

МИНИСТЕРСТВО ОБРАЗОВАНИЯ КАЛИНИНГРАДСКОЙ ОБЛАСТИ
государственное бюджетное учреждение
Калининградской области
профессиональная образовательная организация
«Технологический колледж»

Рабочая программа
«Комплексная защита информации в организации»

Заведующий
по учебно-методической работе
Ивашкина Н. А. Ивашкина

Рабочая программа составлена в соответствии с требованиями квалификационных характеристик по профессии (ЕТКС).

Приказа МИНОБР РФ № 292 от 18 апреля 2013 г. «Об утверждении порядка организации и осуществления образовательной деятельности по основным программам профессионального обучения»;

Квалификационного справочника должностей руководителей, специалистов и других служащих

Организация-разработчик: государственное бюджетное учреждение Калининградской области профессиональная образовательная организация «Технологический колледж» (ГБУ КО ПООТК)

Разработчики:

педагогические работники ГБУ КО ПООТК

Рассмотрена на заседании методической кафедры математических, естественнонаучных дисциплин и информационных технологий

Ульянова О.М.

СОГЛАСОВАНО:

работодатель

ООО «Альфа 39»

Директор В.Ю. Ижигов



ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Интенсивный курс повышения квалификации руководителей и специалистов, ответственных за защиту конфиденциальной информации от утечки по техническим каналам, направленный на практическую подготовку к использованию методов и средств выявления и блокирования технических каналов утечки информации.

Основная цель обучения по данной программе заключается в ознакомлении слушателей с: необходимостью, существом и содержанием защиты в системах обработки и передачи данных; современными и перспективными концепциями, методами и средствами защиты информации; организацией комплексной защиты информации на современных объектах с определенным уровнем закрытости циркулирующей на них информации; практической работой по использованию средств и систем защиты.

Специалист по защите информации должен знать и уметь использовать:

- основные положения теории информации, принципы построения систем обработки и передачи информации, основы семантического подхода к анализу информационных процессов; современные аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите государственной тайны;
- основные правовые положения в области информационной безопасности и защиты информации.

методы анализа и оценки величины возможного ущерба, наносимого безопасности Российской Федерации вследствие несанкционированного (противоправного) распространения информации, составляющей государственную тайну;

основные правовые понятия, правовые акты Российской Федерации в области защиты государственной тайны;

законодательные основы организации защиты государственной тайны, задачи органов защиты государственной тайны;

Количество часов на освоение программы: всего – 256 часов.

Продолжительность обучения по данному курсу – 3 месяца

Программа учебного курса

Раздел 1. Введение. Персональные данные в организации (на предприятии)

- Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни.
- Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных.
- Персональные данные в системе документооборота предприятия. Персональные данные в автоматизированных системах и приложениях.
- Значимые утечки персональных данных в России и примеры неправомерного использования персональных данных.

Раздел 2. Основные понятия Федерального закона "О персональных данных"

- Содержание категории "персональные данные".
- Область применения закона. Ограничения.
- Обработка персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.
- Принципы обработки персональных данных.
- Условия обработки персональных данных. Согласие субъекта. Согласие в письменной форме.
- Общедоступные, подлежащие опубликованию или обязательному раскрытию персональные данные.
- Специальные категории персональных данных и особенности их обработки. Данные о судимости.
- Биометрические персональные данные.
- Трансграничная передача персональных данных. Страны, обеспечивающие адекватную защиту прав субъектов персональных данных. Локализация персональных данных российских граждан после 1 сентября 2015 года.
- Особенности обработки персональных данных при предоставлении государственных и муниципальных услуг.
- Права субъектов персональных данных и их соблюдение при обработке.
- Обязанности оператора персональных данных.
- Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
- Ответственность за нарушение требований по обращению с персональными данными. Практика правоприменения.

Раздел 3. Работа с персональными данными на предприятии (в организации)

- Мероприятия по защите сведений ограниченного доступа. Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства.

- Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением.
- Локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, их содержание, порядок разработки и ввода в действие.
- Особенности обработки персональных данных, осуществляемой без использования средств автоматизации.
- Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

Раздел 4. Техническая защита персональных данных в информационных системах

- Требования Федерального закона "О персональных данных" и Постановления Правительства РФ 2012 г. № 1119 к обеспечению безопасности персональных данных.
- Уровни защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) в зависимости от угроз безопасности этим данным, категорий персональных данных и количества субъектов, чьи данные обрабатываются в ИСПДн.
- Построение системы защиты персональных данных. Положения приказов ФСТЭК России 2013 г. № 21 и ФСБ России 2014 г. № 378, определение базовых, адаптивных и компенсирующих мер защиты.

Раздел 5. Биометрическая идентификация

- Цель создания Единой биометрической системы, полномочия и обязанности участников системы биометрической идентификации.
- Защита данных при проведении первичной и удаленной биометрической идентификации; контроль и надзор за соблюдением установленных требований.
- Согласие субъекта на обработку персональных данных при проведении биометрической идентификации.

Раздел 6. Лицензирование деятельности по технической защите конфиденциальной информации

- Понятие технической защиты как лицензируемого вида деятельности.
- Лицензионные требования.
- Ответственность за незаконную деятельность в области защиты информации.
- Незаконное предпринимательство.
- Оценка и управление риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации.

Раздел 7. Аутсорсинг обработки персональных данных и их технической защиты

- Требования, выдвигаемые законом к порядку обработки персональных данных внешней организацией, содержание договора на обработку персональных данных.
- Передача внешней организации функций технической защиты персональных данных.

- Передача внешней организации функций лица, ответственного за организацию обработки персональных данных
- Достоинства и недостатки аутсорсинга обработки персональных данных и их защиты.

Раздел 8. Контроль и надзор за соблюдением законодательства о персональных данных

- Система государственного контроля и надзора за обеспечением безопасности персональных данных.
- Порядок планирования, организации и проведения проверок.
- Права и обязанности проверяемых и проверяющих.
- Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений.
- Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений.

Раздел 9. Новый европейский регламент защиты персональных данных GDPR

- Цели принятия нового регламента и его основные отличия от ранее принятых документов.
- Применимость GDPR к деятельности российских компаний.
- Основные понятия регламента.
- Права субъекта данных.
- Требования GDPR к технической защите персональных данных.

Список литературы:

1. Синаторов С.В. Пакеты прикладных программ. Учебное пособие : учебное пособие / С.В. Синаторов. — М.: КноРус, 2019. — 195 с.
2. Базы данных (для ссузов). Учебник : учебник / И.А. Кумскова. — Москва : КноРус, 2018. — 400 с.
3. Мельников В.П. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов. — М.: КноРус, 2018. — 267 с.
4. Бубнов А.А. Основы информационной безопасности (2-е изд., стер.) учебник
5. Паклина О.В, Организация производственной деятельности на предприятиях инфокоммуникационных технологий и систем связи учебник для студентов учреждений СПО/.-М.: Академия, 2018
6. Белов Е.Б., Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности : учебное пособие для студентов учреждений СПО/ Белов Е.Б., Пржегорлинский В.Н.-М.: Академия, 2018
7. Коваленко Ю.И. Методика защиты информации в организациях : монография / Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин. — М.: Русайнс, 2018. — 162 с
8. Защита информационных технологий. Справочник : справочник / Ю.И. Коваленко. — Москва : Русайнс, 2018. — 321 с
9. Зверева В. П., Назаров А. В. Организация и технология работы с конфиденциальными документами: учебник.-М.: КУРС: Инфра-М., 2018
10. Шевцова Г.А. Организация и технология работы с конфиденциальными документами (1-е изд.) учеб. пособие.-М.: Академия, 2018
11. Курилова А.В. Хранение, передача и публикация цифровой информации (3-е изд.) учебник
12. Кравченко В.Б. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении (1-е изд.) учеб. пособие-М.: Академия, 2018