

Министерство науки и высшего образования Республики Казахстан
НАО «Павлодарский педагогический университет имени Әлкей Марғұлан»
Институт дополнительного образования

УТВЕРЖДАЮ

Член правления –

проректор по академическим вопросам



О.К. Андрющенко
«20» / 05 2025 г.

Образовательная программа
курса повышения квалификации учителей
"Кибербезопасность и защита информации в образовательной среде"

РАЗРАБОТАНА:

PhD, ассоциированный профессор

Абыкенова Д.Б.
«19» / 05 2025 г.

к.п.н., профессор

Жилбаев Ж.О.
«19» / 05 2025 г.

к.п.н., профессор

Асаинова А.Ж.
«19» / 05 2025 г.

СОГЛАСОВАНО:

Директор ИДО:

Р. Жаева
«15» / 05 2025 г.

Павлодар 2025 г.

I. Общие положения

Современная образовательная среда все активнее интегрирует цифровые технологии, что требует от учителей не только владения инструментами дистанционного обучения и цифровыми ресурсами, но и осведомленности в области кибербезопасности. Учителя играют ключевую роль в формировании цифровой культуры обучающихся, обеспечении безопасного использования информационных технологий и защите персональных данных в образовательном процессе.

Программа повышения квалификации учителей разработана в рамках грантового финансирования проекта ИРН AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента» и составлена на основе следующих документов:

1. Закон Республики Казахстан от 27 июля 2007 года № 319-III. «Об образовании» с изменениями и дополнениями на 15 апреля 2025 год.
2. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации» с изменениями и дополнениями на 08 января 2025 года.
3. Закон Республики Казахстан от 1 июля 2024 года № 103-VIII ЗРК «О науке и технологической политике».
4. Правила профилактики травли (буллинга) ребенка, Приказ Министра просвещения Республики Казахстан от 21 декабря 2022 года № 506.
5. Закон Республики Казахстан от 3 мая 2022 года № 118-VII ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам защиты прав ребенка, образования, информации и информатизации».
6. Послание Президента Республики Казахстан народу Казахстана «Новое политическое направление государства со Стратегией Казахстан-2050», 14 декабря 2012 года. Приоритеты нашей работы в сфере образования: «Мы должны интенсивно внедрять инновационные методы, решения и инструменты в отечественную систему образования, включая дистанционное обучение и обучение в режиме онлайн, доступные для всех желающих».
7. Национальный план развития Республики Казахстан до 2029 года. Этот документ был утверждён Указом Президента Республики Казахстан от 24 апреля 2024 года № 611.
8. Государственные общеобязательные стандарты дошкольного воспитания и обучения, начального, основного среднего и общего среднего, технического и профессионального, послесреднего образования, Приказ Министра просвещения Республики Казахстан от 3 августа 2022 года № 348, с изменениями и дополнениями на 15 апреля 2025 года.
9. Типовые квалификационные характеристики должностей педагогических работников и приравненных к ним лиц. Приказ МОН РК от 13 июля 2009 года № 338 - в редакции приказа Министра образования и науки РК

от 30.04.2020 № 169, с внесенными изменениями и дополнениями Приказом Министра просвещения Республики Казахстан от 30 апреля 2025 года № 98.

10. Концепция кибербезопасности ("Киберщит Казахстана"). Утверждена Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями на: 17.03.2023).

11. Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы, утвержденная Постановлением Правительства Республики Казахстан от 28 марта 2023 года № 269.

12. Профессиональный стандарт "Педагог", утвержденный приказом и.о. Министра просвещения Республики Казахстан от 15 декабря 2022 года № 500.

13. Стандарт кибербезопасности СТ РК IEC/PAS 62443-3-2017 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления» (IEC PAS 62443-3:2008 Security for industrial process measurement and control - Network and system security, IDT).

14. Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности, Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89, с изменениями на 20 марта 2025 года.

15. Постановление Правительства Республики Казахстан от 13 мая 2024 года № 372, О внесении изменений и дополнений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности".

Образовательная программа курса повышения квалификации "Кибербезопасность и защита информации в образовательной среде" предназначена для учителей организаций среднего образования (далее Слушатели). Она направлена на развитие компетенций Слушателей в вопросах профилактики киберугроз среди учащихся. В ходе курса Слушатели ознакомятся с основами кибербезопасности, принципами безопасной работы в цифровой образовательной среде, методами защиты персональных данных и стратегиями формирования цифровой грамотности у школьников и студентов.

Сегодня учителям школ необходимо не только осваивать современные образовательные технологии, но и уметь идентифицировать потенциальные риски цифровой среды, предотвращать утечки данных и обучать учащихся безопасному поведению в интернете. Особое внимание в курсе уделяется методическим аспектам преподавания основ кибербезопасности, организации работы с родителями и учащимися по вопросам цифровой гигиены, а также интеграции принципов кибербезопасности в образовательный процесс.

Кибербезопасность в образовании охватывает широкий спектр вопросов: от технических аспектов защиты данных до формирования цифровой культуры и ответственного поведения в сети. Важной задачей курса является развитие у учителей компетенций в области цифровой гигиены, навыков работы с персональными данными, анализа рисков и использования защитных инструментов, а также понимания правовых основ информационной безопасности в образовательных учреждениях.

Курс ориентирован на учителей общеобразовательных школ, но также может быть полезен для преподавателей колледжей и вузов, методистов и администраторов образовательных учреждений. По завершении программы слушатели смогут эффективно применять полученные знания в профессиональной деятельности, разрабатывать методические рекомендации по кибербезопасности для обучающихся и коллег, родителей, а также повышать цифровую безопасность образовательной сред.

Уровень образования: организации среднего образования.

Категория слушателей: учителя организаций среднего образования.

Количество часов: 80 часов.

Язык обучения: русский, казахский.

II. Глоссарий

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

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

Безопасность информационной технологии - защищенность технологического процесса переработки информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

Защита информации от несанкционированного доступа - деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

Злоумышленник - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Кибербуллинг – это травля с использованием цифровых технологий. Кибербуллинг может происходить в социальных сетях, мессенджерах, на игровых платформах и в мобильных телефонах. Это целенаправленная модель поведения, которая ставит своей задачей запугать, разозлить или опозорить того, кто стал объектом травли.

Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные

нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка.

Конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Казахстан.

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Казахстан, или по договору.

Парадигма образовательная – это совокупность теоретических и методических предпосылок, определяющих конкретные действия педагога в различных видах образовательной деятельности, предпосылок, которыми он руководствуется в качестве образца действия.

Парадигма педагогическая – система научно-педагогических взглядов, представляющая собой совокупность теоретических положений, методологических оснований, понятий и ценностных критериев педагогической деятельности.

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Казахстан внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.

Пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею.

Пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими.

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц.

Система информационной безопасности – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности Банка.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Скам – это мошенничество в сети Интернет.

Смишинг – вид мошенничества, целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения. Смишинг-сообщение обычно имеет схожий внешний вид сообщения от банка,

государственного учреждения, оператора электросвязи, известного магазина, а также о внезапном выигрыше в лотерею или акции и т.д.

Угроза – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного (неумышленного) нарушения режима функционирования объекта и нарушения свойств защищаемой информации или других ресурсов объекта.

Угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации.

Фишинг – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.).

Цифровая гигиена – это свод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет. Относится к сфере знаний о цифровой безопасности.

III. Тематика Программы

Степень новизны программы «Кибербезопасность образовательной среды и защита информации» заключается в комплексном подходе к обучению учителей практическим знаниям и навыкам обеспечения цифровой безопасности в образовательном процессе. В отличие от существующих курсов по цифровой грамотности, данная программа направлена не только на развитие индивидуальных компетенций учителей в области кибербезопасности, но и на формирование их готовности к преподаванию основ цифровой безопасности школьникам.

Научные исследования и практика показывают, что уровень цифровой безопасности образовательных учреждений во многом зависит от уровня подготовки учителей. Данная программа предлагает научно-обоснованные методы обучения учителей предметников, классных руководителей, методистов и администраторов образовательных организаций основам защиты информации, цифровой этики и формирования культуры безопасного поведения в сети у учащихся.

Программа охватывает широкий спектр вопросов: от нормативно-правового регулирования кибербезопасности в образовании до методик преподавания основ цифровой гигиены и защиты данных. В курсе используются современные методы адаптации образовательных программ к требованиям цифровой безопасности, методики защиты информации, технологии анализа и предотвращения киберугроз, а также стратегии эффективного обучения учащихся и их родителей принципам кибербезопасности.

Таким образом, программа не только восполняет существующий пробел в подготовке учителей по вопросам кибербезопасности, но и способствует повышению общего уровня цифровой культуры в образовательной среде.

IV. Цель, задачи и ожидаемые результаты Программы

Цель программы – подготовить педагогические кадры к эффективному обеспечению кибербезопасности в образовательной среде, формированию цифровой культуры и защите информации.

Программа направлена на развитие профессиональных компетенций учителей в области цифровой безопасности, обучение практическим навыкам защиты данных и информационных систем, а также на формирование у них методик преподавания основ кибербезопасности, учитывающих возрастные особенности и потребности учащихся.

Особое внимание уделяется разработке и реализации образовательных программ по цифровой гигиене, профилактике интернет-угроз, а также обучению педагогов стратегиям защиты данных, цифровой этики и правовым аспектам кибербезопасности в образовательных учреждениях.

Задачи курса:

1. Ознакомить Слушателей с основами кибербезопасности, актуальными угрозами и успешными примерами их предотвращения в образовательной среде.

2. Обучить терминологии и ключевым концепциям информационной безопасности, цифровой гигиены и защиты персональных данных в образовательных учреждениях.

3. Изучить методы формирования у учащихся и педагогов цифровой культуры, безопасного поведения в интернете и навыков противодействия киберугрозам.

4. Ознакомить с современными технологиями защиты данных, инструментами шифрования, управления доступом и безопасного использования облачных сервисов.

5. Рассмотреть правовые и этические аспекты кибербезопасности, включая законодательство в сфере защиты персональных данных и авторского права.

6. Обучить Слушателей методикам проведения уроков по кибербезопасности с учетом возрастных и психологических особенностей учащихся.

7. Разработать рекомендации по интеграции принципов кибербезопасности в образовательный процесс, включая адаптацию учебных материалов и организацию безопасной цифровой образовательной среды.

По завершении программы участники смогут:

- Эффективно организовывать образовательный процесс с учетом принципов кибербезопасности, обеспечивая защиту персональных данных и цифровой информации в образовательной среде.

- Применять современные технологии и методики защиты информации в образовательных учреждениях, включая средства аутентификации, шифрования и контроля доступа.

- Разрабатывать и адаптировать учебные материалы по кибербезопасности, учитывая возрастные и когнитивные особенности учащихся.

- Формировать у учеников цифровую грамотность, культуру ответственного поведения в интернете и навыки противодействия киберугрозам.

- Взаимодействовать с коллегами и техническими специалистами для создания безопасной цифровой образовательной среды, а также консультировать учеников и их родителей по вопросам информационной безопасности.

Требования к результатам освоения курса

- Понимание: Слушатели должны демонстрировать глубокое понимание принципов кибербезопасности, основных угроз и рисков в образовательной среде, а также осознавать важность защиты персональных данных и цифровой информации.

- Способность: Способность разрабатывать и адаптировать программы повышения цифровой грамотности, применять методы защиты информации и обеспечивать безопасную работу в цифровой образовательной среде.

- Навыки командной работы: Умение эффективно взаимодействовать с коллегами, IT-специалистами, администрацией образовательных организаций, а также обучающимися и их родителями для обеспечения комплексной защиты информации.

- Использование цифровых технологий: Владение современными инструментами и программными средствами для защиты данных, обеспечения кибербезопасности образовательных платформ и предотвращения киберугроз.

- Оценка и обратная связь: Умение проводить аудит информационной безопасности образовательного учреждения, выявлять уязвимости и разрабатывать рекомендации по их устранению, а также предоставлять конструктивную обратную связь по вопросам цифровой безопасности.

- Исследовательские навыки: Способность анализировать современные тенденции в области кибербезопасности, изучать новые подходы и методики защиты данных, а также проводить собственные исследования в данной области.

- Адаптация к контексту: Гибкость и готовность адаптировать меры кибербезопасности в соответствии с изменяющимися условиями цифровой образовательной среды, законодательными требованиями и техническими возможностями образовательного учреждения.

- Профессиональное развитие: Стремление к постоянному повышению квалификации, освоению новых технологий и методик в области кибербезопасности, активное участие в профессиональных сообществах и конференциях.

- Демонстрация эффективности: Способность разрабатывать и внедрять эффективные стратегии обеспечения кибербезопасности, анализировать

результаты и повышать уровень цифровой безопасности образовательного учреждения.

V. Структура и содержание Программы

Структура программы (в 80 академических часах)

№	Тема	Лекция Кол-во часов	Практические занятия Кол-во часов	Самостоятельная работа Кол-во часов	Всего
Модуль 1. Основы кибербезопасности в образовании					
1.1	Введение в кибербезопасность: ключевые термины, угрозы и современные вызовы. Обзор нормативно-правовых актов в области защиты информации в образовательных учреждениях.	1	2	3	12
1.2	Основные аспекты информационной безопасности в школах и вузах. Роль учителя в формировании цифровой грамотности и культуры безопасного поведения в сети.	1	2	3	
Модуль 2. Киберугрозы и методы их предотвращения					
2.1	Виды киберугроз: фишинг, вредоносное ПО, утечка данных, социальная инженерия и др. Методы защиты	1	2	3	12

	персональных данных учащихся и педагогов.				
2.2	Управление рисками в образовательной среде: анализ и предотвращение атак. Практические кейсы и разбор реальных инцидентов кибератак на образовательные учреждения	1	2	3	
Модуль 3. Защита данных и цифровая гигиена					
3.1	Основные принципы защиты персональной и корпоративной информации. Политики безопасности образовательного учреждения: разработка и внедрение.	1	2	2	10
3.2	Настройка безопасного интернет-доступа в школах и вузах. Основы цифровой гигиены: безопасное использование устройств и облачных сервисов	1	2	2	
Модуль 4. Информационная безопасность учащихся и педагогов					
4.1	Работа с паролями и учетными записями: многофакторная аутентификация и шифрование. Противодействие буллингу и онлайн-угрозам среди учащихся.	1	2	3	12
4.2	Безопасность в социальных сетях и мессенджерах: защита личных данных.	1	2	3	

	Организация работы с родителями по вопросам интернет-безопасности детей				
Модуль 5. Организация безопасного образовательного процесса					
5.1	Основы защиты образовательных платформ и цифровых ресурсов. Работа с безопасными облачными сервисами и системами управления обучением (LMS).	1	2	3	12
5.2	Интерактивные методы обучения основам кибербезопасности для школьников. Проведение уроков, тренингов и практических занятий по кибербезопасности	1	2	3	
Модуль 6. Реагирование на инциденты и кризисное управление					
6.1	План действий в случае кибератаки или утечки данных. Роль администратора и учителя в устранении последствий инцидента.	1	2	2	10
6.2	Взаимодействие с правоохранительными органами и ИТ-специалистами при угрозах. Разбор реальных кейсов кибератак в образовательной среде	1	2	2	
Модуль 7. Будущее кибербезопасности и развитие компетенций					
7.1	Современные тренды в кибербезопасности и цифровых технологиях. Обучение педагогов и	1	2	3	12

	учащихся основам этичного хакерства и безопасного программирования.				
7.2	Возможности для профессионального развития в области кибербезопасности. Разработка персонального плана действий по повышению цифровой безопасности в образовательной среде	1	2	3	
	Всего	14	28	38	80

Содержание программы

Модуль 1. Основы кибербезопасности в образовании

Введение в кибербезопасность: ключевые термины, угрозы и современные вызовы. Обзор нормативно-правовых актов в области защиты информации в образовательных учреждениях. Основные аспекты информационной безопасности в школах и вузах. Роль учителя в формировании цифровой грамотности и культуры безопасного поведения в сети.

Модуль 2. Киберугрозы и методы их предотвращения

Виды киберугроз: фишинг, вредоносное ПО, утечка данных, социальная инженерия и др. Методы защиты персональных данных учащихся и педагогов. Управление рисками в образовательной среде: анализ и предотвращение атак. Практические кейсы и разбор реальных инцидентов кибератак на образовательные учреждения.

Модуль 3. Защита данных и цифровая гигиена

Основные принципы защиты персональной и корпоративной информации. Политики безопасности образовательного учреждения: разработка и внедрение. Настройка безопасного интернет-доступа в школах и вузах. Основы цифровой гигиены: безопасное использование устройств и облачных сервисов.

Модуль 4. Информационная безопасность учащихся и педагогов

Работа с паролями и учетными записями (тіркелгі): многофакторная аутентификация и шифрование. Противодействие буллингу и онлайн-угрозам среди учащихся. Безопасность в социальных сетях и мессенджерах: защита

личных данных. Организация работы с родителями по вопросам интернет-безопасности детей.

Модуль 5. Организация безопасного образовательного процесса

Основы защиты образовательных платформ и цифровых ресурсов. Работа с безопасными облачными сервисами и системами управления обучением (LMS). Интерактивные методы обучения основам кибербезопасности для школьников. Проведение уроков, тренингов и практических занятий по кибербезопасности.

Модуль 6. Реагирование на инциденты и кризисное управление

План действий в случае кибератаки или утечки данных. Роль администратора и учителя в устранении последствий инцидента. Взаимодействие с правоохранительными органами и ИТ-специалистами при угрозах. Разбор реальных кейсов кибератак в образовательной среде.

Модуль 7. Будущее кибербезопасности и развитие компетенций

Современные тренды в кибербезопасности и цифровых технологиях. Обучение педагогов и учащихся основам этичного хакерства и безопасного программирования. Возможности для профессионального развития в области кибербезопасности. Разработка персонального плана действий по повышению цифровой безопасности в образовательной среде.

Ожидаемые результаты:

По окончании курса участники смогут:

Эффективно защищать данные учащихся и педагогов от киберугроз.

Разрабатывать и внедрять политики информационной безопасности в образовательных учреждениях.

Преподавать основы кибербезопасности школьникам и студентам.

Реагировать на киберинциденты и минимизировать их последствия.

Взаимодействовать с родителями и коллегами для формирования безопасной цифровой среды.

VI. Организация учебного процесса

Единицей учебного процесса является урок. Объяснение учебного материала будет проводиться с учетом адаптации к курсу с учетом универсального подхода - демонстрация, видео, иллюстрация, консультация. Курс будет разбит на части и организован в течении нескольких недель, объемом - 80 часов.

К особенностям организации учебного процесса относятся организационные формы, методы и приемы, применяемые при изучении активных методов обучения и цифровых технологий. Учебный процесс будет

реализован с активным вовлечением слушателей в групповые формы обучения, обучения с помощью кейсов и проблемных ситуаций, оценки и обратной связи.

Текущий контроль будет организован с помощью наблюдения за ходом выполненных заданий, самостоятельной реализации. Все итоговые выполненные задания в виде разработок уроков по кибербезопасности и проекта для индивидуальной работы со школьниками должны быть загружены на сайт проекта <https://cyberacademy.ppu.edu.kz/>. Задания имеют адаптированный характер по содержанию и оформлению. Тематический контроль будет произведен по завершению определенного модуля. Итоговый контроль осуществляется по завершению всего курса и загрузки материала на сайт проекта.

VII. Учебно-методическое обеспечение

При организации курса дополнительно будут предоставлены.

Учебные материалы: Готовые учебные материалы, учебные презентации, разработанные для использования в курсе.

Онлайн-ресурсы: условно бесплатный доступ к электронным ресурсам, включая веб-сайты, онлайн-курсы и образовательные платформы для поддержки обучения и работы с цифровыми технологиями.

Интерактивные инструменты: условно бесплатный доступ к приложениям для создания интерактивных учебных материалов, веб-конференций, тестирования и других онлайн-активностей.

Образовательные технологии: Информация и ресурсы для обучения преподавателей использованию образовательных технологий, включая Learning Management Systems (LMS).

Методические материалы: инструкции по созданию уроков, раздаточного материала.

Примеры лучших практик: Информация об интерактивных методах обучения и психолого-педагогических подходов в обучении кибербезопасности детей.

VIII. Оценивание результатов обучения

По завершению курса Слушатели проведут собственные уроки по кибербезопасности в классах, где преподают. Учебные материалы будут загружены на сайт <https://cyberacademy.ppu.edu.kz/> в свободном доступе.

Ожидаемые результаты: требования к результатам освоения программы (сформированность общекультурных и профессиональных компетенций).

Критерии оценки уровня освоения дисциплины

Оценка «зачтено» выставляется Слушателям:

- которые продемонстрировали свои знания основного материала курса программы в объеме, необходимом для дальнейшего обучения и будущей работы по специальности.
- за выполненные программы задания.

- которые обладают необходимыми знаниями, имеют допустимые неточности при устных ответах или письменном выполнении задач.
- которые показали большую часть прочитанного материала и также осознанное усвоение и исправление ошибок, допущенные после пояснений преподавателя.

Оценка «не зачтено»

- присваивается Слушателю, показавшему существенные пробелы в знании основного материала, допустившему принципиальные ошибки при выполнении заданий, предусмотренных программой; в то же время Слушатель показывает, что большую часть прочитанного материала он не знает, не может решать практические задачи и не может ответить на дополнительные вопросы.

Промежуточный контроль осуществляется в ходе практических занятий в виде интерактивного обсуждения вопросов и фиксирования выполнения заданий в рамках самостоятельной работы слушателей (СРС), максимальное количество баллов за промежуточный контроль – 60 баллов.

Итоговый контроль осуществляется в виде максимального количества баллов за промежуточный контроль – 40 баллов. Программа курса считается пройденной, если участник набирает не менее 50 баллов из ста.

По окончании курсов участники должны

Знать:

- Основные принципы, цели и нормативные требования кибербезопасности в образовательной среде.
- Современные угрозы информационной безопасности в школе: фишинг, утечки данных, социальная инженерия, вредоносное ПО.
- Методологию организации безопасной цифровой среды в школе, включая защиту персональных данных учащихся и педагогов.
- Принципы цифровой гигиены и информационной безопасности для педагогов, учеников и родителей.
- Основы киберэтики, правовые аспекты защиты информации и персональных данных в образовании.
- Способы адаптации материалов по кибербезопасности для разных возрастных групп учащихся.

Уметь:

- Адаптировать учебные материалы и методы обучения кибербезопасности для учащихся разного возраста и уровня цифровой грамотности.
- Применять цифровые технологии и интерактивные инструменты для создания доступной, безопасной и мотивирующей учебной среды.
- Развивать навыки командной работы, взаимодействовать с коллегами, педагогами-ассистентами и ИТ-специалистами для обеспечения эффективного обучения кибербезопасности.
- Оценивать уровень цифровой безопасности учащихся, проводить диагностику цифровых рисков и разрабатывать индивидуальные рекомендации.

– Разрабатывать и адаптировать проектные задания по кибербезопасности, включая практические кейсы, сценарии киберинцидентов и задания по цифровой гигиене.

По окончании курса участники будут оснащены комплексным пониманием кибербезопасности в образовательной среде и специфическими навыками, необходимыми для эффективного обеспечения цифровой безопасности учащихся и педагогов. Они смогут внедрять безопасные цифровые практики, адаптировать учебные материалы по кибербезопасности и формировать устойчивую культуру информационной безопасности в школе.

IX. Посткурсовое сопровождение

Посткурсовое сопровождение включает:

- Менторство и поддержка для участников в процессе реализации проектов.
- Вебинары и семинары с экспертами в области кибербезопасности образовательной среды.
- Групповые дискуссии и форумы для обмена опытом и ресурсами.
- Оценка участников через проекты, самооценку и учебные портфолио.

Эта программа позволит Слушателям уверенно внедрять знания и умения области кибербезопасности образовательной среды, повышая качество образования.

X. Список основной и дополнительной литературы

Основная литература:

1. Закон Республики Казахстан от 27 июля 2007 года № 319-III. «Об образовании» с изменениями и дополнениями на 15 апреля 2025 год.
2. Закон Республики Казахстан от 24.11.2015 г. «Об информатизации» с изменениями и дополнениями на 08 января 2025 года.
3. Закон Республики Казахстан от 1 июля 2024 года № 103-VIII ЗРК «О науке и технологической политике».
4. Правила профилактики травли (буллинга) ребенка, Приказ Министра просвещения Республики Казахстан от 21 декабря 2022 года № 506.
5. Закон Республики Казахстан от 3 мая 2022 года № 118-VII ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам защиты прав ребенка, образования, информации и информатизации».
6. Послание Президента Республики Казахстан народу Казахстана «Новое политическое направление государства со Стратегией Казахстан-2050», 14 декабря 2012 года. Приоритеты нашей работы в сфере образования: «Мы должны интенсивно внедрять инновационные методы, решения и инструменты в отечественную систему образования, включая дистанционное обучение и обучение в режиме онлайн, доступные для всех желающих.

7. Национальный план развития Республики Казахстан до 2029 года. Этот документ был утверждён Указом Президента Республики Казахстан от 24 апреля 2024 года № 611.

8. Государственные общеобязательные стандарты дошкольного воспитания и обучения, начального, основного среднего и общего среднего, технического и профессионального, послесреднего образования, Приказ Министра просвещения Республики Казахстан от 3 августа 2022 года № 348, с изменениями и дополнениями на 15 апреля 2025 года.

9. Типовые квалификационные характеристики должностей педагогических работников и приравненных к ним лиц. Приказ МОН РК от 13 июля 2009 года № 338 - в редакции приказа Министра образования и науки РК от 30.04.2020 № 169, с внесенными изменениями и дополнениями Приказом Министра просвещения Республики Казахстан от 30 апреля 2025 года № 98.

10. Концепция кибербезопасности ("Киберщит Казахстана"). Утверждена Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями на: 17.03.2023).

11. Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы, утвержденная Постановлением Правительства Республики Казахстан от 28 марта 2023 года № 269.

12. Профессиональный стандарт "Педагог", утвержденный приказом и.о. Министра просвещения Республики Казахстан от 15 декабря 2022 года № 500.

13. Стандарт кибербезопасности СТ РК IEC/PAS 62443-3-2017 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления» (IEC PAS 62443-3:2008 Security for industrial process measurement and control - Network and system security, IDT).

14. Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности, Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89, с изменениями на 20 марта 2025 года.

15. Постановление Правительства Республики Казахстан от 13 мая 2024 года № 372, О внесении изменений и дополнений в постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 "Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности".

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> (на англ.).
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> (на англ.).
 3. Vasileiou I., Furnell S. (ed.). Cybersecurity education for awareness and compliance. – IGI Global, 2019. – 305 с. (на англ.).
 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> (на англ.).
 5. Kitchenham B., Charters S. Guidelines for performing systematic literature reviews in software engineering. – 2007. URL: https://www.elsevier.com/data/promis_misc/525444systematicreviewsguide.pdf (на англ.).
 6. Belastock E. Our Biggest Nightmare Is Here //Education Next. – 2022. – Т. 22. – №. 2. URL: <https://go.gale.com/ps/> (на англ.).
 7. Torres M., Mullins A., Thompson N. Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector // ACIS 2022 Proceedings. 96. – 2022. – С. 1-10. URL: <https://aisel.aisnet.org/acis2022/96/> (на англ.).
 8. Richardson M. D. et al. Planning for Cyber Security in Schools: The Human Factor //Educational Planning. – 2020. – Т. 27. – №. 2. – С. 23-39. URL: <https://eric.ed.gov/?id=EJ1252710> (на англ.).
 9. Ulven J. B., Wangen G. A systematic review of cybersecurity risks in higher education //Future Internet. – 2021. – Т. 13. – №. 2. – С. 1-40. URL: <https://doi.org/10.3390/fi13020039> (на англ.).
 10. White T. About the K12 Security information exchange: Annual report. – 2022. – 30 с. URL: <https://info.identityautomation.com/hubfs/PDFs/StateofK12Cybersecurity2022.pdf> (на англ.).
 11. Diana I., Ismail I. A., Zairul M. Cyber Risk among High School Students: A Thematic Review //Malaysian Journal of Social Sciences and Humanities (MJSSH). – 2023. – Т. 8. – №. 4. – С. 1-19. URL: <https://doi.org/10.47405/mjssh.v8i4.2251> (на англ.).
 12. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832. URL: <https://adilet.zan.kz/rus/docs/P1600000832>.