

Департамент информатизации Тюменской области
Государственное автономное учреждение дополнительного образования
Тюменской области
«Региональный информационно-образовательный центр»

СОГЛАСОВАНО

Заместитель Губернатора
Тюменской области,
директор
Департамента информатизации
Тюменской области

С.И. Логинов

«10» августа 2026



УТВЕРЖДАЮ

Заместитель директора
ГАУ ДО ТО «РИО-Центр»

О.А. Кононенко

«10» августа 2026



УЧЕБНАЯ ПРОГРАММА

«Информационная безопасность и кибербезопасность»

Трудоемкость программы – 5 академических часов

Форма обучения – очная, очно-заочная с применением дистанционных образовательных технологий.

Режим занятий – 5 академических часов в день

Уровень развития компетенций – начальный

Программа предназначена для обучения сотрудников органов государственной власти, местного самоуправления Тюменской области и подведомственных им учреждений и жителей Тюменской области, заинтересованных данной темой.

Цель обучения: сформировать у слушателей базовые цифровые компетенции по вопросам безопасного пользования информационно-коммуникационными технологиями.

Реализация учебной программы возможна в формате очного обучения, а также очно-заочного с применением дистанционных образовательных технологий (ДОТ). При очном обучении слушатели посещают аудиторные занятия, прослушивают лекции и выполняют практические задания по темам совместно с тренером и самостоятельно в рамках аудиторной работы.

Очно-заочное обучение с применением дистанционных технологий проходит в формате веб-занятия (вебинары, дистанционные уроки/курсы). В формате вебинаров прослушивается лекционный материал, практические задания выполняются параллельно с тренером (при наличии технической возможности), разбираются вопросы в режиме реального времени. Также предусматривается самостоятельная внеаудиторная работа (очно-заочная форма с применением ДОТ).

Промежуточная оценка качества освоения программы осуществляется путем устного опроса в ходе занятий (очное обучение, вебинар). Итоговая оценка осуществляется в виде тестирования. По окончании обучения слушателям выдается сертификат о прохождении курса.

В результате освоения данной программы слушатели приобретут базовые знания, умения, навыки по информационной безопасности и кибербезопасности.

Знания:

- базовые понятия и различия между информационной безопасностью и кибербезопасностью, их цели и задачи;
- ключевые принципы защиты информации: конфиденциальность (доступ только для уполномоченных лиц), целостность (сохранность и неизменность данных), доступность (обеспечение доступа к информации в нужное время), неотказуемость (возможность подтвердить авторство и факт совершения действия), а также основы аутентификации (подтверждение личности) и авторизации (предоставление прав доступа);
- основные виды киберугроз и механизмы их реализации: вредоносное ПО (вирусы, трояны, шпионские программы), DDoS-атаки (перегрузка ресурсов), фишинг (мошеннические сообщения для кражи данных), социальная инженерия (манипуляции для получения доступа), уязвимости нулевого дня (неизвестные разработчикам уязвимости, для которых ещё нет исправлений);
- современные технологии и инструменты защиты: антивирусные решения, криптографические методы шифрования данных, межсетевые экраны (брандмауэры), системы обнаружения (IDS) и реагирования на угрозы (EDR).

Умения:

- идентифицировать потенциальные киберугрозы в повседневных ситуациях (например, распознавать фишинговые письма, подозрительные ссылки, попытки социальной инженерии);
- применять базовые принципы кибербезопасности для оценки рисков при работе с информацией (проверять надёжность источников, анализировать уровень доступа к данным, оценивать необходимость передачи персональных сведений);
- правильно использовать средства защиты информации: настраивать и применять антивирусное ПО, понимать назначение и базовые сценарии использования брандмауэров, использовать шифрование для защиты конфиденциальных данных;
- выбирать адекватные меры защиты в зависимости от типа угрозы и контекста (например, применять многофакторную аутентификацию для критически важных аккаунтов, избегать открытия вложений из непроверенных источников).

- применять на практике правила кибергигиены: создавать надёжные пароли, настраивать двухфакторную аутентификацию, регулярно обновлять ПО, проверять источники информации.

Навыки:

- безопасного поведения в цифровой среде: создавать и управлять надёжными паролями, использовать менеджеры паролей, регулярно обновлять ПО для устранения уязвимостей;
- защиты персональных данных: минимизировать раскрытие личной информации в интернете, проверять настройки конфиденциальности в сервисах и приложениях, осознанно предоставлять доступ к данным;
- реагирования на инциденты: знать алгоритм действий при подозрении на взлом аккаунта или заражение вредоносным ПО (смена паролей, уведомление ответственных лиц, изоляция заражённого устройства);
- критического анализа цифровой среды: отличать легитимные запросы от мошеннических, проверять подлинность сайтов (HTTPS, сертификаты), избегать рискованных действий под давлением или из-за срочности запроса.

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование разделов и тем	Всего (часов)	В том числе:	
			Лекции (часов)	Практические занятия/Самостоятельная внеаудиторная работа (часов)
1.	Информационная безопасность. Кибербезопасность.	0,3	0,3	
2.	Ключевые аспекты кибербезопасности.	1,3	0,5	0,8
3.	Виды угроз и методы защиты.	2	1,5	0,5
4.	Личная информационная безопасность и кибергигиена.	0,9	0,1	0,8
5.	Итоговое тестирование.	0,5		0,5
	Всего (часов)	5	2,4	2,6

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и тем	Всего (часов)	В том числе:	
			Лекции (часов)	Практические занятия/Самосто- ятельная внеаудиторная работа (часов)
1.	Информационная безопасность. Кибербезопасность.	0,3	0,3	
2.	Ключевые аспекты кибербезопасности.	1,3	0,5	0,8
3.	Виды угроз и методы защиты.	2	1,5	0,5
3.1	Основные виды угроз.	0,9	0,9	
3.2	Правила кибербезопасности.	1,1	0,6	0,5
4.	Личная информационная безопасность и кибергигиена.	0,9	0,1	0,8
5.	Итоговое тестирование.	0,5		0,5
	Всего (часов)	5	2,4	2,6

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Кибербезопасность.

Понятие информационной безопасности и кибербезопасности.

2. Ключевые аспекты кибербезопасности:

Конфиденциальность. Целостность. Доступность. Неотказуемость. Аутентификация и авторизация.

3. Виды угроз и методы защиты.

3.1. Основные виды угроз: вредоносное ПО, DDoS-атаки, фишинг, социальная инженерия, уязвимости нулевого дня.

3.2. Правила кибербезопасности.

Противостоять киберугрозам помогают технологии защиты информации, например антивирусные программы, криптографические методы шифрования данных, брандмауэры и программы для выявления подозрительной активности, например систем классов IDS и EDR.

4. Личная информационная безопасность и кибергигиена.

Принципы кибергигиены, как комплекс повседневных мер по обеспечению личной информационной безопасности. Параметры безопасности учётных записей в ключевых цифровых сервисах: на портале Госуслуг, в популярных мессенджерах и социальных сетях (двухфакторная аутентификация, приватность профиля, контроль доступа).

4. Итоговое тестирование.

КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и тем	Учебный день
1.	Информационная безопасность. Кибербезопасность.	1
2.	Ключевые аспекты кибербезопасности.	
3.	Виды угроз и методы защиты.	
4.	Личная информационная безопасность и кибергигиена.	
5.	Итоговое тестирование.	

Итого: 1 календарный день

