СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБРАЗОВАНИЕ НАЦИОНАЛЬНЫЕ ПРОЕКТЫ РОССИИ

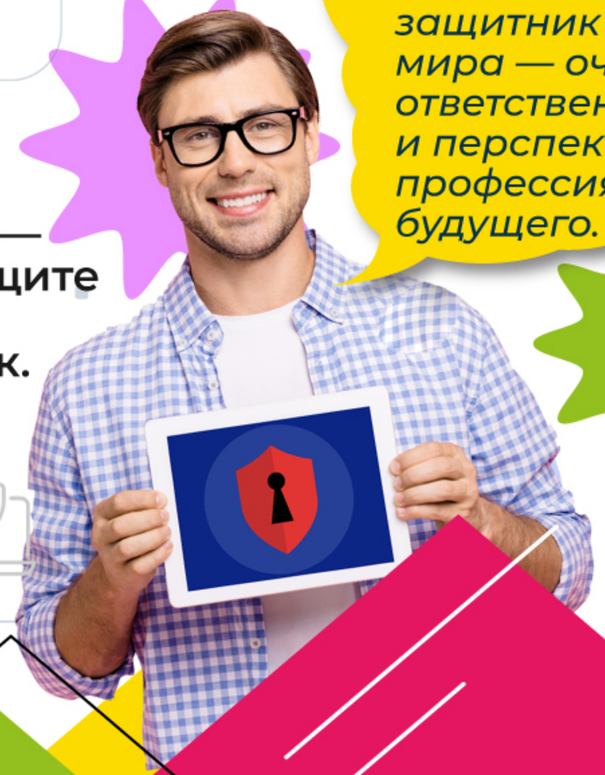
ПРОСВЕТ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ

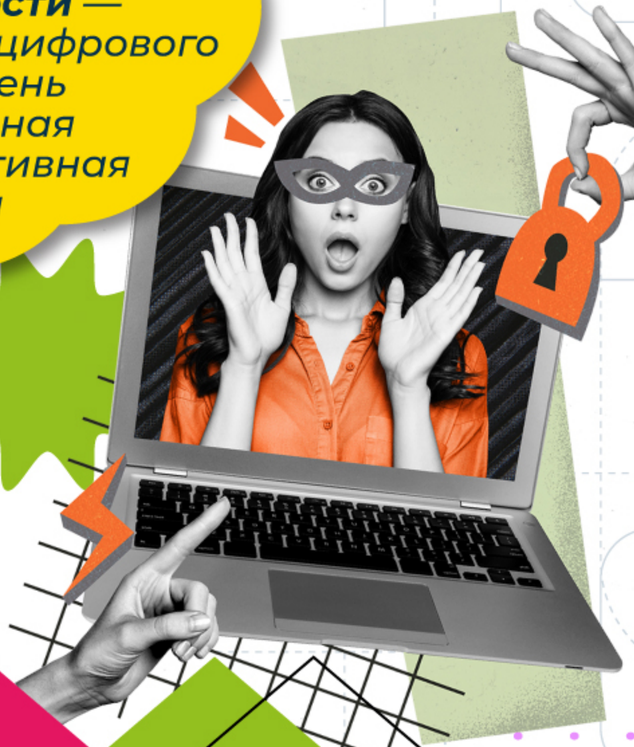
ШОУ ПРОФЕССИЙ

ЗАЩИТИМ ВАШУ ИНФОРМАЦИЮ!

Государственные организации, промышленные и коммерческие предприятия, образовательные и медицинские учреждения, банки — все нуждаются в защите от компьютерных вирусов и кибератак.

Специалист по информационной безопасности — *защитник цифрового мира — очень ответственная и перспективная профессия будущего.*





Банковские операции и онлайн-сервисы, железнодорожное и авиасообщение, все виды связи, энергетика, металлургия и нефтегазодобыча не могут существовать без информационной безопасности.

ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Принцип конфиденциальности:
информацию могут получать только те пользователи, которые имеют на это право.

Принцип целостности:
информация должна быть полной, достоверной, актуальной.

Принцип доступности:
информация должна быть доступна только законным пользователям и только в установленное время.

Защитить информацию на 100 % невозможно!

ИЗ ИСТОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1981 г.

Первые программы-вирусы

1984г.

Первые антивирусные программы

1986 – 1989 гг.

Первые вирусные эпидемии

1987– 1997 гг.

Появление и распространение фишинга

2000 – 2020 гг.

Формирование и развитие системы обеспечения информационной безопасности

ЭТО ВАЖНО ЗНАТЬ!

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. При создании аккаунтов в электронной почте и в сети используйте надежные пароли.
2. Не посещайте сомнительные сайты и не открывайте неизвестные ссылки.
3. Не открывайте файлы, полученные от незнакомых людей; они могут содержать вирусы.
4. Используйте антивирусные программы.
5. Не публикуйте в сети свои личные данные, а также данные родственников и друзей (номера телефонов, паспортные данные, адреса электронной почты).

ЭТО ПОЛЕЗНО ЗНАТЬ!

САМЫЕ РАСПРОСТРАНЕННЫЕ КИБЕРУГРОЗЫ

Компьютерные вирусы — программы, которые могут размножаться и портить файлы и другие программы на компьютере.

Фишинг — интернет-мошенничество, получение доступа к секретным данным пользователей — логинам, паролям, номерам кредитных карт.

DoS-, DDoS-атаки — хакерские атаки типа «отказ в обслуживании», перегрузка серверов компаний и организаций с целью парализовать их работу.

Утечка персональных данных — намеренное или случайное раскрытие конфиденциальной, личной или защищаемой информации.

Социальная инженерия («атака на человека») — психологические приемы и методы, позволяющие получить конфиденциальную информацию.

ЧЕМ ЗАНИМАЮТСЯ СПЕЦИАЛИСТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Обеспечивают конфиденциальность данных
- Предотвращают утечку или несанкционированный доступ к информации
- Принимают участие в создании системы защиты информации, ее аудите и мониторинге
- Анализируют информационные риски, разрабатывают и внедряют мероприятия по их предотвращению
- Устанавливают, настраивают и обслуживают технические средства защиты информации

КАКИЕ СПЕЦИАЛИСТЫ РАБОТАЮТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аналитик IT-безопасности

Собирает, обрабатывает и анализирует информацию о возможных угрозах; отвечает за то, чтобы обнаружить и предупредить утечку данных или кибератаку

Архитектор IT-безопасности

Проектирует, создает и внедряет системы обеспечения информационной безопасности

Компьютерный криминалист

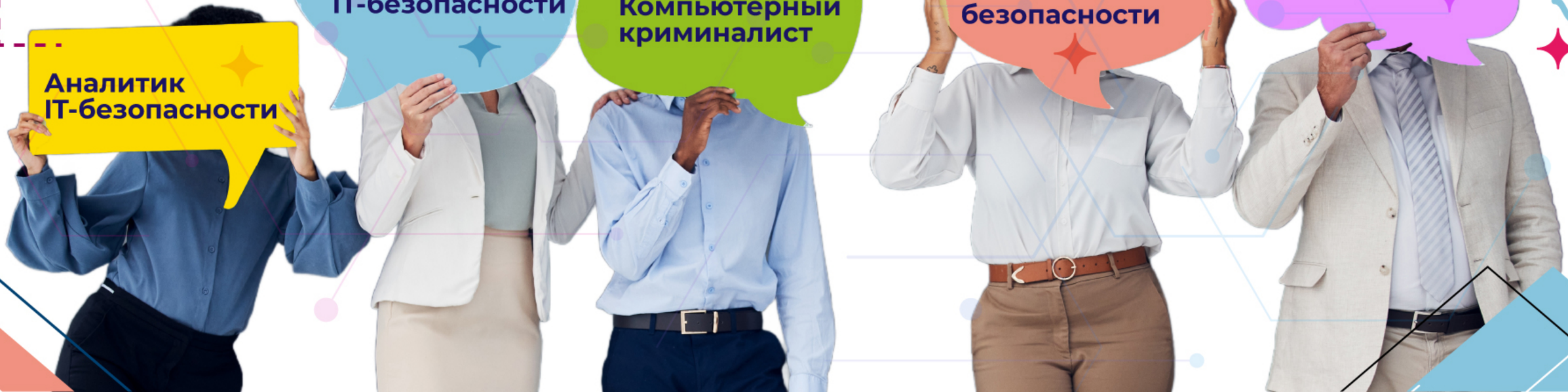
Расследует произошедшее киберпреступление, оценивает его последствия, ищет слабые места в системе защиты

Администратор систем безопасности

Обслуживает компьютеры и сетевое оборудование, устанавливает, настраивает и администрирует сервисы для обеспечения информационной безопасности

Разработчик систем защиты

Создает программное обеспечение для отслеживания кибератак и защиты от них IT-систем организации



ГДЕ ВОСТРЕБОВАНЫ СПЕЦИАЛИСТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Государственные организации

IT-компании

Образовательные и медицинские учреждения

Банки и финансовые учреждения

Корпорации и предприятия

Аудиторские фирмы

ПОДОЙДЕТ ЛИ ТЕБЕ ПРОФЕССИЯ

Аналитический склад ума

Терпеливость

Умение работать в команде

Умение принимать ответственные решения

Проверь, обладаешь ли ты всеми необходимыми качествами, которые обеспечат тебе успех в работе

Методичность

Стрессоустойчивость

Ответственность

Внимательность к деталям

Если у тебя 1–2 совпадения — есть надежда, но придется приложить усилия.

Если 3–5 совпадений — у тебя есть хороший потенциал для работы по этой специальности.

Если 6–8 совпадений — миру очень повезет, если в нем появится такой специалист!

ГДЕ МОЖНО ПОЛУЧИТЬ СПЕЦИАЛЬНОСТЬ

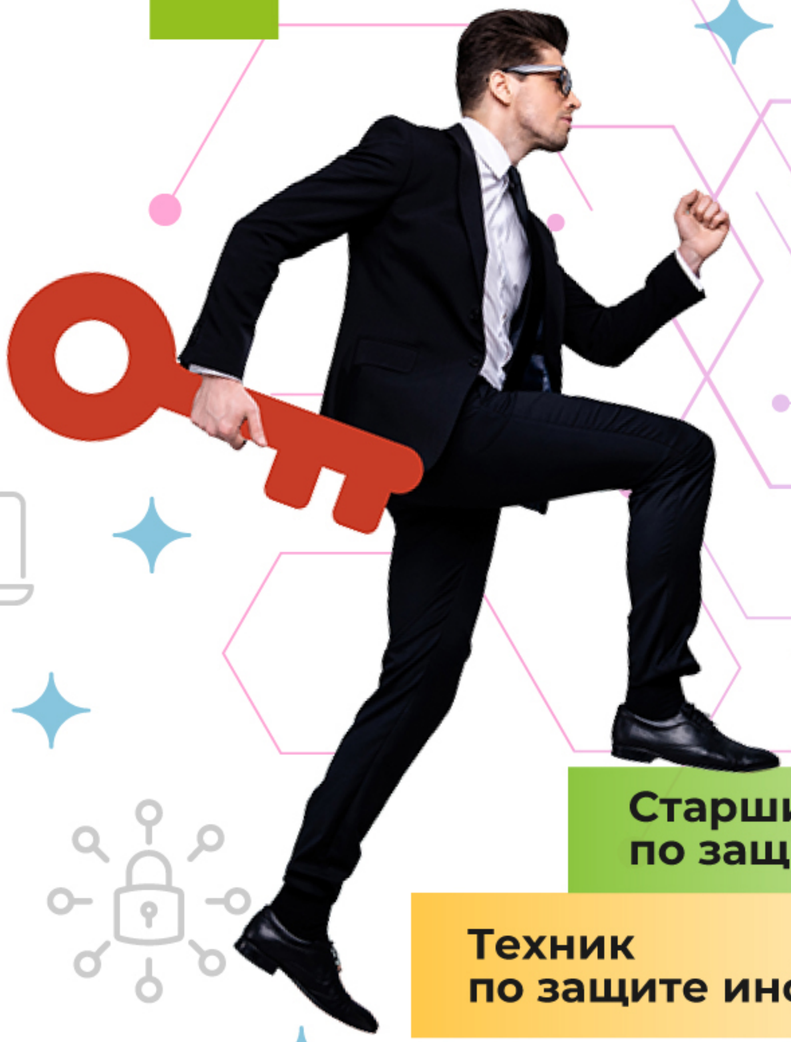
Получить специальность можно в профильных учреждениях среднего профессионального образования.

Например, в техникумах и колледжах

ПРОФЕССИОНАЛИТЕТА

- Уфимский многопрофильный профессиональный колледж
- Омский авиационный колледж имени Н.Е. Жуковского
- Томский индустриальный техникум
- Ногинский колледж (Московская область)

КАРТА ПРОФЕССИОНАЛЬНОГО РОСТА



Директор по информационной безопасности

Менеджер по информационной безопасности

Старший специалист по информационной безопасности

Специалист по информационной безопасности

Старший техник по защите информации

Техник по защите информации

БУДУЩЕЕ ПРОФЕССИИ

Дополненная реальность (AR) и виртуальная реальность (VR) — способ обучения специалистов

Искусственный интеллект — помощник в принятии решений, предсказании неисправностей и оптимизации систем защиты информации

Интернет вещей — средство взаимодействия со сложными системами защиты информации, с большими объемами данных