ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
курса повышения квалификации педагогов
«Информационная безопасность и кибергигиена в среднем образовании: от теории к практике»

1. Общие положения

Образовательная программа курса повышения квалификации педагогов «Информационная безопасность и кибергигиена в среднем образовании: от теории к практике» разработана в соответствии с «Правилами разработки, согласования и утверждения образовательных программ курсов повышения квалификации педагогов» (Приказ Министра образования и науки РК № 175 от апреля 2020 года), а также с учетом Государственного общеобязательного стандарта образования Республики Казахстан. Стандарт предусматривает формирование у обучающихся навыков безопасного и осознанного использования информационно-коммуникационных технологий, развитие цифровой грамотности и применение компетентностного подхода в образовательных программах.

В соответствии с Законом Республики Казахстан «Об образовании», одним из ключевых направлений является цифровизация образовательной среды и обеспечение ее безопасности. Особое внимание в рамках национальной политики уделяется защите прав участников образовательного процесса в онлайн-среде и предотвращению угроз, связанных с киберрисками.

Мировые тренды подтверждают необходимость формирования цифровых и киберкомпетенций у педагогов. В рекомендациях ОЭСР подчеркивается значимость развития цифровых навыков и устойчивых практик информационной безопасности как необходимого компонента качества образования. ЮНЕСКО, в свою очередь, выделяет приоритеты этичного и инклюзивного использования цифровых технологий, включая вопросы безопасности данных и защиты прав обучающихся в виртуальной среде.

Особое значение в рамках курса уделяется практико-ориентированным подходам к преподаванию. Международный опыт (платформы CYBER.ORG, U.S. Cyber Range, инициативы ENISA) показывает высокую эффективность использования киберполигонов - специализированных виртуальных сред для моделирования угроз, отработки защитных сценариев и проведения соревнований в формате Capture The Flag (CTF). Такие решения позволяют педагогу не просто передавать знания, а формировать у обучающихся реальные навыки работы с киберрисками, развивать критическое мышление, командное взаимодействие и ответственность за цифровую безопасность.

Программа курса направлена на развитие у педагогов понимания современных угроз в цифровой среде, освоение инструментов преподавания кибергигиены и ИБ, а также интеграцию этих тем в учебный процесс. Практические задания, симуляционные упражнения и групповая работа обеспечивают устойчивое применение полученных знаний в педагогической

практике. Итоговая аттестация позволит слушателям продемонстрировать готовность к внедрению цифровой безопасности в образовательную среду и сопровождению обучающихся в условиях возрастающих киберугроз.

2. Глоссарий

Аутентификация - процесс проверки подлинности пользователя или системы с помощью учетных данных (пароля, сертификата, токена и т.п.).

Брутфорс - метод подбора пароля или ключа путем перебора всех возможных комбинаций.

DDoS - распределенная атака отказа в обслуживании, при которой множество компьютеров одновременно отправляют запросы на целевой сервер, перегружая его.

Форензика- процесс сбора, сохранения и анализа цифровых артефактов (логи, файлы, образы дисков) для расследования инцидентов безопасности.

Информационная безопасность - состояние защищенности информационных ресурсов (конфиденциальность, целостность, доступность) от угроз и несанкционированного доступа.

Кибергигиена - набор практик и привычек (надежные пароли, обновления ПО, установка антивирусов), направленных на поддержание безопасного состояния устройств и данных.

Криптография - наука о методах преобразования информации (шифрование/расшифровка, цифровые подписи) для обеспечения ее конфиденциальности и целостности.

Методы пассивной разведки - сбор открытой (публичной) информации об объекте атаки без прямого взаимодействия с ним (OSINT, WHOIS, поиск в социальных сетях).

Методы активной разведки - сканирование и опрос целевых систем (port-scanning, fingerprinting), при которых инициируются запросы к целевому ресурсу для выявления уязвимостей.

Многофакторная аутентификация - схема подтверждения личности, требующая два и более независимых факторов (что-то, что вы знаете; что-то, что у вас есть; и т.п.).

OSINT (Open-Source INTelligence) - сбор и анализ информации из публичных источников (сайты, базы данных, социальные сети).

Пентест - Тестирование на проникновение — имитация атак на систему для выявления и оценки ее уязвимостей перед злоумышленниками.

Песочница - изолированная виртуальная среда, в которой выполняются подозрительные файлы или кейсы атак, исключая риск инфицирования реальной инфраструктуры.

Сниффинг - перехват и анализ сетевого трафика (пакетов), часто с помощью инструментов типа Wireshark.

Социальная инженерия - метод психологического воздействия на человека с целью получения конфиденциальной информации или доступа к

системе.

Фишинг - специально организованная атака, при которой жертве отправляются поддельные сообщения (электронные письма, сайты) для кражи учетных данных.

Шифрование - процесс преобразования открытого текста в зашифрованный (нечитаемый) вид с помощью алгоритма и ключа.

Эксплойт - программный или скриптовый код, использующий конкретную уязвимость системы для выполнения нежелательных действий.

Capture The Flag (CTF) - соревновательный формат обучения, где команды решают практические задачи («флаги») по различным аспектам ИБ (криптография, форензика, уязвимости).

3. Тематика Программы

Программа ориентирована на развитие цифровых компетенций педагогов в условиях роста киберугроз и расширения цифровой образовательной среды. Она направлена на решение актуальной задачи – формирование у педагогов готовности к системному преподаванию тем, связанных с информационной безопасностью и кибергигиеной, на уровне среднего образования. Программа сочетает теоретическую основу с практико-ориентированными подходами, включая моделирование киберугроз, анализ цифровых рисков, обучение через действие в виртуальной среде и применение формата Capture The Flag.

В рамках программы педагоги знакомятся с ключевыми принципами цифровой безопасности, криптографии, OSINT, анализа сетевого трафика и цифровой криминалистики, а также осваивают инструменты преподавания этих тем с учётом возрастных особенностей обучающихся. Особое внимание уделено внедрению педагогических технологий, основанных на реальных кейсах, киберсимуляциях и командной работе.

Анализ образовательных программ, согласованных с Министерством просвещения Республики Казахстан на 2023–2025 годы, показывает наличие курсов, частично пересекающихся с данной тематикой: «Информационная безопасность ребёнка» и «Современные стратегии профилактики буллинга и кибербуллинга: создание безопасной образовательной среды». Однако ни одна из существующих программ не предлагает комплексного и системного подхода к подготовке педагогов по вопросам преподавания основ информационной безопасности и кибергигиены в структуре общего среднего образования.

Предлагаемая программа восполняет этот пробел, сочетая международный опыт (платформы CYBER.ORG, ENISA, U.S. Cyber Range), современные педагогические методы и актуальные требования к цифровой грамотности. Программа направлена на формирование у педагогов профессиональных компетенций, позволяющих не только осознанно использовать технологии, но и обучать школьников устойчивому, безопасному и критическому взаимодействию с цифровой средой.

Таким образом, программа органично дополняет существующую линейку

курсов повышения квалификации и представляет собой значимый вклад в подготовку педагогов к современным вызовам цифровой трансформации образования.

4. Цель, задачи Программы и ожидаемые результаты

Целью Программы является формирование у педагогов цифровых компетенций и практических навыков преподавания основ информационной безопасности и кибергигиены в среднем образовании с использованием современных образовательных технологий, кейсов и симуляционных заданий.

Задачи Программы:

- ознакомить слушателей с основными понятиями, угрозами и принципами информационной безопасности и цифровой гигиены;
- раскрыть специфику преподавания основ ИБ и кибергигиены обучающимся с учётом возрастных особенностей и уровня цифровой зрелости;
- развить у педагогов навыки анализа цифровых угроз, работы с OSINT-инструментами, криптографией, лог-анализом и средствами мониторинга сетевого трафика;
- продемонстрировать возможности использования виртуальных учебных сред (киберполигонов) и формата Capture The Flag (CTF) в образовательной практике;
- обучить методам разработки уроков и заданий, направленных на формирование критического мышления и устойчивых моделей цифрового поведения у обучающихся;
- обеспечить методическую поддержку по интеграции тематики ИБ в учебный процесс, включая индивидуальные, групповые и проектные форматы работы.

Ожидаемые результаты:

По завершении курса слушатели будут:

- знают современные угрозы информационной безопасности, принципы кибергигиены и нормативные основы цифровой безопасности в образовании;
- умеют объяснять обучающимся ключевые понятия ИБ, использовать кейсы и практические ситуации для формирования цифровой грамотности;
- применяют методы анализа цифровых рисков, распознавания угроз и безопасного поведения в сети;
- разрабатывают уроки и задания с использованием инструментов моделирования киберугроз, анализа логов, криптографии и форензики;
- используют формат CTF, киберсимуляции и игровые механики для вовлечения обучающихся в освоение основ ИБ;
- интегрируют цифровые навыки безопасности в учебный процесс с опорой на компетентностный подход и формирование функциональной грамотности.

5. Структура и содержание Программы

Программа курса включает четыре модуля, направленные на формирование и развитие профессиональных компетенций педагогов в области преподавания информационной безопасности и кибергигиены в условиях цифровизации образования.

Каждый модуль охватывает ключевые аспекты цифровой безопасности — от понимания современных угроз до использования практических инструментов, таких как OSINT, криптография, тестирование на проникновение и работа с логами. Особое внимание уделено методике преподавания этих тем школьникам, развитию навыков критического мышления, а также внедрению форматов командной работы и симуляционных упражнений, таких как Capture The Flag (CTF).

Программа завершается итоговой аттестацией, которая включает выполнение проектной практической работы или мини-CTF с защитой, а также письменное тестирование для оценки степени усвоения теоретического материала и готовности к самостоятельной реализации программы ИБ в учебной практике.

Учебно-тематический план теории и практики курса

№	Тематика занятий	Теоретические занятия	Практические занятия	Всего
1	**Модуль 1. Основы информационной безопасности и цифровой гигиены**			**20 ч.**
1.1	Введение в информационную безопасность и кибергигиену	1	3	4
1.2	Основные цифровые угрозы и инциденты	1	3	4
1.3	Принципы безопасного поведения в сети	1	3	4
1.4	Защита персональных данных и цифровая этика	1	3	4
1.5	Цифровая идентичность и управление репутацией	1	3	4
2	**Модуль 2. Методы угроз и педагогические подходы к обучению ИБ**			**18 ч.**
2.1	Методы социальной инженерии и защита от фишинга	1	3	4
2.2	Аутентификация, пароли и многофакторная защита	1	3	4
2.3	Кибергигиена в практике педагога	1	3	4
2.4	Преподавание тем цифровой безопасности в школьной программе	2	4	6
3	**Модуль 3. Инструменты и технологии информационной безопасности**			**18 ч.**
3.1	Основы работы в OS Linux и командной строке	1	3	4
3.2	Пассивная и активная разведка (OSINT, Nmap и др.)	1	3	4
3.3	Основы криптографии: шифрование, цифровые подписи	1	3	4

3.4	Анализ логов и сетевого трафика	2	4	6
4	**Модуль 4. Инцидент-менеджмент и командная практика**			**20 ч.**
4.1	Методы тестирования на проникновение	1	3	4
4.2	Форензика и анализ цифровых артефактов	1	3	4
4.3	Безопасность веб-приложений и OWASP Top 10	1	3	4
4.4	Методика проведения Capture The Flag и командная работа	1	3	4
4.5	Сценарии реагирования на инциденты и планирование защиты	1	3	4
	Итоговая аттестация			
1	Итоговая проектная работа / мини-CTF / защита кейса		3	3
2	Итоговое тестирование		1	1
	ИТОГО	**30**	**50**	**80 ч.**

Примечание: 1 академический час – 45 минут

Краткое описание содержания модулей и взаимосвязь ожидаемых результатов с целью и задачами Программы

Модуль 1. Основы информационной безопасности и цифровой гигиены

Модуль направлен на формирование у педагогов базовых знаний об информационной безопасности и цифровой гигиене как неотъемлемых компонентах современного образовательного процесса. Основной акцент сделан на осознание актуальности цифровых рисков, развитие критического отношения к цифровой среде и понимание роли педагога в формировании безопасного поведения обучающихся в сети.

В ходе изучения модуля слушатели познакомятся с ключевыми понятиями: информационная безопасность, кибергигиена, цифровые угрозы, приватность, фишинг, социальная инженерия и др. Особое внимание уделено вопросам защиты персональных данных, основам правовой и цифровой этики, а также требованиям к поведению в онлайн-среде, отраженным в нормативных документах и международных рекомендациях.

Каждая тема сопровождается практическими заданиями, направленными на освоение базовых действий: распознавание фишинговых атак, настройка параметров приватности, создание безопасных паролей и внедрение принципов цифровой гигиены в повседневную школьную практику. Практические упражнения моделируют типовые ситуации, с которыми могут столкнуться обучающиеся, и дают педагогам готовые методические решения для профилактики цифровых рисков.

Модуль обеспечивает связь с целью и задачами Программы, поскольку закладывает фундаментальные представления об информационной безопасности

как педагогической задаче. Ожидаемым результатом является готовность педагога формировать у обучающихся культуру безопасного поведения в цифровой среде и интегрировать темы ИБ в общешкольные мероприятия и учебные занятия.

Модуль 2. Методы угроз и педагогические подходы к обучению ИБ

Модуль направлен на развитие у педагогов понимания механизмов распространённых киберугроз и освоение методических подходов к преподаванию тематики цифровой безопасности обучающимся. В центре внимания — социальная инженерия, фишинг, пароли и аутентификация, а также инструменты и стратегии формирования цифровой устойчивости у школьников.

Слушатели познакомятся с принципами работы манипулятивных техник в цифровой среде (фишинг, подмена адресов, обман доверия), узнают, как грамотно объяснить обучающимся эти механизмы и обучить их выявлению подобных угроз. Также будет рассмотрена система многофакторной аутентификации и построения надёжной системы цифровой идентификации, что составляет основу грамотного поведения в цифровой среде.

Особое внимание уделяется роли педагога как медиатора между цифровым пространством и учениками. В рамках модуля предлагаются примеры уроков, внеурочных мероприятий и ситуационных кейсов, направленных на формирование устойчивых поведенческих стратегий у обучающихся. Педагоги также проанализируют риски чрезмерного контроля, этические аспекты и необходимость соблюдения баланса между цифровой защитой и доверием.

Практическая часть модуля включает разработку элементов учебных занятий: блоков объяснения, обсуждений и упражнений для формирования навыков цифровой гигиены у школьников. Кроме того, слушатели отработают навыки адаптации материалов под возрастные особенности обучающихся и составят методическую карту урока по теме ИБ.

Таким образом, модуль способствует достижению задач Программы в части подготовки педагогов к осознанному и методически выверенному включению тем информационной безопасности в образовательный процесс. Ожидаемым результатом является готовность педагога применять понятные, этичные и эффективные подходы к обучению цифровой безопасности в разных возрастных группах.

Модуль 3. Инструменты и технологии информационной безопасности

Модуль ориентирован на освоение педагогами базовых технических инструментов и практик, используемых в сфере информационной безопасности. Он призван развить у слушателей прикладные навыки, позволяющие не только понимать цифровые угрозы, но и демонстрировать обучающимся, как технически реализуются механизмы защиты, мониторинга и анализа инцидентов в цифровой среде.

В рамках модуля рассматриваются инструменты командной строки в среде Linux, пассивная и активная разведка с помощью OSINT-платформ и утилит, таких как Nmap, а также основы криптографии — от простых алгоритмов шифрования до понимания принципов цифровой подписи. Значительное внимание уделяется анализу логов, мониторингу сетевого трафика и выявлению подозрительной активности — как базовому элементу цифровой осведомленности.

Практическая часть построена на выполнении заданий, приближенных к реальным сценариям: анализ следов сетевой активности, поиск открытых данных в интернете, дешифровка кодов и моделирование инцидентов. Слушатели пошагово осваивают рабочие процессы, с которыми могут столкнуться как в рамках обучающих кейсов, так и при организации учебных проектов с обучающимися.

Модуль обеспечивает реализацию задач Программы, направленных на освоение инструментов и развитие технологических компетенций педагога в области цифровой безопасности. Ожидаемый результат — способность самостоятельно применять базовые технологии информационной безопасности в образовательной деятельности, демонстрировать их обучающимся в доступной форме и использовать в проектной и исследовательской работе.

Модуль 4. Инцидент-менеджмент и командная практика

Модуль направлен на развитие у педагогов навыков управления цифровыми инцидентами и проведение командных форматов обучения на основе практических сценариев. В центре внимания — концепции пентестинга, цифровой форензики, уязвимостей веб-приложений, а также методика организации учебных Capture The Flag (CTF) соревнований как формы активного освоения цифровой безопасности.

Слушатели познакомятся с этапами тестирования на проникновение, включая выявление уязвимостей, анализ системной безопасности и составление отчетов об инцидентах. Отдельный блок посвящен цифровой криминалистике — методам восстановления и анализа цифровых артефактов, необходимых для понимания природы инцидентов и выстраивания логики расследования.

Будут рассмотрены принципы безопасности веб-приложений, включая OWASP Top 10 — наиболее распространённые типы уязвимостей, которые важно уметь распознавать и объяснять обучающимся. Кроме того, участники курса освоят методику построения командной работы через формат CTF — симуляционных заданий, направленных на поиск и устранение угроз, работу с шифрами, анализ уязвимостей и совместное принятие решений.

Практическая часть включает подготовку и проведение мини-CTF по шаблону, адаптированному для школьной аудитории, а также моделирование кейсов по цифровым инцидентам. Участники курса разработают сценарии упражнений для включения в учебную деятельность с обучающимися.

Модуль способствует достижению задач Программы, направленных на

интеграцию командных форматов и проектного подхода в преподавание цифровой безопасности. Ожидаемый результат — готовность педагога организовать обучение в интерактивной, исследовательской форме, а также реагировать на инциденты в школьной цифровой среде и вовлекать обучающихся в решение практических задач в формате цифровой симуляции.

Итоговое оценивание

Итоговое оценивание предназначено для комплексной проверки уровня освоения учебного материала, сформированности практических навыков и готовности слушателей применять полученные знания в профессиональной деятельности.

Оценивание включает два компонента:

Проектная работа / мини-CTF / защита кейса – слушатели выполняют индивидуальное или групповое практическое задание, отражающее ключевые элементы курса. Это может быть разработка урока с элементами цифровой безопасности, создание сценария симуляции киберинцидента или участие в учебном мини-CTF с последующим разбором решений. Данный компонент позволяет оценить способность применять полученные знания в условиях, приближенных к реальной педагогической практике.

Итоговое тестирование – представляет собой набор вопросов, охватывающих теоретические аспекты курса: базовые понятия информационной безопасности, принципы кибергигиены, методы защиты, инструменты анализа и подходы к обучению цифровой безопасности. Тестирование позволяет объективно зафиксировать степень усвоения ключевых понятий и логики программы.

Итоговое оценивание обеспечивает обратную связь, выявляет уровень сформированности компетенций и позволяет слушателям отрефлексировать собственную образовательную траекторию. Результаты оценки служат основой для выдачи сертификата о прохождении курса повышения квалификации.

6. Организация учебного процесса

Курс повышения квалификации педагогов реализуется в дистанционном формате, что обеспечивает его доступность, гибкость и возможность совмещения обучения с профессиональной деятельностью. Продолжительность курса составляет 80 академических часов, каждый из которых включает в себя комплекс учебных элементов, направленных на освоение теоретических основ и практическое применение изученного материала в педагогической практике.

Обучение проходит на платформе app.interactiverange.com, где слушателям нужно зарегистрироваться и создать личный кабинет. Через него предоставляется доступ ко всем курсам повышения квалификации педагогов.

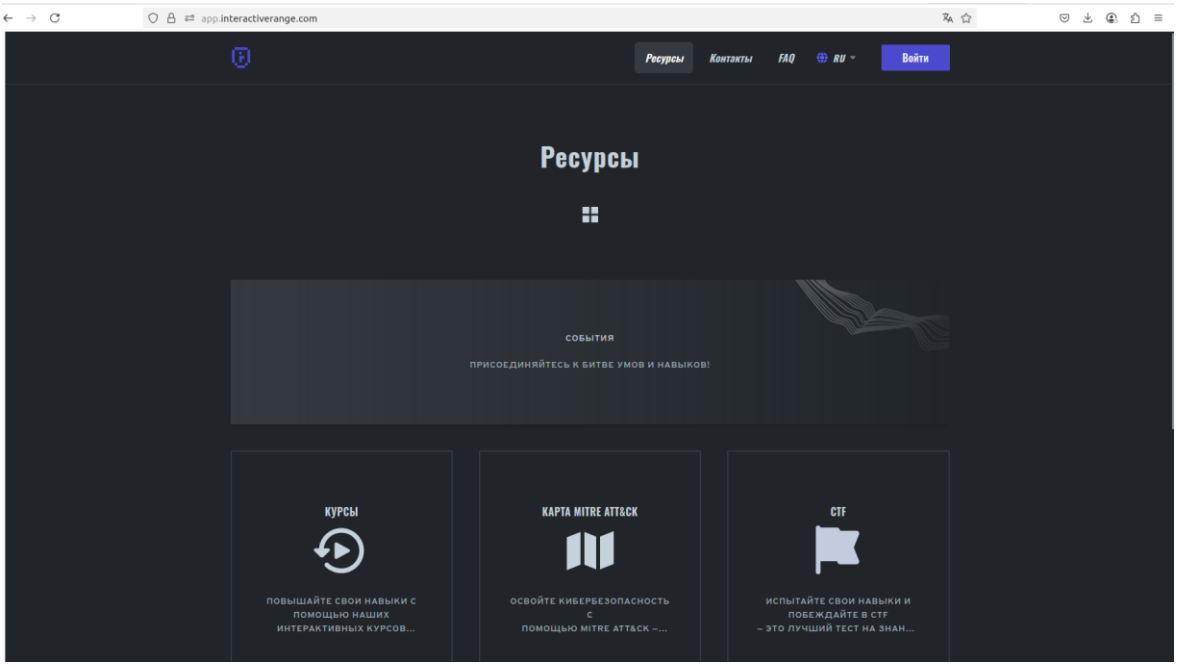

Рис. 1. Главная страница киберполигон Interactive Range

После регистрации пользователи переходят в курсы, где представлены доступные программы повышения квалификации. В каталоге слушатели могут ознакомиться и выбрать необходимый курс для обучения.

Обучение на платформе позволяет слушателям изучать материалы и выполнять задания в удобное время. В процессе обучения слушатели проходят последовательные этапы: изучение теоретических материалов, просмотр видеоуроков, выполнение интерактивных заданий, прохождение лабораторных работ на базе киберполигона, а также ознакомление с инструкциями и прохождение итогового тестирования.

Данный формат обучения обеспечивает гибкость, доступность и возможность планирования темпа обучения, позволяя слушателям осваивать материал и внедрять новые методики в свою профессиональную деятельность.

7. Учебно-методическое обеспечение Программы

Учебно-методическое обеспечение Программы представляет собой целостную дидактическую систему, ориентированную на освоение теоретических основ, формирование прикладных навыков и развитие методических умений педагогов в области информационной безопасности и кибергигиены.

Программа реализуется с опорой на комбинацию теоретических материалов, интерактивных заданий, симуляционных упражнений и практико-ориентированных кейсов, направленных на закрепление ключевых понятий курса. Каждая учебная тема сопровождается:

- доступным теоретическим блоком (в виде текстов, презентаций, видеоуроков), содержащим основные понятия, принципы, примеры угроз и алгоритмы действий;

- заданиями на понимание и применение (разбор ситуаций, работа с цифровыми инструментами, анализ инцидентов);

- практическими задачами в симуляционной среде (например, киберполигон, формат Capture The Flag), позволяющими выработать навыки решения задач в условиях, приближённых к реальным;

- рефлексивными вопросами и чек-листами самооценки, которые способствуют осмыслению личной траектории освоения содержания курса и формированию метапредметных умений.

Ключевой методической особенностью является интеграция задания и критерия оценки: к каждому практическому заданию прилагается четкий набор индикаторов успешного выполнения, по которым педагог может как провести самодиагностику, так и подготовить аналогичные критерии для обучающихся в своей педагогической практике.

Для углубления освоения материала предусмотрены:

- разноуровневые задания (базовые, продвинутые, исследовательские);

- сценарии уроков и внеурочных мероприятий с методическими рекомендациями;

- шаблоны заданий и кейсов, адаптируемые под возрастную специфику обучающихся;

- рекомендации по формирующему и итоговому оцениванию в школьной практике.

Таким образом, учебно-методическое обеспечение курса направлено не только на освоение содержания, но и на формирование готовности к методически грамотному преподаванию тематики ИБ в условиях цифровой школы. Оно поддерживает развитие у педагогов как предметной, так и методической компетентности, а также обеспечивает условия для устойчивого внедрения полученных знаний в учебную и воспитательную деятельность.

8. Оценивание результатов обучения

Оценивание направлено на объективную и прозрачную оценку знаний и навыков, приобретенных слушателями в ходе обучения. 100-балльная система позволяет учитывать как теоретические знания, так и практические умения. Для успешного завершения курса и получения сертификата необходимо набрать не менее 50 баллов.

Оценивание включает тесты, интерактивные задания (вопросы с выбором ответа, задания на соединение, перемещение, ситуационные кейсы), практическую и самостоятельную работу. Итоговое тестирование охватывает все модули курса и оценивается по 100-балльной системе.

Шкала оценивания:

90-100 баллов: высокий уровень владения материалом, готовность к внедрению новых методик.

75-89 баллов: уверенное владение материалом, способность применять знания на практике.

60-74 балла: достаточный уровень знаний, требующий дополнительной проработки отдельных тем.

50-59 баллов: минимально необходимый уровень, требуется дополнительное изучение.

Менее 50 баллов: недостаточный уровень, необходимо повторное прохождение курса.

Слушателям, успешно прошедшим итоговое оценивание в соответствии с образовательной программой курса повышения квалификации, ТОО «CyberLabs» выдает сертификат по теме курса повышения квалификации с указанием темы, объема часов и даты выдачи, а также приложение к сертификату. Сертификат имеет QR-код для проверки подлинности.

Слушатели, не прошедшие итоговое оценивание, имеют возможность на повторное оценивание знаний не более трех раз в год.

9. Посткурсовое сопровождение

Посткурсовое сопровождение курса направлено на поддержку педагогов в процессе внедрения изученных методик преподавания.

ТОО «CyberLabs» в течение одного календарного года после завершения курса оказывает педагогам методическую и консультативную помощь, способствуя успешному применению полученных знаний в образовательной практике. Для этого предусмотрены следующие форматы посткурсового сопровождения:

1. Методическая поддержка через платформу

– Педагоги сохраняют доступ к учебным материалам курса (видеоуроки, презентации, методические рекомендации) для повторного изучения.

2. Персональные онлайн-консультации по запросу

– Слушатели могут подать запрос на консультацию через специальную форму, прикрепленную к курсу.

– Сотрудник ТОО «CyberLabs» в течение 5 рабочих дней готовит ответ и направляет его на электронную почту педагога, при необходимости проводят предварительную беседу для уточнения деталей запроса.

3. Сетевое взаимодействие в профессиональном сообществе

– Педагогам предлагается участие в онлайн-форумах, чатах или профессиональных сообществах для обмена опытом, обсуждения кейсов и получения поддержки от коллег.

4. Мониторинг внедрения изученных методик

– Проведение анкетирования педагогов для оценки эффективности образовательной программы и уровня применения изученных методик в практике.

10. Список основной и дополнительной литературы

Основная литература

1. Закон Республики Казахстан от 27 июля 2007 года № 319-III «Об образовании» (с дополнениями от 5 марта 2022 года) – Статья 7. Информационное обеспечение органов управления системой образования. URL: https://adilet.zan.kz/rus/docs/Z070000319_
2. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации». URL: https://adilet.zan.kz/rus/docs/Z1500000418
3. Закон Республики Казахстан от 05.07.2004 г. «О связи». URL: https://adilet.zan.kz/rus/docs/Z040000567_
4. Послание Президента Республики Казахстан народу Казахстана «Новое политическое направление государства со Стратегией Казахстан-2050», 14 декабря 2012 года. URL: https://adilet.zan.kz/rus/docs/K1200002050
5. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 — 2029 годы». URL: https://adilet.zan.kz/rus/docs/P2300000269
6. Постановление Правительства Республики Казахстан от 20.12.2016 г. № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». URL: https://adilet.zan.kz/rus/docs/P1600000832
7. Постановление Правительства Республики Казахстан от 09.08.2018 г. № 488 «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности». URL: https://adilet.zan.kz/rus/docs/P1800000488
8. Национальный проект «Качественное образование «Образованная нация» на 2021–2025 годы. URL: https://adilet.zan.kz/rus/docs/P2100000726
9. Концепция развития науки Республики Казахстан на 2022–2026 годы : постановление Правительства Республики Казахстан от 25 мая 2022 года № 376. URL: https://adilet.zan.kz/rus/docs/V2200029767
10. Белоус А.И., Солодуха В.А., Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. Москва: ТЕХНОСФЕРА, 2021. – 482 с. ISBN 978-5-94836-612-8
11. Вангородский, С. Н., Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019. — 238, [1] с. — (Российский учебник). ISBN 978-5-358-22190-1
12. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. А.И. Белоус
13. Kitchenham B., Charters S. Guidelines for performing systematic literature reviews in software engineering. – 2007. URL: https://www.elsevier.com/data/promis_misc/525444systematicreviewsguide.pdf

Дополнительная литература

1. Yusif S., Hafeez-Baig A. Cybersecurity Policy Compliance in Higher

Education: A Theoretical Framework // Journal of Applied Security Research. – 2023. – Т. 18. – № 2. – С. 267–288. URL: https://doi.org/10.1080/19361610.2021.1989271
2. Harris M. A., Martin R. Promoting cybersecurity compliance // Cybersecurity education for awareness and compliance. – IGI Global, 2019. – С. 54–71. URL: https://www.igi-global.com/chapter/promoting-cybersecurity-compliance/225917
3. Vasileiou I., Furnell S. (ed.). Cybersecurity education for awareness and compliance. – IGI Global, 2019. – 305 с.
4. Sadiku M. N. O., Chukwu U. C., Sadiku J. O. Cybersecurity for Education // European Journal Of Innovation in Nonformal Education. – 2023. – Т. 3. – № 6. – С. 182–188. URL: http://www.inovatus.es/index.php/ejine/article/view/1828/1831