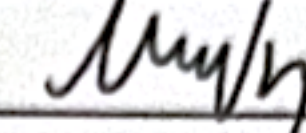


АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО
ОБРАЗОВАНИЯ "ИНСПИРЕЙШН (ВДОХНОВЕНИЕ)"

УТВЕРЖДЕНО

Генеральный директор

АНО ДО "ИНСПИРЕЙШН (ВДОХНОВЕНИЕ)"



/ Б. Д. Миронов

Приказ № 3 от «20» июня 2026 г.



ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА –
ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
«Умный пользователь основы безопасности в цифровом мире.»

Направленность: социально-гуманитарная

Срок реализации программы: 16 ак.ч.

Автор-составитель:
Миронов Борис Дмитриевич

г. Санкт-Петербург– 2026г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА.....	3
1 КОМПЛЕКС ОСНОВНЫХ ХАРАКТЕРИСТИК ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»	3
1.1 Общая характеристика дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	4
1.2 Цели и задачи дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	4
1.3 Планируемые результаты освоения дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	4
2. ДОКУМЕНТЫ, ОПРЕДЕЛЯЮЩИЕ СОДЕРЖАНИЕ И ОРГАНИЗАЦИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»	6
2.1 Учебный план дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	8
2.2 Календарный учебный график дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	8
3 СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»	9
4 ФОРМЫ И МЕТОДЫ КОНТРОЛЯ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»	11
5 ОРГАНИЗАЦИОННО – ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»	11
5.1 Особенности реализации дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	11
5.2 Требования к минимальному материально - техническому обеспечению дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»	12
5.3 Рекомендации к материально-техническим условиям со стороны обучающегося (потребителя образовательной услуги) дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	12
5.4 Кадровое обеспечение реализации дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	13
5.5 Учебно-методическое обеспечение дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	13
5.6 Оценочные материалы дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.».....	13
ПРИЛОЖЕНИЕ 1.....	15
ПРИЛОЖЕНИЕ 2.....	16

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная программа – дополнительная общеразвивающая программа «Умный пользователь основы безопасности в цифровом мире.»- далее «Программа» разработана на основе следующих нормативных правовых документов:

1. Федерального закона Российской Федерации от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации»;
2. Приказ Министерства Просвещения РФ от 27 июля 2022 г. N 629 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам».
3. Постановление Правительства РФ от 11 октября 2023 года №1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»
4. Постановление Главного государственного санитарного врача РФ от 28.09.2020 N 28 "Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно- эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей, и молодежи";

Направленность программы – социально-гуманитарная

Адресат – взрослые от 18 лет, без специального образования

Актуальность программы обусловлена стремительной цифровизацией повседневной жизни и одновременным ростом изощрённости киберугроз: фишинг, мошенничество при онлайн-покупках, утечки персональных данных и кибербуллинг стали распространёнными явлениями, затрагивающими самые разные слои общества. Особенно уязвимыми оказываются дети и подростки — они активно пользуются смартфонами, соцсетями и платёжными сервисами, но зачастую не обладают достаточным опытом, чтобы распознать манипуляции или оценить риски. При этом угрозы всё чаще строятся не на технических уязвимостях, а на эксплуатации человеческого фактора: срочность, обещание выгоды, имитация авторитета — эти приёмы эффективно снижают критичность восприятия. В такой ситуации умение осознанно и безопасно взаимодействовать с цифровой средой превращается в базовый жизненный навык, сопоставимый по значимости с финансовой грамотностью или правилами дорожного движения. Существенный разрыв между скоростью появления новых угроз и темпами формирования соответствующих компетенций у населения делает подобные программы крайне востребованными — они закрывают пробел между формальными знаниями и реальными поведенческими навыками, необходимыми для защиты личной и семейной безопасности.

Новизна программы состоит в её практической и поведенческой направленности: она не ограничивается перечислением правил, а выстраивает целостную модель безопасного цифрового поведения, охватывая все ключевые точки контакта человека с рисками — от распознавания подозрительных писем и создания надёжных паролей до настройки приватности в соцсетях, безопасных онлайн-платежей, грамотного использования мобильных устройств и чётких действий при взломе. Особое внимание уделяется не только «как делать», но и «почему мы часто делаем неправильно»: в содержание органично встроены элементы поведенческой психологии — разбор типичных когнитивных ловушек, из-за которых люди выбирают простые пароли, доверяют срочным сообщениям или бездумно принимают разрешения приложений. Новизну усиливает включение родительского компонента: программа даёт инструменты не только взрослым, но и детям, помогая выстроить единую систему безопасности в семье и преодолеть разрыв в цифровой грамотности между поколениями.

Педагогическая целесообразность программы проявляется в её способности трансформировать абстрактные знания в устойчивые привычки и алгоритмы действий. Программа целенаправленно развивает критическое мышление: учит не принимать информацию на веру, а задавать вопросы о мотивах отправителя, целях сообщения и возможных последствиях.

1 КОМПЛЕКС ОСНОВНЫХ ХАРАКТЕРИСТИК ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»

1.1 Общая характеристика дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Обучение по программе осуществляется с применением исключительно электронного обучения, дистанционных образовательных технологий. Обучение проводится средствами платформы в формате презентаций и онлайн консультаций. Для работы в системе обучающемуся выделяется логин и пароль.

Программа по виду образования – дополнительное

Подвид – дополнительное образование детей и взрослых

Направленность программы – социально-гуманитарная

Форма организации занятий – индивидуально – групповая.

Условия формирования групп: взрослые от 18 лет

Условия набора: принимаются все желающие

Количество обучающихся в группе – 15 человек

Форма организации образовательной деятельности – индивидуальная и (или) групповая.

Продолжительность академического часа составляет 30 минут.

Нормативный срок обучения - 16 ак. часов

Продолжительность обучения – 4 недели

Рекомендованный режим занятий: 2 раза в неделю по 2 академических часов.

Обучающийся вправе распределять нагрузку по своему графику при условии завершения всех модулей/тем/разделов до итоговой аттестации.

Язык реализации: русский.

Итоговый документ об окончании курсов по ДО - сертификат установленного образца.

1.2 Цели и задачи дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Цель программы – сформировать у обучающихся понятия и умения безопасного поведения в цифровой среде, позволяющие распознавать киберугрозы, защищать персональные и финансовые данные, грамотно использовать цифровые сервисы и устройства, а также действовать по чёткому алгоритму при возникновении инцидентов.

Обучающие задачи

- Сформировать систему базовых знаний о типах киберугроз (фишинг, мошенничество, вредоносные приложения, кибербуллинг) и механизмах их реализации, чтобы обучающиеся могли уверенно различать наиболее распространённые схемы обмана и понимать, на каких психологических приёмах они строятся.
- Дать чёткие представления о правилах защиты учётных записей: принципах создания надёжных паролей, целесообразности и рисках использования менеджеров паролей, а также порядке включения и применения двухфакторной аутентификации на разных платформах.
- Обучить практическим приёмам проверки безопасности онлайн-сервисов и платёжных операций — в том числе распознаванию защищённого соединения, анализу репутации сайта, выявлению подозрительных условий сделки и правилам обращения с реквизитами банковской карты.
- Раскрыть риски, связанные с публикацией персональной информации в соцсетях (включая геометки, фото документов, детали распорядка дня), и сформировать понимание того, как настройки приватности позволяют управлять видимостью контента и ограничивать доступ к личным данным.
- Сформировать знания о безопасном использовании мобильных устройств: правилах установки приложений, анализе запрашиваемых разрешений, необходимости резервного копирования и корректного удаления данных при передаче или утилизации устройства.

- Дать алгоритм действий при инцидентах информационной безопасности (взлом аккаунта, подозрительные списания, утечка данных), включая приоритетные шаги по минимизации ущерба и перечень официальных каналов обращения (поддержка сервисов, банки, Роскомнадзор, МВД).
- Обеспечить освоение инструментов и практик цифровой безопасности для родителей и детей: принципов настройки родительского контроля, способов фильтрации контента, типовых тем и формулировок для доверительных разговоров о рисках в интернете и действий при кибербуллинге.

Развивающие задачи

- Развивать способность критически оценивать входящие сообщения, ссылки и предложения в цифровой среде: выделять маркеры подозрительности, сопоставлять факты, проверять достоверность источников и не поддаваться на приёмы социальной инженерии (срочность, обещание выгоды, имитация авторитета).
- Формировать регулятивные умения, необходимые для безопасного цифрового поведения: планировать собственные действия при онлайн-покупках и регистрации на сервисах, контролировать соблюдение правил защиты данных, корректировать поведение при появлении признаков угрозы.
- Развивать способности анализа и интерпретации визуальной и текстовой информации: распознавать поддельные интерфейсы сайтов, выявлять несоответствия в письмах и объявлениях, читать и понимать условия использования сервисов и политики конфиденциальности в адаптированном виде.
- Стимулировать познавательную активность и самостоятельность в освоении новых цифровых инструментов: умение находить официальные инструкции по настройке приватности, включению MFA, обновлению ПО, а также оценивать полезность и безопасность новых приложений и функций.
- Формировать стрессоустойчивость и способность действовать по алгоритму в напряжённых ситуациях (например, при обнаружении подозрительных списаний или травли в сети), снижая эмоциональную реакцию и повышая ориентацию на последовательные, безопасные шаги.
- Развивать рефлексию собственного цифрового поведения: умение анализировать свои привычки (использование паролей, публикация фото, установка приложений), выявлять уязвимые места и осознанно менять поведение для повышения уровня безопасности.

Воспитательные задачи

- Воспитывать ответственное отношение к персональным данным — как к своим, так и к чужим: понимание ценности конфиденциальности, недопустимости распространения чужих фото и сведений без согласия, а также последствий утечки информации для себя и окружающих.
- Формировать культуру безопасного и этичного поведения в онлайн-среде: уважение к границам других пользователей, отказ от участия в травле и распространении фейков, готовность поддержать пострадавшего от кибербуллинга и предложить алгоритм действий.
- Воспитывать осознанность и осторожность при взаимодействии с незнакомыми людьми и предложениями в интернете: привычку не делиться чувствительной информацией, не переходить по сомнительным ссылкам и не принимать поспешных решений под давлением.
- Развивать чувство личной ответственности за безопасность своего цифрового пространства: понимание, что защита аккаунта и устройства — это регулярная практика, а не разовое действие, и что игнорирование базовых правил может привести к реальным финансовым и репутационным потерям.
- Формировать готовность обращаться за помощью при возникновении угроз: преодолевать стеснение и страх, воспринимать обращение в поддержку сервисов, к родителям или в уполномоченные органы как нормальную и необходимую часть безопасного поведения.
- Воспитывать цифровую зрелость и критическое отношение к информации: не принимать сообщения и «новости» на веру, проверять факты, избегать распространения непроверенных данных и осознавать свою роль в формировании безопасной онлайн-среды.

- Способствовать формированию доверительных отношений между детьми и взрослыми по вопросам цифровой безопасности: поощрять открытый диалог о рисках и инцидентах, совместное обсуждение правил и ситуаций, а также взаимную поддержку при освоении новых технологий.

1.3 Планируемые результаты освоения дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Требования к результатам освоения программы определяются ключевыми задачами предметные, личностные и метапредметные результаты освоения курса.

Предметные результаты

- Называет и объясняет основные киберугрозы (фишинг, мошенничество, кибербуллинг, вредоносные приложения) и распознаёт их маркеры в сообщениях, на сайтах, в письмах.
- Применяет на практике правила защиты аккаунтов: создаёт надёжные пароли, понимает смысл и использует двухфакторную аутентификацию.
- Проверяет безопасность онлайн-сервисов и платёжных операций: видит признаки защищённого соединения, анализирует репутацию сайта, не вводит реквизиты карты на подозрительных ресурсах.
- Осознаёт риски публикации личных данных (имя, адрес, фото документов, геолокация) и настраивает приватность в соцсетях.
- Следует правилам безопасного использования устройств: анализирует запрашиваемые приложениями разрешения, делает резервные копии, корректно удаляет данные.
- Знает алгоритм действий при инцидентах (взлом аккаунта, подозрительные списания): что сделать в первую очередь, куда обратиться (поддержка, банк, взрослые).
- Понимает принципы настройки родительского контроля и фильтрации контента, знает, как выстроить доверительный диалог с родителями о рисках в сети.

Метапредметные результаты

- Критически оценивает информацию: выделяет тревожные сигналы, проверяет достоверность источников, не поддаётся на приёмы социальной инженерии (срочность, обещание выгоды).
- Планирует действия перед онлайн-операциями (покупка, регистрация): составляет короткий чек-лист шагов, чтобы действовать осознанно.
- Анализирует цифровые подсказки: «читает» значки безопасности в браузере, понимает смысл всплывающих уведомлений и запросов разрешений.
- Самостоятельно ищет инструкции (например, как включить защиту в сервисе) и пробует разбираться в новых функциях.
- Чётко формулирует проблему (что случилось, когда, что уже сделано) при обращении за помощью — к родителям, в поддержку сервиса.
- Осознаёт последствия своих действий в сети и несёт за них ответственность.
- Вносит коррективы в своё цифровое поведение, если ситуация изменилась (появилась новая угроза, сервис обновил настройки безопасности).

Личностные результаты

- Формирует бережное отношение к личным данным, понимает, что это не просто «строчки в профиле», а информация, требующая защиты.
- Проявляет уважительное поведение в сети: не распространяет слухи, не участвует в травле, умеет поддержать того, кому некомфортно.
- Привыкает делать паузу перед действиями в интернете (особенно если сообщение давит на эмоции), учится не действовать импульсивно.
- Осознаёт ценность безопасного образа жизни в цифровой среде.

- Интериоризирует (принимает как свою норму) правила безопасного поведения в информационно-телекоммуникационной среде — не только знает их, но и руководствуется в повседневной жизни.
- Проявляет готовность обсуждать сложные темы с родителями или другими взрослыми, не боится просить помощи.

2. ДОКУМЕНТЫ, ОПРЕДЕЛЯЮЩИЕ СОДЕРЖАНИЕ И ОРГАНИЗАЦИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»

2.1 Учебный план дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Название темы	Всего	В том числе		Формы контроля
		Теория	Практика	
Входной контроль.	0,5	-	0,5	Анкета
Тема 1. Как не попасться на удочку мошенников: распознаём фишинг и обман.	2	1	1	Задание /Наблюдение
Тема 2. Надежные пароли и двухэтапная проверка: защищаем аккаунты	2	1	1	Задание /Наблюдение
Тема 3. Безопасность в соцсетях: что можно и нельзя публиковать	1,5	1	0,5	Задание /Наблюдение
Промежуточная аттестация	0,5	-	0,5	Устный опрос
Тема 4. Безопасный шопинг и платежи онлайн	2	1	1	Задание /Наблюдение
Тема 5. Дети в интернете: правила для родителей и школьников	2	1	1	Задание /Наблюдение
Тема 6. Мобильные устройства: защищаем смартфон и планшет	2	1	1	Задание /Наблюдение
Тема 7. Что делать, если вас взломали: первые шаги	2	1	1	Задание /Наблюдение
Онлайн консультация	0,5	-	0,5	-
Итоговый контроль	1	-	1	Тест
Итого	16	7	9	

2.2 Календарный учебный график дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

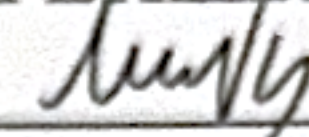
Место проведения	Форма проведения	Наименование тем	Общая трудоемкость, час.	Реализация программы			
				1 неделя	2 неделя	3 неделя	4 неделя
Онлайн -платформа	Анкетирование	Входной контроль	0,5	-/0,5	-	-	-
Онлайн -платформа	Презентации / Прямой эфир	Умный пользователь основы безопасности в цифровом мире.	13,5	2/1,5	2/1,5	2/2	1/1,5
Онлайн -платформа	Прямой эфир	Промежуточная аттестация	0,5	-	-/0,5	-	-
Онлайн -платформа	Прямой эфир	Онлайн консультация	0,5	-	-	-	-/0,5
Онлайн -платформа	Прямой эфир	Итоговый контроль	1	-	-	-	-/1
		Итого:	16	4	4	4	4

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО
ОБРАЗОВАНИЯ "ИНСПИРЕЙШН (ВДОХНОВЕНИЕ)"

УТВЕРЖДЕНО

Генеральный директор

АНО ДО "ИНСПИРЕЙШН (ВДОХНОВЕНИЕ)"



/ Б. Д. Миронов

Приказ № 3 от «20» июня 2026 г.



РАБОЧАЯ ПРОГРАММА

«Умный пользователь основы безопасности в цифровом мире.»

Направленность: социально-гуманитарная

Срок реализации программы: 16 ак.ч.

Автор-составитель:

Миронов Борис Дмитриевич

г. Санкт-Петербург– 2026г.

3 СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»

Программа вариативна, возможны изменения в содержании тем. Педагог может вносить изменения в содержания тем, дополнять практические занятия новыми приемами практического исполнения.

Входной контроль. Анкета (Приложение 1).

Тема 1. Как не попасться на удочку мошенников: распознаём фишинг и обман.

Теория: Признаки фальшивых писем и сайтов. Что делать, если получили подозрительное сообщение. Примеры реальных схем обмана (поддельные лоты, «выигрыш в лотерею»).

Практика: Распишите 2–3 признака, по которым можно заподозрить, что письмо — фишинг.

Что нужно сделать в первую очередь, если ты получил сообщение «Ты выиграл приз, перешли данные карты»?

Приведи один пример распространённой мошеннической схемы (кроме «выигрыша в лотерею») и коротко скажи, почему люди на неё попадают.

Тема 2. Надежные пароли и двухэтапная проверка: защищаем аккаунты

Теория: Как придумывать сложные пароли. Менеджеры паролей: за и против. Включение MFA в соцсетях и почте.

Практика: Распиши два правила, которые помогут придумать надёжный пароль.

Что такое двухфакторная (двухэтапная) аутентификация и зачем она нужна?

В чём плюс и в чём минус использования менеджера паролей? Ответь одним предложением для каждого

Тема 3. Безопасность в соцсетях: что можно и нельзя публиковать

Теория: Настройки приватности в VK. Опасность геометок и фото документов. Как реагировать на травлю и фейки.

Практика: Какие данные лучше вообще не выкладывать в открытый доступ (назови 2 примера)?

Зачем в соцсетях нужны настройки приватности и что с их помощью можно контролировать?

Что стоит сделать, если в соцсети тебя травят или публикуют про тебя фейки? Назови один первый шаг.

Промежуточная аттестация. Прямой эфир

Тема 4. Безопасный шопинг и платежи онлайн

Теория: Как проверить сайт магазина. Оплата картой: что нельзя сообщать. Возврат денег и спорные операции.

Практика: Как быстро проверить, что сайт магазина безопасный (назови один явный признак)?

Какие данные банковской карты нельзя никому сообщать (назови минимум два элемента)?

Что делать, если с карты списали деньги за покупку, которую ты не делал? Назови первый шаг.

Тема 5. Дети в интернете: правила для родителей и школьников

Теория: Родительский контроль и фильтры контента. Обсуждение цифровых рисков с ребёнком. Что делать при кибербуллинге.

Практика: Какой один простой способ можно использовать, чтобы защитить ребёнка в интернете?

Как в двух словах начать разговор с ребёнком про безопасность в сети?

Что нужно сделать в первую очередь, если ребёнка обижают в интернете?

Тема 6. Мобильные устройства: защищаем смартфон и планшет

Теория: Установка приложений: откуда брать, на что смотреть. Разрешения приложений: какие давать, какие отзывать. Резервное копирование и удаление данных.

Практика: Для чего нужен родительский контроль и что он обычно умеет делать (назови одну функцию)?

Какой простой разговор можно провести с ребёнком, чтобы он понимал цифровые риски? Приведи пример одного вопроса, который можно задать.

Если ребёнок столкнулся с кибербуллингом, кому он может рассказать в первую очередь (назови вариант из ближайшего окружения)?

Тема 7. Что делать, если вас взломали: первые шаги

Теория: Смена паролей и уведомление сервисов. Куда жаловаться: Роскомнадзор, МВД, банки.

Практика: Откуда безопаснее всего устанавливать приложения на телефон (назови официальный источник)?

Почему важно внимательно читать разрешения, которые запрашивает приложение, и что делать, если запрос кажется подозрительным?

Зачем нужно резервное копирование данных и как часто его разумно делать? Дай короткий ответ (1–2 предложения).

Онлайн консультация. Прямой эфир.

Итоговый контроль. Тест (Приложение 2)

4 ФОРМЫ И МЕТОДЫ КОНТРОЛЯ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»

В ходе обучения осуществляется несколько видов контроля: входной, текущий, итоговый.

Входной контроль проводится в начале курса для определения уровня знаний, обучающихся на начало обучения по программе. Проводится в форме анкеты. (Приложение 1)

Текущий контроль успеваемости обучающихся представляет систематическую проверку учебных достижений обучающихся, проводимую педагогом в ходе осуществления образовательной деятельности в соответствии с образовательной программой.

Проведение текущего контроля успеваемости направлено на обеспечение выстраивания образовательного процесса максимально эффективным образом для достижения результатов освоения дополнительной программы.

Текущий контроль результатов подготовки осуществляется педагогом учебной группы в ходе изучения каждой темы на каждом занятии, в целях получения информации:

- о выполнении требуемых действий в процессе учебной деятельности;
- о правильности выполнения требуемых действий;
- о соответствии формы действия данному этапу усвоения учебного материала;
- о формировании действия с должной мерой обобщения, освоения (автоматизированности, быстроты выполнения и др.) и т.д.

Промежуточная аттестация проводится в середине курса, в форме устного опроса.

Освоение образовательной программы заканчивается итоговым контролем. (Приложение 2)

Итоговый контроль проводится на платформе в виде тестирования, с присвоением каждому обучающемуся результата «зачет / незачет».

Критерии оценивания итогового контроля:

5 баллов – 13-15 правильно выполненных заданий из 15;

4 балла – 10-12 правильно выполненных задания из 15;

3 балла – 7-9 правильно выполненных задания из 15;

3 балла – 4-6 правильно выполненных задания из 15;

2 балла – 3 и менее правильно выполненных задания из 15;

Итоговый контроль пройден – от 3 до 5 баллов

Итоговый контроль не пройден – 2 балла

5 ОРГАНИЗАЦИОННО – ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ – ДОПОЛНИТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «УМНЫЙ ПОЛЬЗОВАТЕЛЬ ОСНОВЫ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ.»

5.1 Особенности реализации дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

При реализации Программы в учебном процессе используются глобальные и локальные компьютерные сети для обеспечения доступа к информационным образовательным ресурсам и для управления учебным процессом независимо от местонахождения человека.

Занятия построены на следующих принципах обучения:

- интерактивности;
- открытости;
- гибкости;
- адаптивности;
- передаваемости;
- ориентация на потребителя;
- индивидуализации;

При проведении занятия с применением дистанционных образовательных технологий и электронного обучения, в водной части следует обозначить правила работы и взаимодействия (объяснить обучающимся технические особенности работы и правила обмена информацией. В процессе занятия педагогу необходимо четко давать инструкции выполнения заданий.

Виды занятий при организации дистанционного обучения:

- Online - занятие. Занятия являются асинхронными – в этом случае у обучающегося есть возможность найти удобное для себя время, чтобы отработать материал программы обучения. Программа включает в себя теоретические и практические занятия;
- online-занятие (online-консультация);
- фрагменты и материалы образовательных Интернет-ресурсов;
- адресные дистанционные консультации.

Уроки-презентации можно смотреть в любое время и выполнять задания.

В программе учитывается следующее:

- современные теории и технологии в области методики обучения и воспитания
- психолого-физиологические особенности обучающихся;
- потребности обучающихся и социальный заказ общества.

Дистанционная поддержка программы предполагает самостоятельное изучение дополнительных материалов с применением информационно - телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников, а также возможности получения консультаций у преподавателя данного курса.

5.2 Требования к минимальному материально - техническому обеспечению дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Существует определенная материально-техническая база, обеспечивающая реализацию образовательной программы. Для работы в системе обучающемуся выделяется логин и пароль.

Рабочее место обучающегося должно быть оснащено компьютером с подключением к сети Интернет.

Услуга подключения к сети Интернет должна предоставляться в режиме 24 часа в сутки 7 дней в неделю. Подключение к Интернет со скоростью не ниже 512 Кбит/с. Материально-социально-гуманитарная база для реализации программы включает следующие составляющие:

- Ноутбук Lenovo ThinkBook 15-III 205M000HIRU (четырёхъядерный процессор Intel Core i5-1035G1 с частотой 1,0 ГГц – 3,6 ГГц, оперативная память DDR4 объёмом 16384 Мб, SSD 512 Гб) — 1 шт.
- Интерактивная доска Classic Solution Dual Touch V66 — 1 шт.
- Web-камера Logitech WebCam C505e — 1 шт.
- USB-микрофон Behringer C-1U Studio Condenser Microphone — 1 шт.
- Звуковая система Dolby Audio — 1 шт.
- Наушники SVEN AP-930M — 1 шт

5.3 Рекомендации к материально-техническим условиям со стороны обучающегося (потребителя образовательной услуги) дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Рекомендуемая конфигурация компьютера:

- Разрешение экрана от 1280x1024;

- Pentium 4 или более новый процессор с поддержкой SSE2;
- 512 Мб оперативной памяти;
- 200 Мб свободного дискового пространства;
- Современный веб-браузер актуальной версии (Firefox 22, Google Chrome 27, Opera 15, Safari 5, Internet Explorer 8 или более новый).

5.4 Кадровое обеспечение реализации дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Реализация программы осуществляется педагогом дополнительного образования в соответствии с действующим нормативно-правовым документом: Приказу Министерства труда и социальной защиты РФ от 22 сентября 2021 г. № 652н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых».

Требования к образованию и обучению:

Высшее образование или среднее профессиональное образование в рамках укрупненных групп специальностей и направлений подготовки высшего образования и специальностей среднего профессионального образования "Образование и педагогические науки", или высшее образование либо среднее профессиональное образование в рамках иных укрупненных групп специальностей и направлений подготовки высшего образования и специальностей среднего профессионального образования при условии его соответствия дополнительным общеразвивающим программам, дополнительным предпрофессиональным программам, реализуемым организацией, осуществляющей образовательную деятельность, и получение при необходимости после трудоустройства дополнительного профессионального образования педагогической направленности, или успешное прохождение обучающимися промежуточной аттестации не менее чем за два года обучения по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующим направленности дополнительных общеобразовательных программ.

Требования к опыту практической работы:

- Не менее двух лет в должности педагога дополнительного образования, иной должности педагогического работника - для старшего педагога дополнительного образования;
- Не менее двух лет в должности тренера-преподавателя или педагога дополнительного образования соответствующей направленности - для старшего тренера-преподавателя.

Особые условия допуска к работе:

- Отсутствие ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации;
- Прохождение обязательных предварительных и периодических медицинских осмотров.

5.5 Учебно-методическое обеспечение дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Учебно-методическое и информационное обеспечение программы обеспечено электронными учебниками, учебно-методической литературой и материалами по всем учебным темам программы.

Литература:

1. Гафнер, В. В. Опасности социального характера и защита от них : учебное пособие / В. В. Гафнер, С. В. Петров, Л. И. Забара. — Москва : Флинта : Наука, 2012. — 320 с.
2. Солдатова Г. У., Зотова Е. Ю., Лебешева М. И., Шляпников В. Н. Интернет: возможности, компетенции, безопасность. — М.: Генезис, 2021. — 208 с.
3. Айкен М. Дядя из интернета любит меня больше, чем ты. Как защитить ребёнка от опасностей интернета. — М.: Эксмо, 2020. — 510 с.

5.6 Оценочные материалы дополнительной общеобразовательной программы – дополнительной общеразвивающей программы «Умный пользователь основы безопасности в цифровом мире.»

Проведение мониторинга успеваемости обучающихся. Содержание учебных модулей и учебно-методических материалов представлено в учебно-методических ресурсах, размещенных в электронной информационно-образовательной среде

Учебно-методическая литература представлена в виде электронных информационных и образовательных ресурсов в библиотеках и в системе дистанционного обучения.

Оценочные материалы по программе размещены на платформе СДО и включают следующие формы и методы для проведения входного, текущего и итогового контроля.

Анкета

1. Фамилия, имя, отчество (при наличии). Укажите, как к вам можно обращаться в ходе занятий.
2. Ваш возраст или год рождения.
3. Расскажите в 2–3 предложениях, в каких цифровых сервисах вы взаимодействуете чаще всего (соцсети, маркетплейсы, банки, рабочие инструменты и т. п.) и для чего они вам нужны в повседневной жизни.
4. Есть ли среди ваших онлайн-привычек что-то, что вы сами считаете потенциально рискованным (например, «сохраняю пароли в браузере», «перехожу по ссылкам из чатов», «использую один пароль на нескольких сайтах»)? Если да — коротко опишите.
5. Вспомните недавнюю ситуацию, когда в интернете вы почувствовали неуверенность или настороженность (странное письмо, сомнительный сайт, неожиданный запрос данных и т. д.). Что именно вас смутило и как вы поступили?
6. Какие цифровые риски кажутся вам наиболее серьёзными лично для вас — финансовые потери, утечка личных данных, компрометирующие публикации, проблемы на работе из-за цифрового следа и т. п.? Назовите 1–2 пункта и поясните, почему именно они вызывают беспокойство.
7. Какими инструментами защиты вы уже пользуетесь (двухфакторная аутентификация, менеджеры паролей, настройки приватности, родительский контроль для детей и т. д.)? Перечислите те, что применяете регулярно, и коротко отметьте, насколько удобно ими пользоваться.

Итоговый контроль

1. Ты получил письмо: «Ваша учётная запись будет заблокирована! Подтвердите данные по ссылке». Адрес отправителя не похож на официальный. Что лучше сделать?

- А) Перейти по ссылке и ввести данные, чтобы не потерять аккаунт.
- Б) Ответить на письмо и попросить прислать другую ссылку.
- В) Не переходить по ссылке, проверить статус аккаунта через официальное приложение или сайт.
- Г) Переслать письмо другу, чтобы он проверил, безопасно ли это.

Правильный ответ: В.

2. Какие три признака чаще всего указывают на фишинговый сайт? Выбери один вариант, где все пункты верные.

- А) Красивый дизайн, много картинок, есть форма входа.
- Б) В адресной строке нет HTTPS, название домена немного отличается от оригинала, срочный призыв к действию.
- В) Сайт открывается быстро, есть отзывы, есть кнопка «Войти через соцсети».
- Г) На сайте есть политика конфиденциальности, контакты и форма обратной связи.

Правильный ответ: Б.

3. Почему сообщение «Ты выиграл приз, перешли код из СМС» почти всегда обман?

- А) Потому что настоящие призы никогда не требуют код из СМС.
- Б) Потому что организаторы лотерей не используют СМС.
- В) Потому что код из СМС нужен мошенникам, чтобы войти в твой аккаунт или подтвердить платёж от твоего имени.
- Г) Потому что все розыгрыши проходят только на официальных сайтах.

Правильный ответ: В.

4. Какой из паролей самый надёжный?

- А) 123456.
- Б) Masha2010.
- В) Password123.
- Г) T7#mP9xLq2!v.

Правильный ответ: Г.

5. Что такое двухфакторная аутентификация (2FA)?

- А) Это когда нужно придумать два пароля для одного аккаунта.
- Б) Это вход в аккаунт с двух разных устройств одновременно.
- В) Это подтверждение входа вторым способом (например, кодом из СМС или через приложение) после ввода пароля.
- Г) Это когда аккаунт защищён только сложным паролем.

Правильный ответ: В.

6. Ты хочешь купить товар в интернет-магазине. Что обязательно нужно сделать для безопасности?

- А) Ввести все данные карты сразу, чтобы быстрее оформить заказ.
- Б) Проверить наличие HTTPS в адресной строке, отзывы о магазине и не вводить лишние данные.
- В) Оплатить через перевод на карту частному лицу — так дешевле.
- Г) Купить по самой низкой цене, даже если сайт выглядит странно.

Правильный ответ: Б.

7. Какие данные банковской карты нельзя никому сообщать?

- А) Только номер карты.
- Б) Номер карты, CVV-код, срок действия, коды из СМС.
- В) Имя владельца и номер карты.
- Г) Только коды из СМС, остальное можно.

Правильный ответ: Б.

8. В чём риск публикации фото с геолокацией и подписью «Уезжаем в отпуск на неделю!»?

- А) Фото может не понравиться друзьям.
- Б) По геолокации и информации об отсутствии дома злоумышленники могут понять, что квартира пуста.
- В) Соцсеть может заблокировать пост за спам.
- Г) Геометки занимают место в памяти телефона.

Правильный ответ: Б.

9. Откуда безопаснее всего устанавливать приложения?

- А) По ссылкам из чатов и писем.
- Б) Из неофициальных сайтов с «бесплатными версиями».
- В) Из официальных магазинов приложений (Google Play, App Store, RuStore).
- Г) С флешек, которые дают знакомые.

Правильный ответ: В.

10. Зачем важно проверять разрешения приложений (доступ к камере, контактам и т. п.)?

- А) Чтобы приложение работало быстрее.
- Б) Чтобы телефон не разряжался слишком быстро.
- В) Чтобы не дать приложению лишних прав и не допустить утечки личных данных.
- Г) Чтобы в настройках было меньше пунктов.

Правильный ответ: В.

11. Что такое цифровой след?

- А) Следы пальцев на экране смартфона.
- Б) Данные, которые остаются о человеке в интернете (лайки, посты, комментарии, история поиска и т. д.).
- В) Отпечаток SIM-карты в сети оператора.
- Г) История звонков и СМС на телефоне.

Правильный ответ: Б.

12. Ребёнок рассказал, что в чате ему пишут обидные вещи и угрожают. Какой первый шаг должен сделать взрослый?

- А) Сразу заблокировать обидчика и удалить переписку, чтобы ребёнок не расстраивался.
- Б) Успокоить ребёнка, сохранить доказательства (скриншоты) и обсудить дальнейшие шаги.
- В) Написать обидчику и потребовать прекратить.
- Г) Запретить ребёнку пользоваться интернетом.

Правильный ответ: Б.

13. Ты заметил списание с карты, которое не делал. Что сделать в первые минуты?

- А) Ничего не делать, подождать, вдруг это ошибка банка и деньги вернутся.
- Б) Сразу заблокировать карту, сообщить банку, проверить другие операции.
- В) Попробовать самостоятельно отменить операцию в приложении.
- Г) Написать в чат поддержки соцсети и спросить, что делать.

Правильный ответ: Б.

14. Куда обратиться при разных инцидентах? Сопоставь правильно.

С карты списали деньги без твоего согласия.

В соцсети распространяют твои личные фото без разрешения.

Получил подозрительное письмо с вредной ссылкой.

Варианты:

- А) Банк.
- Б) Поддержка соцсети, Роскомнадзор.
- В) Не переходить по ссылке; при необходимости — сообщить в поддержку почтового сервиса.

Правильные пары: 1 — А, 2 — Б, 3 — В.

15. Что из перечисленного помогает снизить риски в интернете?

- А) Использовать один и тот же пароль везде, чтобы не забыть.
 - Б) Переходить по всем ссылкам, если они пришли от «знакомых» контактов.
 - В) Регулярно обновлять приложения, включать 2FA, не делиться кодами из СМС.
 - Г) Хранить все пароли в записках на телефоне.
- Правильный ответ: В.