ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КИРОВСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФГБОУ ВО Кировский ГМУ Минздрава России)

Центр дополнительного образования

УТВЕРЖДАЮ
Руководитель ЦДО _____ С.В. Глушкова
«09» февраля 20 22 г.

Рабочая программа учебной дисциплины

«Меры по защите информации (защите персональных данных)»

для дополнительной профессиональной программы профессиональной переподготовки

«Специалист по оказанию государственных услуг в области занятости населения»

Киров, 20 22 г.

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Пояснительная записка.

Актуальность учебной дисциплины «Меры по защите информации (защите персональных данных)» объясняется тем, что в последнее время вырос интерес к вопросам защиты информации. Это связывают с тем, что стали более широко использоваться вычислительные сети, что приводит к тому, что появляются большие возможности для несанкционированного доступа к передаваемой информации.

Цель: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи учебной дисциплины:

- освоить основные положения в области защиты персональных данных;
- сформировать умения обеспечить защиту информации и объектов информатизации;
- сформировать навыки обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия.

Компетенции обучающихся, формируемые, а также подлежащие совершенствованию в результате освоения дисциплины / модуля.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Готовность содействия гражданам в поиске подходящей работы (ПК-1).

знать: нормативные правовые акты в области содействия занятости населения федерального и регионального уровней, в области профессионального образования и социальной защиты инвалидов, административные регламенты; региональные программы содействия занятости населения; особенности рынка труда и потребность в кадрах; требования по защите персональных данных при обработке информации; Правила межличностного общения, этика делового общения и межкультурной коммуникации, особенности общения с инвалидами; правила и порядок ведения делопроизводства и электронного документооборота (далее – ЭДО), порядок и сроки представления отчетности;

уметь: оказывать госуслуги по трудоустройству инвалидам с учетом требований законодательства Российской Федерации о социальной защите инвалидов; использовать в работе данные мониторинга рынка труда, информацию о рабочих местах, размещаемую в системе «Работа в России», в средствах массовой информации (далее – СМИ) и в информационно-телекоммуникационной сети «Интернет»; учитывать в общении с гражданами их социально-психологические особенности, в том числе имеющиеся у инвалидов ограничения; вести документацию и служебную переписку в соответствии с требованиями руководящих документов, регламентирующих деятельность ЦЗН, правил и порядка ведения делопроизводства;

иметь навыки и (или) опыт деятельности: владеть способностью поиска вакансий, подбора и предложения вариантов подходящей работы заявителю при

личном обращении или с использованием электронных средств коммуникации; организация сопровождения при содействии занятости инвалидов, нуждающихся в данном сопровождении;

Способность к оказанию психологической поддержки безработным (ПК-2).

знать: категории и характеристики граждан – получателей услуг ЦЗН, основные типы их проблем и возрастные особенности развития личности; методы и методики социальной психологии; технологии психологического консультирования; методы организации и проведения психодиагностики, психологического тестирования и психологического тренинга; требования по защите персональных данных при обработке информации; правила и порядок ведения делопроизводства и ЭДО, порядок и сроки представления отчетности;

уметь: подбирать эффективные формы и методы психологической поддержки в соответствии с выявленными проблемами граждан; проводить индивидуальные или групповые психологические занятия и тренинги для решения проблем граждан; применять разные виды и методы психологического консультирования в соответствии с возрастом, полом и особенностями ситуации граждан; учитывать в общении с гражданами их социально-психологические особенности, в том числе имеющиеся у инвалидов ограничения; вести документацию и служебную переписку в соответствии с требованиями руководящих документов, регламентирующих деятельность ЦЗН, правил и порядка ведения делопроизводства;

иметь навыки и (или) опыт деятельности: владеть способностью подбора комплекса психологических методик, планирования и проведения обследования безработных граждан; владеть способностью психологического тестирования (анкетирования) безработных граждан, в том числе с использованием электронных средств коммуникации; владеть способностью проведения диагностических бесед с безработными гражданами для выявления основных проблем, препятствующих их трудоустройству; владеть навыком ведения личных дел получателей услуг на различных носителях информации, подготовка дел к сдаче в архив и их хранение;

Способность мониторинга рынка труда, потребности в кадрах и качества оказываемых госуслуг (ПК-3).

знать: состав показателей, характеризующих ситуацию на рынке труда, методология их формирования и источники получения; особенности рынка труда и потребность в кадрах, современные тенденции и направления развития рынка труда; правила межличностного общения, этика делового общения и межкультурной коммуникации; требования по защите персональных данных при обработке информации; правила и порядок ведения делопроизводства и ЭДО, порядок и сроки представления отчетности;

уметь: собирать и обрабатывать статистическую информацию о ситуации на рынке труда; проводить статистический анализ данных мониторинга; использовать в работе данные мониторинга рынка труда, информацию о вакантных рабочих местах, размещаемую в системе «Работа в России, в СМИ и в информационно-телекоммуникационной сети «Интернет»;

– *иметь навыки и (или) опыт деятельности:* владеть навыком проведения мониторинга ситуации на рынке труда; владеть навыком сбора и систематизации

информации (сведений) о соискателях на портале системы «Работа в России»; владеть навыком сбора информации о созданных рабочих местах для инвалидов и об их трудоустройстве, формирования базы вакансий; владеть навыком мониторинг трудоустройства граждан и их удовлетворенности полнотой и качеством предоставленных госуслуг.

1.2. Содержание учебной дисциплины.
Объем учебной дисциплины и виды учебной работы

Виды учебной работы	Часов
Трудоемкость, всего	22
Аудиторные занятия, в том числе:	4
Лекции	2
Практические занятия	2
Самостоятельная работа	18

Тема 1. Основы информационной безопасности и защиты информации.

Основные понятия и определения. Современное состояние и перспективы развития защиты информации. Принципы организации системы защиты, политика информационной безопасности, направления, способы и методы защиты.

Тема 2. Нормативно-правовая база информационной безопасности.

Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций. Виды тайн и законодательство по ограничениям оборота информации, относимой к различным тайнам.

Тема 3. Виды и особенности угроз информационной безопасности. Каналы утечки информации.

Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Предпосылки и причины. Понятие и классификация каналов утечки информации. Характеристика каждого канала. Классификация каналов.

Тема 4. Организационные основы защиты информации организации.

Понятие, цели и задачи системы защиты информации. Принципы построения системы, её технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принципы надёжности и превентивности

1.3. Перечень основной и дополнительной литературы.
Основная литература.

1. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.

2. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

Дополнительная литература.

3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

4. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.

5. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

Ресурсы

Информационные справочные системы, Интернет-ресурсы (электронные образовательные ресурсы)

1. Электронно-библиотечная система Университета;
2. Образовательный сайт Кировского ГМУ (http://student.kirovgma.ru);
3. Платформа для создания и проведения онлайн вебинаров, видеокурсов, тестов и опросов Pruffme. com

2. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

2.1. Методические рекомендации для преподавателя

При подготовке и проведении занятий преподавателю необходимо соблюдать следующие рекомендации:

– к каждому аудиторному занятию преподаватель готовит пакет дидактических материалов в электронном и/или текстовом варианте;

– аудиторные занятия сопровождает мультимедийными презентациями;

– аудиторные занятия проводит в интерактивном режиме, с использованием приемов современных образовательных технологий;

– в процессе обучения предлагает обучающимся задания для самостоятельной работы по углублению и расширению знаний, для формирования и совершенствования умений и практических навыков, обеспечивающих качественное усвоение учебного материала.

При подготовке к практическому занятию преподавателю необходимо уточнить план его проведения, продумать формулировки и содержание учебных вопросов, выносимых на обсуждение, ознакомиться с новыми публикациями по теме занятия и составить список обязательной и дополнительной литературы по вопросам плана занятия. Оказывать методическую помощь обучающимся в подготовке докладов, планов и презентаций.

В ходе практического занятия во вступительном слове раскрыть теоретическую и практическую значимость темы занятия, определить порядок его проведения, время на обсуждение каждого учебного вопроса. Дать возможность выступить всем желающим. Целесообразно в ходе обсуждения учебных вопросов задавать выступающим и аудитории дополнительные и уточняющие вопросы с целью выяснения их позиций по существу обсуждаемых проблем. Поощрять выступления с места в виде кратких дополнений и постановки вопросов

выступающим и преподавателю. Для наглядности и закрепления изучаемого материала преподаватель может использовать модели, таблицы, схемы, карты, мультимедийные презентации, видеофильмы.

В заключительной части практического занятия следует подвести его итоги: дать объективную оценку выступлений каждого обучающегося и учебной группы в целом. Раскрыть положительные стороны и недостатки проведенного практического занятия. Ответить на вопросы обучающихся. Назвать тему очередного занятия.

Проводить групповые и индивидуальные консультации обучающихся, рекомендовать в помощь учебные и другие материалы, а также справочную литературу.

2.2. Методические указания для обучающихся

В процессе обучения обучающимся необходимо выяснить:

- цели и конечный результат обучения по программе;
- основные требования к уровню усвоения содержания программы;
- виды учебной работы.

Обучение осуществляется в соответствии с методическими указаниями, действующей программой, нормативно-правовыми документами и учебной литературой.

В процессе реализации программы необходимо посещать практические занятия с целью углубления и расширения знаний, для формирования и совершенствования умений и практических навыков, обеспечивающих качественное усвоение учебного материала.

При подготовке к практическим, семинарским занятиям, обучающимся рекомендуется использовать учебную и справочную литературу.

В процессе обучения осваивать рекомендованную литературу, самостоятельно находить книги, публикации и информационные материалы по изучаемым темам, использовать Интернет-сайты. Во время учебных занятий задавать преподавателям дополнительные вопросы.

Каждому обучающемуся необходимо быть готовым к контролю текущей успеваемости. Форму текущего контроля определяет преподаватель.

2.3. Методические рекомендации по организации самостоятельной работы обучающихся

Самостоятельная работа включает изучение материала лекций, вебинаров, литературы, предоставляемых преподавателем, вынесенных на самостоятельное изучение, подготовку к зачет.

2.4.Контроль и оценка результатов обучения

Форма контроля – зачет по учебной дисциплине.

Оценочное средство – тест.

Материалы оценочного средства:

Примерный перечень вопросов для проведения зачета

1. Персональные данные – это:

А) совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Б) персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом;

В) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2. Персональные данные, разрешенные субъектом персональных данных для распространения – это:

А) персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом;

Б) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

В) совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Оператор – это:

А) коммерческая организация самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Б) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

В) общественная организация самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

4. Обработка персональных данных – это:

А) обработка персональных данных с помощью средств вычислительной техники;

Б) ручная обработка персональных данных;

В) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5. Автоматизированная обработка персональных данных – это:

А) обработка персональных данных с помощью средств вычислительной техники;

Б) любое действие (операция) или совокупность действий (операций), совершаемых оператором;

В) ручная обработка персональных данных.

6. Распространение персональных данных – это:

А) А) действия, направленные на раскрытие персональных данных определенному кругу лиц;

Б) действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

В) передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

7. Предоставление персональных данных – это:

А) действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Б) передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

В) действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

8. Блокирование персональных данных – это:

А) временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Б) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

В) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

9. Уничтожение персональных данных – это:

А) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Б) временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

В) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

10. Обезличивание персональных данных – это:

А) временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Б) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

В) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

11. Информационная система персональных данных – это:

А) любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных;

Б) совокупность взаимосвязанных частей (элементов), каждая из которых предназначена для выполнения определённых полезных функций;

В) совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

12. Трансграничная передача персональных данных – это:

А) передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Б) передача персональных данных местному органу власти федеральным органом;

В) передача персональных данных органу федеральному власти органом местного самоуправления.

13. Обработке подлежат только персональные данные, которые:

А) отвечает запросам граждан;

Б) отвечает запросам общества;

В) отвечают целям их обработки.

14. При обработке персональных данных должны быть обеспечены:

А) конфиденциальность и пунктуальность;

Б) точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

В) раскрытие персональных данных определенному кругу лиц.

15. Обработка персональных данных не допускается в следующих случаях:

А) обработка персональных данных осуществляется без согласия субъекта персональных данных на обработку его персональных данных;

Б) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

В) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

16. Может ли быть отозвано субъектом персональных данных согласие на обработку персональных данных?

А) может;

Б) не может;

В) на усмотрение оператора.

17. Обработка специальных категорий персональных данных касается:

А) даты рождения, образования, места жительства;

Б) расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

В) даты рождения, места жительства, места работы, социального статуса.

18. Биометрические персональные данные – это:

А) сведения, которые характеризуют внешний вид человека;

Б) сведения, которые характеризуют гражданина с точки зрения социального статуса;

В) сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

19. Обеспечение безопасности персональных данных достигается:

А) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

Б) применением прошедших в установленном порядке процедуру оценки несоответствия средств защиты информации;

В) отсутствием контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

20. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в государственных информационных системах персональных данных осуществляются:

А) федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных;

Б) федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных;

В) федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

21. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан:

А) осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки;

Б) осуществить правомерно обработка персональных данных, относящихся к этому субъекту персональных данных;

В) обработка персональных данных другим лицом, действующим по поручению оператора.

22. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан:

А) блокировать обрабатываемые персональные данные, относящихся к этому субъекту персональных данных;

Б) передать обработку персональных данных третьему лицу;

В) уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

23. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора в срок, не превышающий:

А) одного рабочего дня с даты этого выявления;

Б) трех рабочих дней с даты этого выявления;

В) пять рабочих дней с даты этого выявления.

24. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

А) в течение двенадцати часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

Б) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных

данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

В) в течение сорока восьми часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом.

25. Информация в зависимости от категории доступа к ней подразделяется на:

А) открытую и скрытую информацию;

Б) гражданскую и военную информацию;

В) общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Разработчики программы:

Колесова Ю.А., специалист по УМР ЦДО
Ложкин Валерий Васильевич, преподаватель ЦДО