НАО «ТОРАЙГЫРОВ УНИВЕРСИТЕТ»

ПРОЕКТ

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
курсов повышения квалификации
«Основы кибербезопасности и защиты данных»

Всего часов: 80 часов

Категория слушателей: педагоги дошкольного воспитания и обучения, начального, основного среднего и общего среднего, технического и профессионального, послесреднего образования

В том числе по формам обучения:

- Лекции: 22
- Практические занятия: 40
- Самостоятельная работа: 18
- Посткурсовая поддержка: 8

Форма аттестации:

- Защита самостоятельной работы: 6

Павлодар

2025

Образовательная программа составлена на основании:

- Приказ Министра просвещения Республики Казахстан от 3 августа 2022 года № 348 «Об утверждении государственных общеобязательных стандартов дошкольного воспитания и обучения, начального, основного среднего и общего среднего, технического и профессионального, послесреднего образования» (с изменениями от 2 мая 2025 года)
- Приказ Министра образования и науки Республики Казахстан от 3 апреля 2013 года № 115 «Об утверждении типовых учебных программ по общеобразовательным предметам, курсам по выбору и факультативам для общеобразовательных организаций»

1. Общие положения

Образовательная программа курсов повышения квалификации «Основы кибербезопасности и защиты данных» разработана ассоциированным профессором, доктором философии (PhD) Потапенко Александрой Олеговной.

Образовательная программа курсов повышения квалификации «Основы кибербезопасности и защиты данных» направлена на помощь в успешном освоении основ кибербезопасности и защиты данных, чтобы они могли передавать эти знания своим ученикам, студентам и коллегам.

Актуальность. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» утверждает единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, предусматривает внедрение систем антивирусной защиты, управления доступом и обучения сотрудников основам кибергигиены.

Согласно Постановлению Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана») существующая казахстанская модель школьного, средне-специального, высшего и послевузовского образования в области ИКТ, включая специализацию в сфере информационной безопасности, требует постоянного и тщательного анализа со стороны всех заинтересованных лиц (включая Министерство образования и науки Республики Казахстан, высшие учебные заведения и потенциальных работодателей) на предмет соответствия современным потребностям общества и тенденциям обеспечения безопасного развития информационных технологий в виду динамического развития данной области.

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. подчеркивает необходимость формирования цифровой грамотности и основ кибербезопасности.

Согласно Приказа Министра образования и науки Республики Казахстан от 17 октября 2018 года № 576 «О внесении изменений в приказ Министра образования и науки Республики Казахстан от 3 апреля 2013 года № 115 «Об утверждении типовых учебных программ по общеобразовательным предметам, курсам по выбору и факультативам для общеобразовательных организаций» в предмет «Информатика» внесены разделы посвящённые кибербезопасности.

Курс разработан специально для слушателей без технического образования и опыта в IT. Он знакомит с базовыми понятиями кибербезопасности, основными интернет-угрозами, простыми инструментами и практическими шагами по защите личных данных, устройств и аккаунтов.

Программа делает упор на реальные примеры из жизни, простые объяснения и практические занятия, которые помогут слушателям не только понять, но и самостоятельно применять полученные знания: как защитить себя и

свою семью в интернете, как распознать мошеннические схемы, как безопасно использовать компьютер, смартфон, интернет-сервисы и облачные платформы.

Обучение проводится с использованием доступных форматов — лекций, практических упражнений, ролевых заданий и самостоятельной работы. По окончании курса слушатели смогут уверенно ориентироваться в базовых вопросах цифровой безопасности и передавать эти навыки своим ученикам, коллегам и близким.

2. Глоссарий

Кибербезопасность Защита компьютеров, телефонов, сетей и данных от взломов, вирусов и мошенников.

Вирус Программа, которая сама распространяется и вредит компьютеру или телефону.

Антивирус Программа, которая помогает находить и удалять вирусы.

Фишинг Мошенничество, когда под видом настоящих писем или сообщений (например, от банка) мошенники пытаются выманить ваши пароли или деньги.

Пароль Секретное слово или набор символов для входа в аккаунт или устройство.

Двухфакторная аутентификация Дополнительная защита, когда кроме пароля нужно подтвердить вход (например, по коду из СМС).

Резервное копирование (бэкап) Создание копии данных, чтобы их можно было восстановить, если что-то случится.

Wi-Fi Беспроводная сеть, через которую ваши устройства подключаются к интернету.

HTTPS Защищённый протокол веб-сайтов (адрес начинается с https://), который помогает защитить ваши данные.

Менеджер паролей Программа, которая хранит все ваши пароли в одном защищённом месте.

Мошенник Человек, который обманывает других в интернете, чтобы получить их деньги или данные.

Аккаунт Ваша личная учётная запись на сайте или в приложении (например, в Instagram, Google или банке).

Облако Сервисы, где данные хранятся не на вашем устройстве, а на удалённых серверах (например, Google Drive, Dropbox).

Социальные сети Онлайн-платформы, где люди общаются и делятся информацией (например, Instagram, Facebook, TikTok).

Персональные данные Информация о вас, например: имя, адрес, телефон, паспортные данные, логины, пароли.

Мошеннический сайт Фальшивый сайт, который маскируется под настоящий, чтобы украсть ваши данные.

Инцидент безопасности Ситуация, когда ваши данные или устройство подверглись угрозе (например, взлом или утечка информации).

Социальная инженерия Методы обмана, когда мошенники пытаются заставить вас раскрыть секреты или сделать что-то вредное (например, «позвонить от имени банка»).

Обновление программ Установка новых версий приложений и операционных систем, чтобы закрыть «дыры» в защите.

Цифровой этикет Правила вежливого и безопасного поведения в интернете.

3. Тематика Программы

Модуль 1. Введение	Концепция кибербезопасности. Сквозные принципы и практики цифровой защиты. Модуль знакомит с понятием кибербезопасности как с системой мер по защите данных, устройств и сетей. Подчёркивается роль базовых принципов защиты — надёжных паролей, обновлений, резервного копирования, осознанного поведения в цифровой среде — в повседневной жизни каждого человека.
	Стандарты цифровой безопасности и основы персональной защиты данных. Рассматриваются основные международные и национальные рекомендации по защите личных данных, в том числе правила безопасного поведения в интернете, цифровой этикет и ответственность пользователя за свои действия в онлайн-пространстве.
	Содержание угроз и основные цифровые риски. Анализируются ключевые угрозы, с которыми сталкиваются обычные пользователи: вредоносные программы (вирусы, трояны, шпионское ПО), попытки взлома аккаунтов, методы социальной инженерии, а также распространённые схемы мошенничества, направленные на кражу данных или денег
	Современные практики формального и неформального обучения цифровой грамотности. Онлайн-сообщества и образовательные ресурсы. Изучение практик цифрового просвещения: курсов, обучающих программ, вебинаров, форумов и онлайн-сообществ, которые помогают людям всех возрастов освоить основы цифровой безопасности. Оценка и обсуждение ресурсов, адаптированных для школьников, студентов, преподавателей и широкой аудитории
Модуль 2. Практическая кибербезопасность для каждого	Как защититься от мошенников и не попасться на удочку Основные схемы обмана: фишинговые письма, подозрительные звонки, поддельные сайты, мошеннические СМС. Объяснение признаков мошенничества: странные ссылки, ошибки в тексте, просьбы сообщить личные данные. Практические советы: как проверять источники, что делать, если пришло подозрительное письмо или сообщение, как обучать детей и пожилых внимательности в интернете.
	Что делать при угрозах: взлом аккаунта, заражение устройства, потеря данных Первые шаги при взломе: смена паролей, проверка аккаунтов, обращение в службу поддержки. Понимание роли антивирусов: что это такое, как выбрать и установить, как проводить сканирование. Резервное копирование данных (бэкап): зачем оно нужно, как создавать копии, какие простые приложения помогают восстановить данные
	Безопасное использование интернета дома, в кафе и в облаке Как защитить домашнюю сеть Wi-Fi: смена пароля, шифрование, отключение ненужных устройств. Правила использования публичных сетей: почему нельзя подключаться бездумно, как использовать VPN или защищённые каналы. Облачные сервисы (Google, Яндекс, Dropbox): как хранить файлы безопасно, какие настройки приватности включать

	Социальные сети и персональная защита в цифровом мире Как защитить личные данные в соцсетях: настройки конфиденциальности, ограничение видимости личной информации, защита от взлома. Программы и приложения для защиты: менеджеры паролей, двухфакторная аутентификация, блокировщики рекламы и трекеров. Как объяснить основы кибербезопасности детям и пожилым: создание памяток, обучение через простые сценарии, демонстрация реальных примеров.
Модуль 3. Безопасность данных и цифровое поведение	Инструменты цифровой защиты: антивирусы и обновления Объяснение, зачем нужен антивирус, как его выбрать и установить. Роль обновлений программ и приложений в защите от угроз: почему обновления закрывают «дыры» в безопасности. Практические советы по регулярному обновлению устройств и программного обеспечения.
	Безопасные онлайн-платежи и финансовая защита Как правильно оплачивать покупки в интернете. Основные правила безопасности: защищённые сайты, двухфакторная аутентификация, запрет на ввод данных на подозрительных сайтах. Как защитить банковские карты и электронные кошельки от кражи данных.
	Ошибки пользователей, которые открывают двери для взлома Частые ошибки: слабые пароли, одинаковые пароли для всех сервисов, переход по подозрительным ссылкам. Как формировать безопасные привычки: регулярные проверки, осторожность с вложениями, настройка уведомлений. Разбор реальных случаев и типичных сценариев, которые приводят к проблемам
	Личные данные и цифровой этикет Что такое персональные данные и почему важно их защищать. Что можно безопасно рассказывать в интернете, а что лучше оставить при себе. Основы цифрового этикета: уважение к другим, корректное поведение в соцсетях, осторожность при публикации информации.
	Кибербезопасность на рабочем месте и карьера в ИБ Основные правила безопасности на работе: корпоративные сети, рабочие устройства, служебные письма. Почему сотрудники часто становятся слабым местом компании и как избежать утечек данных. Обзор профессий в сфере кибербезопасности: чем занимаются специалисты, какие навыки востребованы, с чего начать путь в этой области
Модуль 4. - Практикум по цифровой безопасности и использование ИИ в кибербезопасности	Настройка безопасного Wi-Fi и защита домашней сети
	Защита и настройка мобильных устройств
	Применение ИИ и автоматических инструментов в кибербезопасности
	Домашний аудит цифровой безопасности
	Практика с мессенджерами и безопасной перепиской.
	Менеджеры паролей — что это и как ими пользоваться
	Практика защиты учетных записей: мониторинг утечек и управление доступом
	Анонимность и конфиденциальность в сети: VPN, TOR, Proxy.
	Безопасная настройка Windows/Mac/Linux: защита от слежки
	Advanced Mobile Security: продвинутые настройки безопасности смартфона
	Настройка базового файервола / VPN

	Настройка DNS и блокировка вредоносных сайтов
Модуль 5. Аттестация.	
Модуль 6. Посткурсовая поддержка.	

4. Цель, задачи и ожидаемые результаты Программы

Цель программы:

Сформировать у педагогов (учителей и преподавателей) базовые и практические компетенции в области кибербезопасности, персональной цифровой защиты и этичного поведения в сети, чтобы они могли:

- уверенно использовать безопасные цифровые практики в личной и профессиональной деятельности;
- передавать знания и навыки по кибербезопасности учащимся, коллегам и родителям;
- формировать цифровую грамотность в образовательной среде и предотвращать распространённые угрозы в онлайн-пространстве.

Задачи Программы:

- Ознакомить слушателей с ключевыми понятиями и принципами кибербезопасности.
- Дать представление о современных интернет-угрозах: вирусах, фишинге, социальной инженерии, утечках данных и мошенничестве.
- Объяснить основы цифрового этикета, ответственности и правового поля (персональные данные, цифровой след).
- Научить слушателей защищать свои устройства, аккаунты и данные с помощью доступных инструментов: антивирусов, менеджеров паролей, резервного копирования, VPN, безопасных настроек Wi-Fi и мобильных устройств.
- Провести практику по анализу и реагированию на реальные угрозы (подозрительные письма, утечки, взломы).
- Научить проверять конфиденциальность в социальных сетях, мессенджерах и облачных сервисах.
- Показать, как использовать ИИ как помощника в цифровой безопасности.
- Обеспечить педагогов адаптированными материалами, примерами и инструментами для обучения кибербезопасности детей, подростков и взрослых.
- Научить строить занятия, ролевые игры и практические задания по темам цифровой безопасности.
- Развить навыки критического мышления в цифровой среде у самих педагогов и их обучающихся.
- Сформировать у слушателей устойчивые привычки цифровой гигиены.
- Повысить осознанность и внимательность к действиям в интернете, включая публикации, установки программ, открытие ссылок и передачу информации.
- Укрепить уверенность в использовании цифровых технологий при соблюдении норм безопасности.

Результаты обучения:

- Понимает ключевые термины и концепции кибербезопасности: цифровая гигиена, фишинг, социальная инженерия, вредоносное ПО, двухфакторная аутентификация, резервное копирование и др.
- Знает основные виды цифровых угроз и способы их распознавания.
- Осведомлён о современных принципах цифровой безопасности и конфиденциальности в интернете.
- Знает правила безопасного поведения в социальных сетях, мессенджерах, облачных платформах.
- Знает, какие международные рекомендации и нормы регулируют защиту персональных данных.
- Имеет представление о возможностях искусственного интеллекта в области кибербезопасности.
- Применяет базовые методы защиты личных данных, устройств и аккаунтов в повседневной жизни.
- Настраивает безопасное подключение к Wi-Fi, применяет антивирусы, блокировщики рекламы, менеджеры паролей.
- Реагирует на инциденты (взлом аккаунта, вирус, подозрительная активность): принимает меры, обращается в службы поддержки, восстанавливает данные.
- Проверяет устройства и аккаунты на уязвимости, использует инструменты контроля утечек.
- Настраивает приватность в социальных сетях, браузерах, мессенджерах.
- Обучает других (учеников, коллег, родителей) основам кибербезопасности, применяет практические методы преподавания цифровой гигиены.

5. Структура и содержание программы

	Тема и содержание занятия	**Кол-во часов**	**Форма занятия**
1	**Введение**	12	
1.1	Концепция кибербезопасности. Сквозные принципы и практики цифровой защиты.	1	лекция
		2	практическое занятие
1.2	Стандарты цифровой безопасности и основы персональной защиты данных.	1	лекция
		2	практическое занятие
1.3	Содержание угроз и основные цифровые риски.	1	лекция
		2	практическое занятие
1.4	Современные практики формального и неформального обучения цифровой	3	лекция

	грамотности. Онлайн-сообщества и образовательные ресурсы.	3	практическое занятие
2	**Практическая кибербезопасность для каждого**	18	Лекция/ практические занятия
2.1	Основные схемы обмана: фишинговые письма, подозрительные звонки, поддельные сайты, мошеннические СМС.	1	лекция
2.2	Взлом аккаунта, заражение устройства, потеря данных	1	лекция
2.3	Резервное копирование данных (бэкап)	2	практика
2.4	Безопасное использование интернета дома, в кафе и в облаке	2	лекция
2.5	Настройки конфиденциальности, ограничение видимости личной информации, защита от взлома	3	практика
2.6	Программы и приложения для защиты: менеджеры паролей, двухфакторная аутентификация, блокировщики рекламы и трекеров	3	практика
2.7	Облачные сервисы (Google, Яндекс, Dropbox): как хранить файлы безопасно, какие настройки приватности включать	2	лекция
2.8	Безопасные транзакции	2	самостоятельная работа
2.9	Как объяснить основы кибербезопасности детям и пожилым: создание памяток, обучение через простые сценарии, демонстрация реальных примеров.	2	самостоятельная работа
3	**Безопасные онлайн-платежи и финансовая защита**	18	Лекция/ практические занятия
3.1	Основные правила безопасности: защищённые сайты, двухфакторная аутентификация, запрет на ввод данных на подозрительных сайтах.	1	лекция
3.2	Как формировать безопасные привычки: регулярные проверки, осторожность с вложениями, настройка уведомлений	2	практическое занятие
3.3	Ошибки пользователей, которые открывают двери для взлома	1	лекция
3.4	Корпоративные сети, рабочие устройства, служебные письма	2	практическое занятие
3.5	Личные данные и цифровой этикет	1	лекция

3.6	Реагирование на инциденты (взлом аккаунта, вирус, подозрительная активность	2	самостоятельная работа
3.7	Кибербезопасность на рабочем месте и карьера в ИБ	1	лекция
3.8	Обучает(учеников, коллег, родителей) основам кибербезопасности, применение практических методов преподавания цифровой гигиены	2	практическое занятие
3.9	Инструменты контроля утечек	1	лекция
3.10	Разработка адаптированных материалов, примеров и инструментов для обучения кибербезопасности детей, подростков и взрослых	2	практическое занятие
3.11	ИИ как помощника в цифровой безопасности	1	лекция
3.12	Практическое занятие по созданию эффективного учебного материала	2	самостоятельная работа
4	**Практикум по цифровой безопасности и использование ИИ в кибербезопасности**	18	Лекция/ практические занятия
4.1	Настройка безопасного Wi-Fi и защита домашней сети	1	лекция
4.2	Защита и настройка мобильных устройств, Wi-Fi	3	практическое занятие
4.3	Применение ИИ и автоматических инструментов в кибербезопасности	1	лекция
4.4	Домашний аудит цифровой безопасности. Advanced Mobile Security: продвинутые настройки безопасности смартфона.	3	практическое занятие
4.5	Менеджеры паролей — что это и как ими пользоваться	1	лекция
4.6	Анонимность и конфиденциальность в сети: VPN, TOR, Proxy	2	лекция
4.7	Безопасная настройка Windows/Mac/Linux: защита от слежки. Настройка базового файервола / VPN. Настройка DNS и блокировка вредоносных сайтов	3	практическое занятие
4.8	Практика с мессенджерами и безопасной перепиской Практика защиты учетных записей: мониторинг утечек и управление доступом	4	самостоятельная работа
5	**Аттестация**	6	портфолио из серий

			занятий
6	**Посткурсовая поддержка**	8	онлайн консультирование

6. Организация учебного процесса

Программы повышения квалификации проводятся в очной форме в соответствии с учебно-тематическим планом. Продолжительность курсов составляет 80 часов. Учебный процесс включает использование интерактивных методов и форм, таких как лекции, семинары, практические занятия, тренинги, мастер-классы, ролевые игры, кейс-методы, обсуждения, совместное решение задач, а также

вебинары, онлайн-форумы, консультации и самостоятельное обучение. В рамках программы для оценки знаний слушателей предусмотрена защита портфолио, включающего серию учебных занятий.

7. Учебно-методическое обеспечение Программы

Учебно-методическое обеспечение курса повышения квалификации «Основы кибербезопасности и защиты данных» включает доступ к учебным материалам, методическим рекомендациям и дополнительным ресурсам для самостоятельного изучения. Участники курса получают доступ к онлайн-платформе, где размещены модули с заданиями и тестами для самооценки знаний. Также предусмотрена поддержка наставников и консультантов, которые помогают разобраться с возникающими вопросами. Взаимодействие с преподавателями и коллегами способствует более глубокому пониманию материала и обмену опытом в образовательной сфере.

8. Оценивание результатов обучения

Оценка достижений слушателей курсов повышения квалификации охватывает не только проверку их теоретических знаний, но и анализ практического применения полученных навыков. Это включает тестирование, анализ выполненных заданий, а также участие в практических сессиях и дискуссиях. Такая оценка помогает подтвердить успешность программы и выявить области, которые можно улучшить для повышения качества обучения.

№	**Целеполагание и постановка проблемы**	**Комментарий**	**Баллы**

1.	Теоретические знания и понимание материала.	Слушатель демонстрирует уверенное владение основными понятиями кибербезопасности, цифровой гигиены и защиты данных. Понимает, что такое вирусы, фишинг, социальная инженерия, двухфакторная аутентификация, резервное копирование, цифровой этикет и др. Знает ключевые угрозы, принципы безопасного поведения и способы защиты в цифровом пространстве.	20
2.	Практическое применение знаний.	Слушатель умеет применять полученные знания на практике: настраивает безопасное соединение Wi-Fi; использует антивирус и менеджер паролей; выполняет резервное копирование; реагирует на инциденты (взлом, подозрительная активность); применяет настройки конфиденциальности в соцсетях, браузерах и мессенджерах.	20
3.	Разработка учебных заданий и материалов.	Слушатель способен создавать простые и понятные обучающие материалы по цифровой безопасности для разных аудиторий (ученики, коллеги, родители). Разрабатывает: памятки и мини-гайды; практические задания и ролевые сценарии; вопросы для викторин и обсуждений; обучающие слайды или карточки.	15
4.	Качество разработки портфолио.	Оценка защиты портфолио, которое включает серию учебных заданий, разработанных на основе курса. Важными аспектами являются полнота, четкость и практическое применение материалов курса.	25
5.	Критическое мышление и аналитические способности.	Слушатель умеет: анализировать ситуации и распознавать потенциальные угрозы; выявлять ошибки в поведении пользователей, ведущие к взлому или утечке; сравнивать и оценивать надёжность инструментов (например, VPN, антивирусов); принимать обоснованные решения в цифровой среде.	10

7.	Коммуникационные навыки.	Оценка способности слушателей эффективно взаимодействовать с коллегами и наставниками в рамках учебного процесса. Важными аспектами являются активное участие в дискуссиях, презентациях и круглых столах.	5
8.	Вклад в развитие курса и инновации.	Оценка предложений и новых идей, которые участники курса вносят в развитие учебных материалов и подходов. Включает участие в разработке новых методов и технологий в процессе обучения.	3
9.	Посткурсовая поддержка и использование онлайн-ресурсов.	Оценка активности слушателей в онлайн-консультациях после окончания курса и использования дополнительных онлайн-ресурсов. Учитывается способность применять знания для дальнейшего профессионального роста.	2
Итого количество баллов:			100

9. Посткурсовое сопровождение

Посткурсовое сопровождение для курса «Основы кибербезопасности и защиты данных» включает в себя серию из четырех онлайн-лекций, направленных на консолидацию полученных знаний и дальнейшее развитие педагогических навыков участников.

Реализация посткурсового сопровождения образовательной программы по теме: «Основы кибербезопасности и защиты данных».

№	Наименование темы	Комментарии	Формы	Периодичность
1	Внедрение практик цифровой безопасности в учебный процесс	Обсуждение опыта участников по передаче знаний о кибербезопасности школьникам и студентам. Обмен разработанными памятками, уроками, интерактивными заданиями. Анализ барьеров и успешных подходов	вебинар	1 сессия

2	Анализ цифровых инцидентов: кейсы из реальной жизни	Разбор инцидентов (фишинг, утечки, взломы), представленных участниками или инструктором. Совместный анализ действий, ошибок и правильных решений. Практика командного реагирования.	семинар	1 сессия
3	Использование инструментов ИИ для повышения цифровой безопасности	Обзор простых инструментов на базе ИИ: генераторы паролей, боты для проверки утечек, фильтрация фишинговых писем. Демонстрация и обсуждение применения в педагогической практике.	семинар	1 сессия
4	Преподавание цифровой грамотности детям, подросткам и взрослым	Рекомендации по адаптации материалов для разных возрастов. Упражнения, игры и модели ролевого обучения. Поддержка педагогов в разработке собственных курсов и программ.	круглый стол	1 сессия

10. Список основной и дополнительной литературы

Основная

1. Столлингс, У. Network Security Essentials: Applications and Standards / У. Столлингс. — 6-е изд. — Бостон: Pearson, 2020. — 464 с.

2. Бирюков, А. Информационная безопасность: защита и нападение / А. Бирюков. — М.: ДМК Пресс, 2021. — 384 с.

3. Столлингс, У. Основы сетевой безопасности: приложения и стандарты = Network Security Essentials: Applications and Standards / У. Столлингс ; пер. с англ. — 6-е глоб. изд. — Бостон: Пирсон, 2020. — 464 с. (Оригинал: Stallings W. Network Security Essentials: Applications and Standards, 6th Global Ed.)

4. Паттон, Х. Э. Продвижение по карьерной лестнице в кибербезопасности = Navigating the Cybersecurity Career Path / Х. Э. Паттон ; пер. с англ. — Себастопол: О’Рейлли Медиа, 2022. — 240 с. (Оригинал: Patton H. Navigating the Cybersecurity Career Path)

Дополнительная