



**ФОНД
ГУМАНИТАРНЫХ
ПРОЕКТОВ**

**Кировское областное государственное профессиональное образовательное
бюджетное учреждение
«Омутнинский колледж педагогики, экономики и права»**

**ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПРОБЫ
«СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

**в рамках проекта по ранней профессиональной ориентации
учащихся 6-9 классов общеобразовательных организаций
«Билет в будущее»**

**г. Омутнинск
2023**

Оглавление

1. Паспорт программы профессиональной пробы.....	3
2. Содержание программы.....	3
3. Инфраструктурный лист	6
4. Приложение и дополнения	6

1. Паспорт программы профессиональной пробы

Профессиональная среда: безопасная

Наименование профессионального направления: специалист по информационной безопасности

Автор программы: *Лусникова Елена Сергеевна, преподаватель КОГПОБУ «Омутнинский колледж педагогики, экономики и права»*

Контакты автора: *Кировская область, г. Омутнинск, e.lusnikova@yandex.ru, 89091334135.*

Площадка: КОГПОБУ «Омутнинский колледж педагогики, экономики и права»,

Кировская область, город Омутнинск, улица Воровского, 3

<i>Вид</i>	<i>Формат проведения</i>	<i>Время проведения</i>	<i>Возрастная категория</i>	<i>Доступность для участников с ОВЗ</i>
Ознакомительный	Очный	60 минут	6-9 классы	Общие заболевания (нарушение дыхательной системы, пищеварительной, эндокринной систем, сердечно-сосудистой системы и т.д.).

2. Содержание программы

Введение (10 мин)

1. **Краткое описание профессионального направления.**

Профессиональное направление предназначено для подготовки специалистов в области информационной безопасности. Эта профессия возникла на стыке двух направлений: информационных технологий и технологий обеспечения безопасности. Без сотрудников по информационной безопасности сегодня не могут обойтись ни коммерческие структуры, ни ведомственные организации. Они предотвращают утечку важной информации, подлог данных и некомпетентность (злой умысел) собственных сотрудников. В государственном масштабе специалисты по информационной безопасности создают системы защиты стратегической информации по обороноспособности страны, формируют секретные базы данных, сохраняют тайну ядерного чемоданчика.

2. **Место и перспективы профессионального направления в современной экономике региона, страны, мира.**

Направление «специалист по информационной безопасности» актуально в современном мире. Внутри направления также существует разделение на узкие специальности:

- **пентестеры** (занимаются поиском уязвимостей, составлением отчетов; тестируют различные компании, работают на аутсорсе или по заказу);

- **специалисты по разработке** (принимают участие в разработке программ, приложений; занимаются изучением архитектуры, готового кода, указывают на возможные ошибки, баги, уязвимости);

- **специалисты по сетям** (занимаются поиском стандартных и необычных новых уязвимостей в сетевых, аппаратных комплексах; способны найти причину взлома и организовать систему с мощной защитой от кибератак).

3. *Необходимые навыки и знания для овладения профессией.*

Специалист по информационной безопасности должен знать методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации. Уметь применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации.

4. *1-2 интересных факта о профессиональном направлении.*

В России 90 миллионов человек пользуются услугами сети Интернет, а во всем мире более 4 миллиардов пользователей сети.

В 80% всех инцидентов нарушения информационной безопасности сотрудники сами впустили в систему вредоносные программы.

5. *Связь профессиональной пробы с реальной деятельностью.*

Представленное задание – часть ежедневной профессиональной деятельности специалиста в области защиты информации.

Постановка задачи (10 мин)

1. С помощью специализированного программного обеспечения научиться извлекать скрытую информацию, передаваемую по сети, в формате изображения, аудио и видео.

2. Демонстрация процедуры.

Выполнение задания (25 мин)

1. *Алгоритм действий:*

- установить на персональный компьютер (ПК, ноутбук) программное обеспечение (демоверсии);
- произвести загрузку любого изображения и передать текстовую информацию;
- получить изображение и расшифровать его;
- передать информацию посредством видеофайла;
- получить видеофайл и расшифровать его;
- передать информацию посредством аудиофайла;
- получить аудиофайл и расшифровать его;
- представить скрины расшифрованных записей.

2. Рекомендации для наставника по организации процесса выполнения задания:

- подготовить распечатанный и электронный материалы с инструкциями по выполнению задания;
- помочь обучающемуся загрузить программу;
- проверить рабочее состояние ПК и программного обеспечения;
- обеспечить необходимые файлы для выполнения задания.

Контроль, оценка и рефлексия (15 мин)

1. Критерии успешного выполнения задания:

- зашифрованный объект загружен в программу;
- передана информация посредством изображения, аудио и видеофайла;
- полученная информация расшифрована;
- сделаны все необходимые скрины (снимки изображений экрана).

2. Рекомендации для наставника по контролю результата, процедуре оценки:

- проверить правильность шифрования изображения, аудио и видео;
- проверить правильность расшифровки изображения, аудио и видео;
- проверить наличие всех скринов.

3. Вопросы для рефлексии учащихся:

- насколько было интересно?
- вам понравился формат профессиональной пробы?
- что нового вы узнали?
- как вы представляете инженера-проектировщика систем безопасности?
- заинтересовала ли вас специальность?
- хотели бы вы продолжить обучение по этому направлению?

3. Инфраструктурный лист

<i>Наименование</i>	<i>Рекомендуемые технические характеристики с необходимыми примечаниями</i>	<i>Количество</i>	<i>На группу / на 1 чел.</i>
Персональный компьютер или ноутбук	Процессор не менее 3,2 ГГц с поддержкой виртуализации или аналог, не менее 4 физических ядер, не менее 8 потоков, не менее 8 ГБ ОЗУ, не менее 256 ГБ SSD, со свободным местом не менее 100 ГБ, ОС Windows/Linux/ с графическим интерфейсом или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналоги	1	на 1 чел.
Монитор	Не менее 20" и разрешением не менее 1920×1080 пкс	1	на 1 чел.
Программное обеспечение	QuickStego	1	на 1 чел.
Программное обеспечение	OpenStego	1	на 1 чел.
Программное обеспечение	SilentEye	1	на 1 чел.
Программное обеспечение	OpenPuff	1	на 1 чел.
Программное обеспечение	S Tools	1	на 1 чел.

4. Приложение и дополнения

<i>Ссылка</i>	<i>Комментарий</i>
https://itsecforu.ru/	Топ 10 инструментов стеганографии