасности - знания закономерностей среды и опасных факторов

Цифровая среда — пространство, доступ в которое осуществляется посредством электронных устройств и в котором с помощью программных средств происходит активное взаимодействие людей между собой или людей с электронными сервисами: создание поисковых запросов и получение информации по ним, публикация постов, фото- и видеоматериалов, отправка сообщений.

Особенности цифровой среды

1. В цифровом пространстве отсутствует контакт «лицом к лицу». Замена его взаимодействием цифровых сущностей создаёт иллюзию анонимности, что снижает у некоторых людей степень ответственности за свои поступки и вызывает желание нарушить правила поведения и этические нормы, которые в реальной жизни они, как правило, соблюдают.
2. Иллюзия приватности — необоснованная уверенность пользователя в том, что он полностью контролирует размещённую в цифровом пространстве им самим информацию, включая персональную. Многие беспечно относятся к необходимости защитить свои персональные данные или данные, по которым их можно идентифицировать, а затем получить и другую информацию: узнать адрес, режим жизни, хобби и т. д. Сведениями личного характера могут воспользоваться злоумышленники в корыстных целях.
3. При работе в цифровом пространстве каждый должен помнить о реально существующей угрозе заражения цифровых устройств вредоносными программами, которые могут вывести технику из строя или привести к потере пользователем важных для него данных.
4. В цифровом пространстве присутствуют опасные персоны, противоправную деятельность которых полностью предотвратить невозможно.

Элементы системы безопасности - знания закономерностей среды и опасных факторов

Основные опасности цифровой среды

Риски, присущие цифровому пространству и так или иначе воздействующие на находящегося в этом пространстве человека, можно разделить на две большие группы:

1. Электронные риски, или кибер-риски, угрожающие самому устройству (смартфону, планшету, ноутбуку), установленным на нём программам, банковским счетам, паролям (программы-трояны, вирусы, кибератаки) и т. п.

2. Информационные риски, угрожающие сознанию владельца цифрового устройства (определённый контент может вызвать у человека цифровую зависимость, привести к разрушению его когнитивных способностей и даже произвести прямые атакующие действия на сознание), фальшивые новости (фейкньюс), опасный контент.

современная школа

Практическое задание:
Ответьте на вопросы

Элементы системы безопасности - средства защиты

Фишинг

Фи́шинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям.

Виды фишинга

1. Почтовый фишинг
2. Целевой фишинг
3. Телефонный фишинг
4. CEO-мошенничество
5. Фишинг в социальных сетях
6. Веб – фишинг

современная школа

Элементы системы безопасности - средства защиты

Основные методы защиты информации:

- быть бдительным при разговоре по телефону: если разговор кажется подозрительным, завершить его и перезвонить в организацию по официальным номерам;
- проверять способ связи: мошенники часто используют мессенджеры, тогда как настоящие представители не звонят через WhatsApp или Telegram;
- не сообщать логины и пароли: читать назначение смс-кодов и не делиться ответами на контрольные вопросы;
- проверять адреса электронной почты отправителя, даже если имя совпадает с известным контактом;
- не открывать чаты от неизвестных отправителей;
- относиться с осторожностью к письмам с призывами к действиям или темами о финансах и угрозах;
- не переходить по ссылкам в письмах, особенно если они короткие или используют сокращатели;
- не открывать вложения с подозрительными расширениями (.zip, .js, .exe и т.д.) и документами с макросами;
- не подключать неизвестные внешние носители информации к компьютерам;
- создавать сложные пароли длиной не менее 12 символов с комбинацией букв, цифр и специальных символов. Избегать простых и легко угадываемых паролей;
- не использовать один и тот же пароль для разных учетных записей;
- менять регулярно пароли (каждые 2 месяца), обновлять их при подозрении на утечку;
- активировать на всех доступных сервисах двухфакторную аутентификацию;
- хранить пароли либо на физическом носителе (только в защищенных местах хранения), либо на компьютере (только в зашифрованном виде).

Элементы системы безопасности - умение человека предвидеть, выявлять и правильно оценивать опасные факторы и адекватно реагировать на них

Цифровая зависимость

Зависимость - постоянная навязчивая потребность в совершении каких-либо действий вопреки осознаваемым неблагоприятным последствиям этих действий для своего здоровья (как физического, так и психического), отношений с людьми и других значимых аспектов жизни.

Цифровая зависимость - это неконтролируемое использование электронных устройств, таких как смартфоны, компьютеры и планшеты, которое оказывает негативное влияние на различные аспекты нашей жизни.

современная школа

Элементы системы безопасности - умение человека предвидеть, выявлять и правильно оценивать опасные факторы и адекватно реагировать на них

Цифровая зависимость

Основные признаки цифровой зависимости:

1. Придание сверхзначимости постоянному присутствию и общению в социальных сетях, непрерывному ознакомлению с лентами новостей и т. п.
2. Формирование эмоциональной зависимости, колебания настроения при ограничении возможности присутствия в Интернете.
3. Потребность в увеличении времени присутствия в Интернете и частоты использования разнообразных устройств доступа в цифровую среду.
4. Возникновение «синдрома отмены» — ухудшение самочувствия при отсутствии возможности доступа в цифровую среду.
5. Возникновение нарушений (недоразумений и конфликтов) в общении в обычной жизни.
6. Потеря самоконтроля, возникновение срывов и рецидивов при попытках отрегулировать время присутствия в цифровой среде.

Дополнительные признаки цифровой зависимости:

1. Ухудшение состояния здоровья (набор или потеря веса, мышечные боли и т. д.), психологическая нестабильность (апатия, тревога, депрессия).
2. Нарушение привычного ритма жизни, пренебрежение семейным и дружеским общением, отказ от ранее любимых увлечений.
3. Использование различных ухищрений и обмана с целью получения доступа в Интернет.

Элементы системы безопасности - умение человека предвидеть, выявлять и правильно оценивать опасные факторы и адекватно реагировать на них

Социальные сети

+	-
1. Позволяют поддерживать связь с друзьями и родственниками, даже если они находятся далеко 2. Предоставляют платформу для саморазвития и обучения 3. Играют важную роль в распространении информации и новостей	1. Кибербуллинг 2. Фейковые новости

Кибербуллинг *– это травля, оскорбления или запугивание, происходящие в цифровом пространстве*

Фейковые новости *– ложные или искаженные сведения, которые намеренно распространяются с целью ввести людей в заблуждение*

Спасибо за внимание!

современная школа