Министерство образования Владимирской области
Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой»

Кафедра цифрового образования и информационной безопасности

«УТВЕРЖДАЮ»
Проректор
_____
«___» _____ 2025

Дополнительная профессиональная программа

(повышение квалификации)

«Цифровые риски и безопасность современного педагога в Интернет»

Владимир
2025

Организация - разработчик: ГАОУ ДПО ВО «Владимирский институт развития образования имени Л.И. Новиковой»

Разработчик(и) программы:

Дубровина Н.Н., зав.кафедрой цифрового образования и информационной безопасности ГАОУ ДПО ВО ВИРО.

Мишина И.Ю., доцент кафедры цифрового образования и информационной безопасности ГАОУ ДПО ВО ВИРО.

Программа **рекомендована** кафедрой цифрового образования и информационной безопасности ГАОУ ДПО ВО ВИРО к использованию в учебном процессе для повышения квалификации педагогов

Протокол №_4_ от «_4_» _12_ 2025 г. Зав.кафедрой _____/Дубровина Н.Н.

Раздел 1. Характеристика программы

1.1. Цель реализации программы совершенствование компетенции сотрудников образовательных организаций в области цифровых рисков и базовых принципов безопасной работы с ресурсами Интернет.

1.2. Планируемые результаты обучения:

Трудовая функция	Трудовое действие	Знать	Уметь
Общепедагогическая функция. Обучение	Разработка и реализация программы развития образовательной организации в целях создания безопасной и комфортной образовательной среды. Формирование навыков, связанных с информационно-коммуникационными технологиями (далее - ИКТ)	– актуальные задачи в области безопасного использования современных цифровых технологий и Интернет в профессиональной деятельности; – понятие и виды цифровых рисков и базовые правила кибергигиены; – способы обеспечения безопасности парольной аутентификации, правила безопасной работы в WEB, признаки типовых атак социальной инженерии в Интернет; – подходы к минимизации контентных и коммуникативных цифровых рисков.	– оценивать цифровые риски, находить актуальную информацию о наиболее актуальных цифровых рисках; – разрабатывать надежные и удобные в использовании пароли, настраивать многофакторную аутентификацию в социальных сетях и электронной почте; – настраивать параметры безопасности и приватности своего профиля, выявлять типовые атаки социальной инженерии и противодействовать им; – принимать меры по минимизации контентных и коммуникативных цифровых рисков.

1.3. Категория слушателей: все категории педагогов.

1.4. Форма обучения: очная с применением ЭО и ДОТ.

1.5. Срок освоения программы: 48 (час)

Раздел 2. Содержание программы

2.1. Учебно-тематический план

№	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ			Формы контроля
			Лекция,	Интеракти	Дистанцио	

			час	вное (практическое) занятие, час	нные занятия, час	
1.	**Модуль 1. Понятие цифровых рисков и актуальность задачи обеспечения безопасности в глобальной информационной среде**					
1.1	Современная политика РФ в сфере образования. Цифровая трансформация	2			2	Тест
1.2	Актуальность задачи обеспечения безопасности в глобальной информационной среде. Понятие кибергигиены	3			3	Практическая работа
1.3	Существующие практики кибергигиены. Понятия и стандарты	2			2	Тест
1.4	Риски современного цифрового мира	3			3	Практическая работа
2.	**Модуль 2. Деструктивный онлайн-контент. Коммуникационные риски и агрессия в Интернет**					
2.1	Деструктивный онлайн-контент. Жестокий контент в Интернете	4			4	Тест Практическая работа
2.2	Деструктивная онлайн-коммуникация. Агрессия в Интернете	4			4	Тест Практическая работа
3.	**Модуль 3. Вопросы безопасности аутентификации и гигиена использования многоразовых паролей**					
3.1	Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Введение в гигиену паролей	2			2	Практическая работа
3.2	Типовые атаки на пароли	4			4	Практическая работа
3.3	Наиболее распространенные	2			2	Практическая работа

	ошибки использования паролей. Правила (политики) парольной защиты					
3.4	Многофакторная аутентификация. Типы аутентификации в распределённых системах	4			4	Тест Практическая работа
4.	**Модуль 4. Принципы и правила обеспечения безопасности при использовании WEB**					
4.1	Что такое и как устроен WEB. Защита канала, при использовании WEB	4			4	Практическая работа
4.2	Структура и безопасность URL	4			4	Практическая работа
4.3	Конфиденциальность в социальных сетях	4			4	Практическая работа
5.	**Модуль 5. Социотехнические атаки на пользователей социальных сервисов Интернет**					
5.1	«Социальная инженерия» информационно-психологические атаки на современного человека. Психология влияния в цифровой среде	4			4	Практическая работа
5.2	Техники интернет мошенничества	2			2	Практическая работа
	Итоговая аттестация	0				Зачёт
	ИТОГО	48			48	

2.2. Рабочая программа

Модуль 1. Понятие цифровых рисков и актуальность задачи обеспечения безопасности в глобальной информационной среде.

1.1 Современная политика РФ в сфере образования. Цифровая трансформация (дистанционные занятия: лекция - 1 ч., практическое занятие - 1 ч.)

Лекция. Современная политика РФ в сфере образования, цифровая трансформация. Цифровая грамотность преподавателя: первые шаги.

Практическое занятие. Прохождение теста по теме.

1.2 Актуальность задачи обеспечения безопасности в глобальной информационной среде. Понятие кибергигиены (дистанционные занятия: лекция - 2 ч., практическое занятие - 1 ч.)

Лекция. Актуальность задачи обеспечения безопасности в глобальной информационной среде. Информационная культура, ИКТ компетенции и медиаграмотность современного педагога. Цифровая грамотность и цифровая компетентность. Киберпространство. Цифровая или кибергигиена. Примеры типовых правил кибергигиены.

Практическое занятие. Онлайн опрос об опыте столкновения с интернет рисками.

1.3 Существующие практики кибергигиены. Понятия и стандарты (дистанционные занятия: лекция - 1 ч., практическое занятие - 1 ч.)

Лекция. Существующие практики кибергигиены: 12 лучших практик. Задачи и направления кибергигиены на уровне руководства. Задачи и направления кибергигиены на уровне организации. Задачи и направления кибергигиены на персональном уровне. Связь современных понятий безопасности цифрового пространства. Стандарт ISO/IEC 27032:2012.

Практическое занятие. Прохождение теста по теме.

1.4 Риски современного цифрового мира (дистанционные занятия: лекция - 2 ч., практическое занятие - 1 ч.)

Лекция. Контентные риски. Коммуникационные риски. Технические Интернет риски. Риски психофизиологической зависимости от цифровой техники и Интернет.

Практическое занятие. Онлайн семинар - оценка рисков современного цифрового мира для педагога.

Модуль 2. Деструктивный онлайн-контент. Коммуникационные риски и агрессия в Интернет.

2.1 Деструктивный онлайн-контент. Жестокий контент в Интернете (дистанционные занятия: лекция - 2 ч., практическое занятие - 2 ч.)

Лекция. Контентные риски в Интернете. Законодательное регулирование в области контентных рисков. Запрещенная информация Понятие «жестокого контента». Пропаганда экстремизма и терроризма в Интернет. Колумбайн. Движение АУЕ в сети. Пропаганда психотропов в Интернет. Фейки и постправда в современном мире.

Практическое занятие. Прохождение теста по теме, разработка проекта презентации по теме «Контентные риски современного школьника. Профилактика контентных рисков Интернет» для классного часа «Цифровые риски».

2.2 Деструктивная онлайн-коммуникация. Агрессия в Интернете (дистанционные занятия: лекция - 2 ч., практическое занятие - 2 ч.)

Лекция. Киберагрессия: отличие от офлайн-агрессии и механизмы воздействия. Виды киберагрессии. Ролевая структура киберагрессии. Кибербуллинг. Жертвы кибербуллинга. Противодействие киберагрессии и кибербуллингу.

Практическое занятие. Прохождение теста по теме, разработка проекта презентации по теме «Коммуникационные риски современного школьника. Профилактика агрессивного поведения в Интернет» для классного часа «Цифровые риски».

Модуль 3. Вопросы безопасности аутентификации и гигиена использования многоразовых паролей

3.1 Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Введение в гигиену паролей (дистанционные занятия: лекция - 1 ч., практическое занятие - 1 ч.)

Лекция. Управление доступом. Этапы входа в информационную систему. Идентификация. Аутентификация. Авторизация. Аудит. Пароли. Достоинства и недостатки парольных систем аутентификации.

Практическое занятие. Поиск и анализ информации из открытых источников об инцидентах ИБ, связанных с компрометацией паролей пользователей

3.2 Типовые атаки на пароли (дистанционные занятия: лекция - 2 ч., практическое занятие - 2 ч.)

Лекция. Словарная атака или атака перебора по словарю (dictionary attack). Атака по персональному словарю. Полный перебор (метод грубой силы, bruteforce). Перебор в ограниченном диапазоне. Защита от атаки грубой силы. Способы составления надежного пароля. Сбор паролей, хранящихся в общедоступных местах. Режим «инкогнито» браузеров. Перехват пароля в канале связи. Социальная инженерия.

Практическое занятие. Практика разработки надежного и удобного пароля

3.3 Наиболее распространенные ошибки использования паролей. Правила (политики) парольной защиты (дистанционные занятия: лекция - 1 ч., практическое занятие - 1 ч.)

Лекция. Критические ошибки использования паролей. Серьезные ошибки использования паролей. Недочеты и рекомендации при использования паролей. Правила (политики) парольной защиты

Практическое занятие. Разработка правил гигиены паролей

3.4 Многофакторная аутентификация. Типы аутентификации в распределённых системах (дистанционные занятия: лекция - 2 ч., практическое занятие - 2 ч.)

Лекция. Многофакторная аутентификация. Факторы аутентификации. Комбинация факторов аутентификации.

Практическое занятие. Прохождение теста по теме, настройка многофакторной аутентификации в социальных сетях и электронной почте

Модуль 4. Принципы и правила обеспечения безопасности при использовании WEB

4.1 Что такое и как устроен WEB. Защита канала, при использовании WEB (дистанционные занятия: лекция - 2 ч., практическое занятие - 2 ч.)

Лекция. Служба WWW (World Wide Web). WWW и Интернет. Web 1.0, Web 2.0 и Web 3.0. Основные компоненты технологии World Wide Web. Язык HTML (Hyper Text Markup Language). Протокол HyperText Transfer Protocol. Адресация в Интернет и Web. Криптография и защита передачи в Интернет. Защищенный протокол HTTPS (HyperText Transfer Protocol Secure). Отличия HTTPS и HTTP. Организация защищенного обмена данными по протоколу HTTPS. SSL сертификат. Инфраструктура открытых ключей PKI.

Практическая работа. Знакомство с компонентами и принципами работы web.

4.2 Структура и безопасность URL (дистанционные занятия: лекция - 1 ч., практическое занятие - 3 ч.)

Лекция. Основы IP адресации в Интернет. Формат и внешний вид IP-адреса. "Белые" и «серые» IP адреса. DNS (Domain Name System «система доменных имён»). URL адрес. Статические и динамические URL – адреса. Кодировка URL адреса.

Практическая работа. Знакомство и практики работы со службой DNS

4.3 Конфиденциальность в социальных сетях (дистанционные занятия: лекция - 1 ч., практическое занятие - 3 ч.)

Лекция. Понятие «социальная сеть». Современные социальные сети Интернета. Риски социальных сетей интернет. Настройки конфиденциальности (приватности) социальных сетей.

Практическая работа. Настройка приватности в популярных социальных сетях

Модуль 5. Социотехнические атаки на пользователей социальных сервисов Интернет

5.1 «Социальная инженерия» информационно-психологические атаки на современного человека. Психология влияния в цифровой среде (дистанционные занятия: лекция - 2 ч., практическое занятие – 2 ч.)

Лекция. Понятие социальной инженерии. Интернет мошенничество. «Искусство обмана» («The Art of Deception»). Основные этапы социального взлома. «Социальная инженерия» и психология влияния. Принципы и приемы влияния.

Практическая работа. Прохождение игры «Знания» по теме Фишинг (Изучи Интернет - управляй им)

5.2 Техники интернет мошенничества (дистанционные занятия: практическое занятие - 2 ч.)

Практическая работа. Онлайн семинар - анализ «Сказок о безопасности»: Король и фишинг, Волк и семеро козлят (или снова о многофакторной аутентификации), Али-Баба и 40 киберугроз.

Раздел 3. Формы аттестации и оценочные материалы

Промежуточный контроль

Раздел программы: Существующие практики кибергигиены. Понятия и стандарты.
Форма: Тест по учебному модулю 1.
Описание, требования к выполнению: Обучающийся должен выбрать ответы на вопросы теста, тест содержит 12 вопросов разного типа.
Критерии оценивания: оценка «зачтено» ставится при условии, если слушатель дал не менее 75% правильных ответов в рамках теста.
Примеры заданий:
1) О каком определении идёт речь?
_____ - риски, возникающие в процессе использования материалов, содержащих противозаконную, неэтичную и вредоносную информацию - насилие, агрессию, эротику и порнографию, нецензурную лексику, пропаганду суицида, наркотических веществ и т.д.

2)Верно ли утверждение?
Потребительские риски – это возможность повреждения программного обеспечения, информации, нарушение её конфиденциальности или взлома аккаунта, хищения паролей и персональной информации злоумышленниками посредством вредоносного ПО и др. угроз.
Выберите один ответ:
Верно
Неверно
Количество попыток: 3

Раздел программы: Деструктивная онлайн-коммуникация. Агрессия в Интернете.

Форма: Тест по учебному модулю 2
Описание, требования к выполнению: Обучающийся должен выбрать ответы на вопросы теста, тест содержит 12 вопросов разного типа.
Критерии оценивания: оценка «зачтено» ставится при условии, если слушатель дал не менее 75% правильных ответов в рамках теста.
Примеры заданий:
1) Подберите соответствующие пары
Основная его цель – вызвать у оппонента негативные эмоции посредством оскорблений и провокативного поведения.
Разжигание спора, публичные оскорбления и эмоциональный обмен репликами в интернете между участниками в равных позициях.
Негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.
Агрессивные, умышленные, повторяющиеся и продолжительные во времени действия, совершаемые группой лиц или одним лицом с использованием электронных форм контакта в отношении жертвы, которой трудно защитить себя.
Троллинг
Флейминг
Хейтинг
Кибербуллинг

2) Укажите верные ответы (более одного) - Информационно-психологическое воздействие и привлечение людей в террористические группы может осуществляется следующими способами:
через средства массовой информации
через сайты государственных структур
через создание веб-сайтов
через создание групп в социальных сетях

3) Укажите верные ответы (более одного). Чаще всего становятся жертвами вербовки…
подростки и молодые люди, одинокие молодые девушки и женщины, люди, находящиеся в угнетенном состоянии
пожилые люди и люди преклонного возраста
активные пользователи социальных сетей, групп, чатов
молодые люди, регулярно размещающие информацию в социальных сетях
Количество попыток: 3

Раздел программы: Многофакторная аутентификация. Типы аутентификации в распределённых системах
Форма: Тест по учебному модулю 3
Описание, требования к выполнению: Обучающийся должен выбрать ответы на вопросы теста, тест содержит 10 вопросов разного типа.
Критерии оценивания: оценка «зачтено» ставится при условии, если слушатель дал не менее 75% правильных ответов в рамках теста.
Примеры заданий:
1) Дайте определение понятию «логин».
Выберите один ответ:
a. это доступ к информации в нарушение установленных правил, доступ информации со стороны лиц, не имеющих разрешения на доступ к этой информации

b. это имя (идентификатор) учётной записи пользователя в компьютерной системе, а также процедура входа (идентификации и затем аутентификации) пользователя в компьютерную систему, как правило, путём указания имени учётной записи и пароля
c. это механизм безопасности, который управляет процессом взаимодействия пользователей с компьютерными системами и их ресурсами, а также систем между собой
d. это процедура распознавания (поиска) субъекта по его идентификатору e. это доступ к информации в нарушение установленных правил, доступ информации со стороны лиц, не имеющих разрешения на доступ к этой информации

2) Что такое аудит?
Выберите один ответ:
a. это создание идентификатора субъекта (учетной записи пользователя) в системе (или проверка и подтверждение при самостоятельной регистрации)
b. это процесс управления доступом субъектов к ресурсам системы
c. это управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата и т. п.)
d. это процесс контроля (мониторинга) доступа субъектов к ресурсам системы, включающий протоколирование и анализ действий субъектов при их доступе к ресурсам системы (отслеживание действий пользователей и процессов по внесению изменений в систему, сбор этой информации, формирование отчётов и оповещение) в целях обнаружения несанкционированных действий
e. это контроль доступа легальных пользователей к ресурсам системы после успешного прохождения ими аутентификации
f. это управление правами доступа субъекта к ресурсам системы
Количество попыток: 3

Раздел программы: Конфиденциальность в социальных сетях.
Форма: практическая работа понастройке параметров конфиденциальности социальной сети
Описание, требования к выполнению: практическая работа из 3 заданий по анализу и настройке.
Критерии оценивания: оценка «зачтено» ставится тогда, когда обучающийся успешно выполнил от 60% заданий практической работы.
Примеры заданий:
Проанализируйте значения параметров безопасности и конфиденциальности Вашего профиля в одной из социальных сетей.
Опишите:
- какие параметры позволяет Вам настраивать социальная сеть?
- какие параметры Вам кажутся не очень оптимально настроенными с точки зрения безопасности? Почему?
- приведите пример настроек конфиденциальности профиля, оптимального с точки зрения ваших потребностей, открытости и безопасности.
Количество попыток: не ограничено

Раздел программы: «Социальная инженерия» информационно-психологические атаки на современного человека. Психология влияния в цифровой среде.
Форма: практическая работа по прохождение игры «Знания» по теме Фишинг (Изучи Интернет - управляй им)
Описание, требования к выполнению: необходимо зарегистрироваться на игру «Знания» проекта «Изучи Интернет - управляй им», изучить материалы и выполнить задания в разделах «Фишинг», «Общение онлайн», «Сетевое общение».

Критерии оценивания: оценка «зачтено» ставится тогда, когда обучающийся успешно выполнил от 60% заданий практической работы.
Примеры заданий:
Укажите, какие из ссылок являются «хорошими», а какие явно «фишинговыми»:
https://m.vk.com/im?sel=88764568
https://qiwi.com/replenish.action?utm_source=landing_new_v1&utm_medium=qw_site&utm_campaign=landing_person
https://passport.yandex.ru/passport?mode=auth&from=mail&retpath=https%3A%2F%2Fmail.yandex.ru&origin=hostroot_ru_nol_mobile_enter
https://mail.google.com/mail/u/0/#inbox
https://vk.ru/albums714895967
Количество попыток: не ограничено

Итоговая аттестация

Итоговая аттестация слушателей проводится после освоения всех модулей программы в форме зачета по совокупности положительных результатов выполнения практических работ и прохождения промежуточных тестов.
Форма: Зачет по совокупности выполненных практических работ и тестов.
Описание, требования к выполнению: необходимо выполнить все практические работы и пройти все тесты по материалам курса
Критерии оценивания: оценка «зачтено» выставляется при условии, если слушатель успешно выполнил от 60% заданий практических работ и дал не менее 75% правильных ответов в рамках каждого теста.

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы

Нормативные документы:

1. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях по защите информации»;
3. Федеральный закон от с 01.01.2008 г. № 152-ФЗ РФ «О персональных данных»;
4. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию";
5. Федеральный закон от 27.07.2010 г. № 210 «Об организации предоставления государственных и муниципальных услуг»
6. Распоряжение Правительства Российской Федерации от 25.10.2014 г. № 2125-р «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
7. Приказ Минобрнауки России от 1.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Локальные акты

- Положение об итоговой аттестации слушателей по программам повышения квалификации в ГАОУ ДПО ВО ВИРО.
- Положение об организации дополнительного профессионального образования слушателей ГАОУ ДПО ВО ВИРО.

- Положение о применении электронного обучения и дистанционных образовательных технологий при реализации дополнительных профессиональных программ в ГАОУ ДПО ВО ВИРО

Литература

Основные источники:

1. Солдатова Г.У. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. / Г.У. Солдатова, С.В Чигарькова, А. А. Дренёва, С. Н. Илюхина – М.: КогитоЦентр, 2019. – 176 с.
2. Лесконог Н. Ю. Риски интернет-коммуникации детей и молодежи : учебное пособие / под общ. ред. Н. Ю. Лесконог, И. В. Жилавской, Е. В. Бродовской. – Москва :МПГУ, 2019. – 80 с.
3. Безмалый, В. Цифровая гигиена / В. Безмалый. – Москва: Издательские решения, 2018. – 602 с.
4. Безмалый, В. Цифровая гигиена. Том 2 / В. Безмалый. – Москва: Издательские решения, 2018. - 510 с.
5. Троицкая, Е.А. Информационные технологии в учебном процессе. Учеб. Пособие / Е.А. Троицкая, Л.А. Артюшина, Владим. гос. ун-т им. А.Г. и Н.Г. Столетовых.- Владимир: Изд-во ВлГУ, 2020.-143 с.

Дополнительные источники:

1. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2007. — 368 с.: ил.
2. Солдатова, Г., Цифровая грамотность и безопасность в Интернете. Методическое пособие для специалистов основного общего образования / Солдатова Г., Зотова Е., Лебешева М., Шляпников В. — М.: Google, 2013. — 311 с.
3. Митник, К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон: Компания АйТи, 2004. – 360 с.

Интернет-ресурсы

1. Интерактивная образовательная платформа проекта "Изучи Интернет- управляй им" [Электронный ресурс] / Координационный центр RU/РФ. Москва. – URL: https://xn----7sbikand4bbyfwe.xn--p1ai/game_list/ (дата обращения: 20.12.2024).

4.2. Материально-технические условия реализации программы

Технические средства обучения

Реализация программы требует наличия у слушателей и преподавателя персонального компьютера с выходом в Интернет и установленным браузером, пакетом офисных программ.

Чикунова Галина Константиновна

Подписано цифровой подписью: Чикунова Галина Константиновна
Дата: 2026.06.05 11:25:42 +03'00'