Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Информзащита»

УТВЕРЖДАЮ

Директор АНО ДПО «Учебный центр «Информзащита»

_____ / Степаненко А.А. /
*(подпись)*

«__11__» _____2017 г.

*М.П*

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

# «КОМПЛЕКСНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

Сокращенное наименование: «КЗПДН»

Код: КП323

Москва
2017

## СОДЕРЖАНИЕ

# 1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая программа повышения квалификации «Комплексная защита персональных данных» (далее – «Программа») относится к дополнительным профессиональным программам в области информационной безопасности (далее - ИБ) и разработана с учетом положений:

- Федерального закона от 29 декабря 2012 г. № 273-03 «Об образовании в Российской Федерации»;
- Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499);
- Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);
- Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденных ФСТЭК России 4 апреля 2015 г.;
- Методических рекомендаций-разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 г. № ВЖ-1032/06);

Программа сформирована с учётом видов профессиональной деятельности, трудовых функций и уровней квалификации, установленных в профессиональных стандартах:

- «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15 сентября 2016 г. № 522н;
- «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 598н;

При разработке содержания Программы учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего образования (ФГОС ВО) по направлению подготовки «Информационная безопасность», а именно:

- ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1509;

Программа повышения квалификации реализуется в АНО ДПО «Учебный центр «Информзащита».

Программа разработана в инициативном порядке в соответствии с Приказом Директора АНО ДПО «Учебный центр «Информзащита» от «17» января 2017 г. №02/01/17.

Программа обсуждена и одобрена на заседании Методического совета АНО ДПО «Учебный центр «Информзащита» «11» мая 2017 г., протокол № 5 и утверждена Приказом Директора от «11» мая 2017 г. № 01/05/17.

Разработчики:

- Журавлёв Владимир Владимирович, заведующий кафедрой юридических проблем защиты конфиденциальной информации;
- Емельянников Михаил Юрьевич, внешний эксперт;
- Ершов Дмитрий Вячеславович, к.т.н., заместитель директора по учебно-методической работе;
- Лепихин Владимир Борисович, заведующий кафедрой сетевой безопасности.

## 2. ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Целью реализации Программы является повышение профессионального уровня обучающихся (слушателей) в рамках имеющейся квалификации, формирование и (или) совершенствование у них компетенций, необходимых для выполнения трудовых функций (должностных обязанностей) в рамках профессиональной деятельности по защите персональных данных и обеспечению безопасности ИСПДн, построенных на базе компьютерных систем и сетей.

Программа направлена на формирование у слушателей знаний и умений по всему комплексу проблем организации обработки и защиты персональных данных в ИСПДн в соответствии с требованиями российского законодательства. Особое внимание уделяется формированию у них умений, необходимых для построения систем технической защиты персональных данных в ИСПДн с использованием правовых, организационных и технических мер в соответствии с методиками ФСБ России, ФСТЭК России.

### 2.1 Характеристика вида профессиональной деятельности

а. **Область профессиональной деятельности** слушателей, обучающихся по Программе, включает сферы техники и технологий, охватывающие совокупность проблем, связанных с:
- защитой персональных данных в автоматизированных информационных системах и обеспечением их безопасности в условиях существования угроз в информационной сфере;
- анализом, оценкой и обеспечением требуемого уровня защищенности ИСПДн от вредоносных программно-технических воздействий;
- эксплуатацией и администрированием средств и систем защиты информации ИСПДн.

**б. Объекты профессиональной деятельности:**
- объекты информатизации, включающие автоматизированные информационные системы (ИСПДн), входящие в них средства обработки, хранения и передачи информации и информационно-технологические ресурсы, подлежащие защите и функционирующие в условиях существования угроз в информационной сфере;
- угрозы безопасности и технологии обеспечения информационной безопасности ИСПДн;
- системы управления информационной безопасностью ИСПДн;
- методы и реализующие их средства защиты информации в ИСПДн;
- процессы, возникающие при защите информации, обрабатываемой в ИСПДн;
- методы и реализующие их системы и средства контроля эффективности защиты информации в ИСПДн;

– система нормативных правовых актов, методических документов и национальных стандартов в области информационной безопасности (защиты персональных данных).

**в. Виды профессиональной деятельности и решаемые задачи**

Программа ориентирована на подготовку слушателей к следующим видам профессиональной деятельности:

организационно-управленческая;

проектная;

контрольно-аналитическая.

Слушатели, успешно завершившие обучение по данной Программе, должны решать следующие задачи в соответствии с видами профессиональной деятельности:

**в организационно-управленческой деятельности:**

- организация работ по выполнению требований режима защиты информации, в том числе персональных данных;
- осуществление организационно-правового обеспечения информационной безопасности ИСПДн;
- разработка нормативных и методических документов и иных организационно-распорядительных документов, регламентирующих работу по защите информации в ИСПДн;
- участие в определении потребности в средствах защиты информации в ИСПДн, контроль их поставки и эксплуатации;

**в проектной деятельности:**

- сбор и анализ исходных данных для проектирования систем защиты ИСПДн;
- определение угроз безопасности ИСПДн на объектах информатизации и рисков от их реализации;
- формирование требований к обеспечению безопасности информации в ИСПДн;
- разработка предложений по применению конкретных способов, методов и программно-аппаратных средств обеспечения безопасности информации и иных ресурсов в ИСПДн;
- поиск рациональных решений при выборе средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения.

**в контрольно-аналитическая деятельности:**

- контроль эффективности реализации политики информационной безопасности ИСПДн;
- участие в обследовании ИСПДн на объектах информатизации, их категорировании и аттестации по требованиям безопасности информации.

## 3. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

Лица, желающие освоить Программу, должны иметь высшее образование, или получать высшее образование (проходить обучение в настоящее время), при условии, что они получат дипломы о первичном образовании в период прохождения обучения по Программе. Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования, предоставляя копии и предъявляя документы об образовании государственного или установленного образца.

Поступающим на обучение желательно иметь стаж работы (не менее 1 года), связанной с процессами обеспечения информационной безопасности в компаниях или организациях, или связанного с внедрением и эксплуатацией автоматизированных информационных (компьютерных) систем.

## 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

### 4.1 Приобретаемые профессиональные компетенции

Процесс освоения обучающимися данной Программы направлен на формирование и (или) совершенствование у них следующих компетенций:

способность организовывать и проводить работы по обеспечению безопасности персональных данных;

способность проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

способность определять уровни защиты персональных данных;

способность обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;

способность определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокировки угроз безопасности персональных данных.

В результате освоения Программы обучающиеся должны получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для нового вида профессиональной деятельности.

Обучающиеся, освоившие учебную дисциплину (модуль, курс), должны:

**знать:**

- правовые основы организации защиты персональных данных, основные требования нормативных правовых актов и методических документов ФСБ России, ФСТЭК России и Роскомнадзора России по защите персональных данных;
- требования к организации обработки персональных данных на всех стадиях жизненного цикла от их сбора до уничтожения;
- порядок оценки правомерности обработки персональных данных, соответствия объема обрабатываемых данных заранее предопределенным целям;
- критерии и порядок определения уровня защищенности (классификации) ИСПДн;

- приёмы оптимизации состава ПДн и процессов их обработки (реинжениринга ИСПДн);
- современные методы снижения рисков нарушения конфиденциальности, целостности и доступности персональных данных с использованием правовых, организационных и технических мер защиты информации;
- основные этапы работ по реализации комплексной системы защиты персональных данных (правовых, организационных и технических мер) и приведению ИСПДн в соответствие требованиям российского законодательства по защите ПДн;
- требования к составу и характеристикам подсистем защиты для различных уровней защищенности ИСПДн, методы их практической реализации;
- правовые нормы по сертификации средств защиты информации, технического обслуживания СКЗИ, лицензионные требования ФСТЭК России и ФСБ России к деятельности в области обеспечения защиты информации ограниченного доступа;
- нормативную базу для формирования моделей угроз безопасности ПДн и моделей нарушителей в ИСПДн;
- требования к реализации организационно-технических мер защиты ПДн в ИСПДн в зависимости от уровней защищенности ИСПДн;
- общий порядок организации обеспечения безопасности ПДн в ИСПДн. проектирования СЗПДн и организации физической защиты;
- структуру, состава и основных функций СЗПДн, обязательные подсистемы и механизмы защиты;
- возможные технические каналы утечки ПДн при их обработке, состав мероприятий по защите ПДн от утечки по техническим каналам для различных классов ИСПДн;
- порядок проведения работ по развёртыванию СЗПДн и настройке ее элементов в ИСПДн, испытаний и опытной эксплуатации СЗПДн;
- организацию системы государственного контроля и надзора в сфере персональных данных.
- примеры из судебной практики и практики прохождения проверок, включая наложение штрафных санкций со стороны государственных надзорных органов и выдачу предписаний на устранение нарушений.

**уметь:**

- правильно определять цели обработки персональных данных, категории субъектов, чьи данные обрабатываются на предприятии (в организации), и состав обрабатываемых персональных данных;
- осуществлять сбор, анализ и документирование исходных данных по ИСПДн, необходимых для, выявления ИСПДн, описание технологий обработки и защиты ПДн, классификации ИСПДн, определения исходной защищённости ИСПДн, определения требуемого уровеня защищенности ИСПДн;
- готовить уведомления в уполномоченный орган по защите прав субъектов персональных данных,
- оценивать типы актуальных угроз безопасности персональных данных и уровни их защищенности;

- формировать частную актуальную модель угроз персональным данным и модель нарушителей на основании нормативно-методических документов ФСТЭК России и ФСБ России;
- планировать защиту персональных данных в ИСПДн с использованием организационных мер, программных и аппаратных средств защиты;
- строить систему технической защиты ПДн в соответствии с требованиями законодательства, а также ФСТЭК России и ФСБ России;
- обоснованно выбирать необходимые меры по обеспечению безопасности персональных данных и программные и программно-аппаратные средства защиты;
- определять перечень предполагаемых к использованию сертифицированных средств защиты информации и их настроек.
- планировать организационные мероприятия по защите ПДн;
- готовить внутренние организационно-распорядительные документы по организации защиты ПДн и эксплуатации СЗПДн в ИСПДн;
- готовить ИСПДн к проверке на соответствие требованиям по безопасности.
- представлять интересы предприятия (организации) при проведении мероприятий государственного контроля и надзора.

в) **владеть навыками:**

- работы с действующей нормативной правовой и методической базой в области обработки и защиты персональных данных;
- выявления и оценки угроз безопасности персональных данных;
- определения задач, проведения организационных и технических мероприятий по защите ИСПДн.

## 5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

### 5.1 Особенности организации учебного процесса

Обучение по Программе осуществляется единовременно (без разрывов), в порядке, определённом образовательной программой на основе договоров об обучении. Форма обучения и конкретные сроки освоения Программы определяются с учётом расписания курсов в Учебном центре и указываются в договоре об обучении.

При использовании дистанционных образовательных технологий (онлайн-вебинаров) слушатели из других часовых поясов должны учитывать, что занятия с онлайн-трансляцией (онлайн-вебинары) проводятся по рабочим дням с 10:00 до 17:30 по московскому времени. При наличии групп слушателей из удалённых регионов (одного или смежных часовых поясов) для них занятия могут быть проведены в иное, специально назначенное для этого, время (с учётом сдвига по времени).

Доступ к электронным учебным пособиям, к системе тестирования, а также к стендам (виртуальным машинам в центре обработки данных - ЦОД) для дистанционного выполнения лабораторных (практических) работ должен предоставляется слушателям

круглосуточно.

Предоставление прав и реквизитов удалённого доступа обучающихся к их «личным кабинетам» и назначенным им курсам и тестам целесообразно осуществлять на весь период обучения по Программе. Контроль за прохождением этапов обучения слушателей должен вестись как лицами, ответственными за СДО и обеспечение проведения занятий с применением дистанционных технологий, и преподавателями, ведущими занятия, так и менеджерами, отвечающими за договора об обучении конкретных слушателей.

### 5.2 Порядок передачи Программы другой образовательной организации

Передача Учебным центром настоящей дополнительной профессиональной программы другим образовательным организациям не предусматривается.

Передача Программы повышения квалификации другой образовательной организации допускается при создании необходимых условий её реализации и соблюдении требований законодательства Российской Федерации о порядке обращения со служебной информацией ограниченного распространения и наличии разрешения органов управления, в ведении которых находятся организации, осуществляющие образовательную деятельность.

### 5.3 Порядок внесения изменений в Программу

Внесение изменений в настоящую дополнительную профессиональную программу осуществляются в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования, защиты государственной тайны и информационной безопасности.

Перечень основной литературы может дополняться при поступлении новых (уточненных) учебных пособий.

Перечень дополнительной литературы подлежит обновлению и (или) уточнению, с учетом введения в действие новых и утративших актуальность нормативных правовых актов и методических документов.

Незначительные правки, вызванные изменениями в нормативной базе или в составе учебных дисциплин (модулей, курсов) вносятся в рабочем порядке.

Существенные изменения в программу рассматривается Методическим советом Учебного центра, а сама Программа повторно утверждается директором Учебного центра и проходит процедуру согласования в установленном порядке.

# 6. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

## 6.1 Оценка качества освоения Программы

Система оценки качества освоения Программы включает текущий контроль успеваемости (контроль посещаемости и активности на занятиях, опросы в начале очередного учебного дня, контроль выполнения практических и лабораторных работ), промежуточные по завершении освоения каждой учебной дисциплины (модуля, курса) Программы и итоговую аттестацию обучающихся.

Освоение каждой дисциплины (модуля, курса) Программы завершается зачетом (без оценки) в форме теста, который подразумевает ответы на контрольные вопросы по материалу курса. Зачет проводится с использованием электронной системы тестирования (основной вариант) или в бумажной форме (резервный вариант). Зачет принимает преподаватель, ведущий занятия по данной дисциплине.

Если краткосрочная программа повышения квалификации состоит только из одной учебной дисциплины (курса, модуля), то для неё промежуточная аттестация по дисциплине (курсу, модулю) является одновременно и итоговой по Программе.

Для каждого теста разработана система оценки, параметрами которой являются количество вопросов, их сложность, полнота ответа на вопрос. По результатам ответа на вопрос испытуемому присваивается определенное системой оценки количество баллов. Итоговое решение о прохождении теста принимается на основании превышения суммарно набранного количества баллов по всем вопросам над определенным системой оценки пороговым значением.

По результатам успешного тестирования и собеседования по каждому слушателю оформляется отдельное решение о прохождении (не прохождении) итоговой аттестации. В случае неуспешной попытки сдачи итогового теста, слушателю предоставляется время на самоподготовку и возможность повторно пройти тестирование.

Лицам, успешно освоившим Программу повышения квалификации, выполнившим все требования учебного плана и прошедшим итоговую аттестацию, выдается Удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговой аттестации или показавшим на итоговой аттестации неудовлетворительные результаты, а также слушателям, освоившим лишь часть Программы и/или отчисленным из организации, выдается справка об обучении (а также Свидетельства о прохождении обучения по отдельным модулям (курсам) Программы).

При освоении Программы слушателем параллельно с получением высшего образования Удостоверение о повышении квалификации выдаётся ему после получения соответствующего документа об основном образовании и о квалификации.

# 7. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ

## 7.1 Категории обучающихся

Программа ориентирована на следующие категории обучающихся (слушателей):

- начальники служб безопасности, руководители подразделений обеспечения информационной безопасности (ОИБ), технической защиты (конфиденциальной) информации (ТЗИ, ТЗКИ), ответственные за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий;
- аналитики подразделений ОИБ (ТЗКИ), отвечающие за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем ИС и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- администраторы средств защиты и специалисты подразделений ОИБ (ТЗКИ), ответственные за защиту конфиденциальной информации техническими средствами.

## 7.2 Формы обучения

Программа реализуется в форме обучения с отрывом от основной работы при проведении обучения в очной форме, - с частичным отрывом от работы, при обучении с использованием дистанционных образовательных технологий (онлайн-вебинаров) и/или электронного обучения.

## 7.3 Продолжительность (трудоёмкость) обучения

Общий объём времени, отводимого на освоение данной Программы, составляет 48 часов, включая 40 академических часов аудиторных занятий (включая зачёты) и 8 академических часов самостоятельной учебной работы слушателя.

## 7.4 Режим занятий

Режим занятий: 8 академических часов учебных (аудиторных) занятий с преподавателем и 1 час самостоятельной работы в день.

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Учебные занятия организованы в одну смену. Время проведения очных занятий и онлайн-вебинаров - по рабочим дням с 10:00 до 17:30 по московскому времени. Доступ к электронным учебным пособиям и виртуальным стендам (в центре обработки данных - ЦОД) для дистанционного выполнения лабораторных работ предоставляется слушателям круглосуточно.

### 7.5 План учебного процесса

| №№ п/п | Наименование учебных модулей, разделов (тем) | Всего учебных часов | Часы занятий с преподавателем | Распределение времени по видам занятий, час | | | | | Самостоятельная работа обучающихся | Формы аттестации и контроля знаний |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Лекции | Семинары | Практические занятия | Лабораторные работы | Промежуточная аттестация | | |
| | **Модуль 1. Защита персональных данных** | **18** | **16** | **15** | | | | **1** | **2** | Опрос на лекции |
| 1. | Введение. Персональные данные в организации (на предприятии) | 1,5 | 1 | 1 | | | | | 0,5 | |
| 2. | Основные положения Федерального закона «О персональных данных» | 2,5 | 2 | 2 | | | | | 0,5 | |
| 3. | Работа с персональными данными на предприятии (в организации) | 4,5 | 4 | 4 | | | | | 0,5 | |
| 4. | Техническая защита персональных данных в информационных системах | 3 | 3 | 3 | | | | | | |
| 5. | Лицензирование деятельности по технической защите конфиденциальной информации | 1 | 1 | 1 | | | | | | |
| 6. | Аутсорсинг систем технической защиты персональных данных | 1 | 1 | 1 | | | | | | |
| 7. | Регулирование отношений в области организации и осуществления государственного контроля и надзора. | 3,5 | 3 | 3 | | | | | 0,5 | |

| №№ п/п | Наименование учебных модулей, разделов (тем) | Всего учебных часов | Часы занятий с преподавателем | Распределение времени по видам занятий, час | | | | | Самостоятельная работа обучающихся | Формы аттестации и контроля знаний |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Лекции | Семинары | Практические занятия | Лабораторные работы | Промежуточная аттестация | | |
| | **Модуль 2. Техническая защита персональных данных** | **28** | **24** | **20** | | **3** | | **1** | **4** | Опрос на лекции |
| 8. | **Введение** | 1 | 1 | 1 | | | | | | |
| 9. | **Тема 1.** Основные этапы работ по обеспечению безопасности ПДн в ИСПДн | 1,5 | 1 | 1 | | | | | 0,5 | |
| 10. | **Тема 2.** Сбор и анализ исходных данных по ИСПДн | 1,5 | 1 | 1 | | | | | 0,5 | |
| 11. | **Тема 3.** Классификация информационных систем персональных данных (определение уровня защищенности) | 3,5 | 3 | 2 | | 1 | | | 0,5 | |
| 12. | **Тема 4.** Формирование модели угроз ПДн и модели нарушителей | 3,5 | 3 | 2 | | 1 | | | 0,5 | |
| 13. | **Тема 5.** Разработка (проектирование) системы защиты персональных данных (СЗПДн) | 8,5 | 8 | 7 | | 1 | | | 0,5 | |
| 14. | **Тема 6.** Разработка и внедрение организационных мер и организационно-распорядительных документов по обеспечению ЗПДн | 2,5 | 2 | 2 | | | | | 0,5 | |
| 15. | **Тема 7.** Развертывание, настройка и опытная | 1,5 | 2 | 1 | | | | | 0,5 | |

| №№ п/п | Наименование учебных модулей, разделов (тем) | Всего учебных часов | Часы занятий с преподавателем | Распределение времени по видам занятий, час | | | | | Самостоятельная работа обучающихся | Формы аттестации и контроля знаний |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Лекции | Семинары | Практические занятия | Лабораторные работы | Промежуточная аттестация | | |
| | эксплуатация СЗПДн в ИСПДн | | | | | | | | | |
| 16. | **Тема 8.** Закрытие технических каналов утечки ПДн в ИСПДн | 2 | 2 | 2 | | | | | | |
| 17. | **Тема 9.** Лицензирование деятельности по защите ПДн в ИСПДн | 1,5 | 1 | 1 | | | | | 0,5 | |
| | **Итоговое тестирование** | 2 | | | | | | 2 | | Зачёт в форме тестирования |
| | **Итого:** | **48** | **38** | **36** | | **2** | | **2** | **8** | |

### 7.6 Сводные данные по бюджету времени

| Общий объем времени, отводимого на освоение программы (календарных дней/часов) | | | Распределение учебного времени (количество часов) | | | | | |
|---|---|---|---|---|---|---|---|---|
| Всего | Из них | | Всего часов учебных занятий | В том числе | | Время на самостоятельную работу | Итоговая аттестация | Резерв учебного времени |
| | Выходные, праздничные дни | Учебное время | | Учебные занятия по расписанию | Практика | | | |
| **6/48** | **0** | **6/48** | **48** | **38** | **-** | **8** | **2** | **-** |

## 8. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

| | | |
|---|---|---|
| Срок обучения по программе повышения квалификации, месяцы | 1 | |
| Срок обучения по программе повышения квалификации, недели | 1 | |
| Виды занятий, предусмотренные программой повышения квалификации | А | И |

А – аудиторная и самостоятельная работа

И – Итоговая аттестация

# 9. РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА

## 9.1 Содержание учебных разделов (модулей, тем)

### Модуль 1. Защита персональных данных

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.
2. **Основные положения Федерального закона «О персональных данных»**
   - Основные понятия. Персональные данные в Федеральном законе и Трудовом кодексе РФ. Содержание категории «персональные данные».
   - Область применения закона. Ограничения.
   - Соотношение с другими категориями тайн. Персональные данные и их взаимосвязь с государственной, коммерческой, налоговой, банковской, адвокатской тайной, тайной связи и другими категориями конфиденциальных сведений.
   - Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.
   - Принципы обработки персональных данных.
   - Условия обработки персональных данных. Согласие субъекта. Обработка биометрических данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных.
   - Специальные категории персональных данных и особенности их обработки.
   - Права субъектов персональных данных и их соблюдение при обработке.
   - Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов.
   - Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
   - Контроль и надзор за обработкой персональных данных.
   - Ответственность за нарушение требований по обращению с персональными данными.
3. **Работа с персональными данными на предприятии (в организации)**
   - Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы. Меры по охране конфиденциальности.
   - Формирование перечня персональных данных
   - Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением. Организация доступа к персональным данным. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие. Контроль за соблюдением режима конфиденциальности.

- Общие сведения о конфиденциальном делопроизводстве.
- Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

4. **Техническая защита персональных данных в информационных системах**
   - Требования Федерального закона и Постановления Правительства РФ № 1119 от 01.11.2012 к обеспечению безопасности персональных данных. Обязательные механизмы защиты.
   - Классификация (определение уровня защищенности) информационных систем персональных данных.
   - Модель угроз персональным данным.
   - Режим обеспечения безопасности персональных данных.
   - Каналы утечки информации при обработке персональных данных в информационных системах.
   - Система защиты персональных данных и ее описание.
   - Предотвращение несанкционированного доступа к персональным данным и обнаружение фактов такого доступа.
   - Регистрация запросов пользователей к информационным системам персональных данных.
   - Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
   - Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.
   - Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Разбирательство нарушений системы безопасности.
5. **Лицензирование деятельности по технической защите конфиденциальной информации**
   - Понятие технической защиты как лицензируемого вида деятельности.
   - Лицензионные требования.
   - Проверка сведений о лицензиате и лицензионный контроль.
   - Ответственность за незаконную деятельность в области защиты информации.
   - Незаконное предпринимательство.
6. **Аутсорсинг систем технической защиты персональных данных**
7. **Регулирование отношений в области организации и осуществления государственного контроля и надзора.**
   - Организация проверки органами государственного контроля и надзора.
   - Порядок проведение проверки.
   - Оформление результатов проверки.
8. **Промежуточный контроль знаний** (в форме зачета)

**Модуль 2. Техническая защита персональных данных**

9. **Введение**
   - Нормативная база организации технической защиты персональных данных. Государственные органы, осуществляющие контроль и надзор в данной сфере деятельности (Роскомнадзор России, ФСБ России, ФСТЭК России, Минкомсвязи России). Ответственность операторов ПДн за невыполнение требований по обеспечению безопасности ПДн при их обработке в ИСПДн.
10. **Тема 1. Основные этапы работ по обеспечению безопасности ПДн в ИСПДн**
    - Перечень основных этапов работ и краткий обзор мероприятий, необходимых для приведения ИСПДн в соответствие требованиям российского законодательства по защите ПДн.
11. **Тема 2. Сбор и анализ исходных данных по ИСПДн**
    - Обследование информационных систем с целью выявления фактов обработки ПДн, форм представления ПДн, целей и законности обработки, способов, сроков и объёмов их обработки, источников получения и др. Формирование перечня ПДн и выделение сегментов ИСПДн.
    - Сбор, анализ и документирование исходных данных по ИСПДн, необходимых для: выявления ИСПДн; классификации ИСПДн; определения исходной защищённости ИСПДн; построения модели угроз и определения актуальности угроз; проектирования СЗПДн и организации физической защиты.
    - Описание технологии обработки и защиты ПДн.
12. **Тема 3. Классификация информационных систем персональных данных (определение уровня защищенности)**
    - Критерии определения уровня защищенности (классификации) ИСПДн. Порядок определения уровня защищенности ИСПДн и её документального оформления.
    - Вопросы оптимизации состава ПДн и процессов их обработки (реинжениринг ИСПДн).
13. **Тема 4. Формирование модели угроз ПДн и модели нарушителей**
    - Нормативная база для формирования модели угроз безопасности ПДн в ИСПДн. Нормативно-методические документы ФСТЭК России и ФСБ России.
    - Традиционный подход к построению моделей угроз и нарушителей.
    - Формирование модели угроз безопасности ПДн на основании документов ФСТЭК России.
    - Определение перечня актуальных угроз.
    - Методология формирования модели угроз безопасности персональным данным на основании документов ФСБ России.
    - Методология формирования модели нарушителей на основании документов ФСБ России.
14. **Тема 5. Разработка (проектирование) системы защиты персональных данных (СЗПДн)**
    - Меры по обеспечению безопасности персональных данных при их обработке. Требования Федерального закона от 27.07.2006 г. №152-ФЗ и Постановления Правительства РФ от 01.11.2012 г. №1119 к обеспечению безопасности персональных данных. Обязательные механизмы защиты.

- Общий порядок организации обеспечения безопасности ПДн в ИСПДн.
- Мероприятия по защите ПДн (требования к мерам и средствам защиты) в зависимости от уровней защищенности ИСПДн.
- Определение структуры, состава и основных функций СЗПДн.
- Определение перечня предполагаемых к использованию сертифицированных средств защиты информации и их настроек.

15. **Тема 6. Разработка и внедрение организационных мер и организационно-распорядительных документов по обеспечению защиты персональных данных**
    - Планирование организационных мероприятий по защите ПДн.
    - Разработка организационно-распорядительной документации, регламентирующей вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.
16. **Тема 7. Развертывание, настройка и опытная эксплуатация СЗПДн в ИСПДн**
    - Обеспечение охраны и физической защиты компонентов ИСПДн.
    - Организация и проведение работ по развёртыванию СЗПДн и настройке ее элементов в ИСПДн.
    - Испытания СЗПДн в процессе развертывания и опытной эксплуатации ИСПДн.
17. **Тема 8. Закрытие технических каналов утечки ПДн в ИСПДн**
    - Технические каналы утечки ПДн при их обработке в ИСПДн. Условия и причины возникновения, особенности проявления, способы и методы защиты.
    - Мероприятия по защите ПДн от утечки по техническим каналам для различных классов ИСПДн.
18. **Тема 9. Лицензирование деятельности по защите ПДн в ИСПДн**
    - Техническая защита конфиденциальной информации и техническое обслуживание СКЗИ как лицензируемые виды деятельности.
    - Получение оператором лицензий ФСТЭК России и ФСБ России. Лицензионные требования.

    **Итоговый зачет (тест).**

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН:

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| **1.** | **Раздел 1. Защита персональных данных.**<br>**Введение. Персональные данные в организации (на предприятии)** | **1** | **1** | **0** | |
| 1.1 | Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни | 0,3 | 0,3 | 0 | |
| 1.2 | Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных | 0,2 | 0,2 | 0 | |
| 1.3 | Персональные данные в системе документооборота предприятия. Персональные данные в автоматизированных системах и приложениях | 0,5 | 0,5 | 0 | |
| **2.** | **Основные понятия Федерального закона «О персональных данных»** | **2** | **2** | **0** | |
| 2.1 | Основные понятия. Персональные данные в Федеральном законе и Трудовом кодексе РФ. Содержание категории «персональные данные» | 0,1 | 0,1 | 0 | |
| 2.2 | Область применения закона. Ограничения | 0,1 | 0,1 | 0 | |
| 2.3 | Соотношение с другими категориями тайн. Персональные данные и их взаимосвязь с государственной, коммерческой, налоговой, банковской, адвокатской тайной, тайной связи и другими категориями конфиденциальных сведений | 0,1 | 0,1 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| 2.4 | Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение | 0,1 | 0,1 | 0 | |
| 2.5 | Принципы обработки персональных данных | 0,1 | 0,1 | 0 | |
| 2.6 | Условия обработки персональных данных. Согласие субъекта. Обработка биометрических данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных | 0,8 | 0,8 | 0 | |
| 2.7 | Специальные категории персональных данных и особенности их обработки | 0,1 | 0,1 | 0 | |
| 2.8 | Права субъектов персональных данных и их соблюдение при обработке | 0,1 | 0,1 | 0 | |
| 2.9 | Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов | 0,2 | 0,2 | 0 | |
| 2.10 | Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных | 0,1 | 0,1 | 0 | |
| 2.11 | Контроль и надзор за обработкой персональных данных | 0,1 | 0,1 | 0 | |
| 2.12 | Ответственность за нарушение требований по обращению с персональными данными | 0,1 | 0,1 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| **3.** | **Работа с персональными данными на предприятии (в организации)** | **4** | **4** | **0** | |
| 3.1 | Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы. Меры по охране конфиденциальности | 1,2 | 1,2 | 0 | |
| 3.2 | Формирование перечня персональных данных | 0,7 | 0,7 | 0 | |
| 3.3 | Ограничение доступа к персональным данным | 1,3 | 1,3 | 0 | |
| 3.4 | Общие сведения о конфиденциальном делопроизводстве | 0,5 | 0,5 | 0 | |
| 3.5 | Подготовка уведомлений об обработке персональных данных в уполномоченный орган | 0,3 | 0,3 | 0 | |
| **4.** | **Техническая защита персональных данных в информационных системах** | **3** | **3** | **0** | |
| 4.1 | Требования Федерального закона и Постановления Правительства РФ № 1119 от 01.11.2012 к обеспечению безопасности персональных данных. Обязательные механизмы защиты | 0,5 | 0,4 | 0 | |
| 4.2 | Определение уровня защищенности информационных систем персональных данных | 0,2 | 0,1 | 0 | |
| 4.3 | Модель угроз персональным данным | 0,7 | 0,6 | 0 | |
| 4.4 | Режим обеспечения безопасности персональных данных | 0,3 | 0,2 | 0 | |
| 4.5 | Каналы утечки информации при обработке персональных данных в информационных системах | 0,4 | 0,3 | 0 | |
| 4.6 | Система защиты персональных данных и ее описание | 0,5 | 0,4 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| 4.7 | Предотвращение несанкционированного доступа к персональным данным и обнаружение фактов такого доступа | 0,3 | 0,2 | 0 | |
| 4.8 | Регистрация запросов пользователей к информационным системам персональных данных | 0,2 | 0,2 | 0 | |
| 4.9 | Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним | 0,2 | 0,2 | 0 | |
| 4.10 | Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных | 0,3 | 0,1 | 0 | |
| 4.11 | Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Разбирательство нарушений системы безопасности | 0,4 | 0,3 | 0 | |
| **5.** | **Лицензирование деятельности по технической защите конфиденциальной информации** | **1** | **1** | **0** | |
| 5.1 | Понятие технической защиты как лицензируемого вида деятельности | 0,1 | 0,1 | 0 | |
| 5.2 | Лицензионные требования | 0,4 | 0,4 | 0 | |
| 5.3 | Проверка сведений о лицензиате и лицензионный контроль | 0,2 | 0,2 | 0 | |
| 5.4 | Ответственность за незаконную деятельность в области защиты информации | 0,2 | 0,2 | 0 | |
| 5.5 | Незаконное предпринимательство | 0,1 | 0,1 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| **6.** | **Аутсорсинг систем технической защиты персональных данных** | **1** | **1** | **0** | |
| **7.** | **Регулирование отношений в области организации и осуществления государственного контроля и надзора.** | **4** | **4** | **0** | |
| 7.1 | Организация проверки органами, осуществляющими государственный контроль и надзор. | 2 | 2 | 0 | |
| 7.2 | Порядок проведение проверки. | 1 | 1 | 0 | |
| 7.3 | Оформление результатов проверки. | 1 | 1 | 0 | |
| **8.** | **Итоговый контроль знаний по разделу** | **1** | **0** | **1** | **зачёт** |
| **9.** | **Введение.** Нормативная база организации технической защиты персональных данных | **1** | **1** | **0** | |
| **10.** | **Основные этапы работ по обеспечению безопасности ПДн в ИСПДн** | **1** | **1** | **0** | |
| 10.1 | Перечень основных этапов работ и краткий обзор мероприятий | 1 | 1 | 0 | |
| **11.** | **Сбор и анализ исходных данных по ИСПДн** | **1** | **1** | **0** | |
| 11.1 | Обследование информационных систем | 0,25 | 0,25 | 0 | |
| 11.2 | Сбор, анализ и документирование исходных данных | 0,5 | 0,5 | 0 | |
| 11.3 | Описание технологии обработки и защиты ПДн | 0,25 | 0,25 | 0 | |
| **12.** | **Определение уровня защищенности информационных систем персональных данных** | **2** | **2** | **0** | |
| 12.1 | Нормативная база определения уровня защищенности ИСПДн. | 0,5 | 0,5 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| 12.2 | Критерии определения уровня защищенности ИСПДн. УЗ ИСПДн. | 1 | 1 | 0 | |
| 12.3 | Вопросы оптимизации состава ПДн и процессов их обработки | 0,5 | 0,5 | 0 | |
| **13.** | **Формирование модели угроз ПДн и модели нарушителей** | **3** | **3** | **0** | |
| 13.1 | Нормативная база для формирования модели угроз | 0,5 | 0,5 | 0 | |
| 13.2 | Традиционный подход к построению моделей угроз и нарушителей | 0,5 | 0,5 | 0 | |
| 13.3 | Формирование модели угроз безопасности ПДн на основании документов ФСТЭК России | 0,5 | 0,5 | 0 | |
| 13.4 | Определение перечня актуальных угроз | 0,5 | 0,5 | 0 | |
| 13.5 | Методология формирования модели угроз безопасности на основании документов ФСБ России. | 0,5 | 0,5 | 0 | |
| 13.6 | Методология формирования модели нарушителей на основании документов ФСБ России. | 0,5 | 0,5 | 0 | |
| **14.** | **Разработка (проектирование) системы защиты персональных данных** | **9** | **9** | **0** | |
| 14.1 | Меры по обеспечению безопасности персональных данных при их обработке | 2 | 2 | 0 | |
| 14.2 | Общий порядок организации обеспечения безопасности ПДн в ИСПДн | 1,5 | 1,5 | 0 | |
| 14.3 | Мероприятия по защите ПДн в зависимости от уровней защищенности ИСПДн | 2 | 2 | 0 | |
| 14.4 | Определение структуры, состава и основных функций СЗПДн | 2 | 2 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| 14.5 | Определение перечня предполагаемых к использованию сертифицированных средств защиты информации | 1,5 | 1,5 | 0 | |
| **15.** | **Разработка и внедрение организационных мер и организационно-распорядительных документов по обеспечению защиты персональных данных** | **1** | **1** | **0** | |
| 15.1 | Планирование организационных мероприятий по защите ПДн | 0,25 | 0,25 | 0 | |
| 15.2 | Разработка организационно-распорядительной документации, | 0,25 | 0,25 | 0 | |
| **16.** | **Развертывание, настройка и опытная эксплуатация СЗПДн в ИСПДн** | **1** | **1** | **0** | |
| 16.1 | Обеспечение охраны и физической защиты компонентов ИСПДн. | 0,25 | 0,25 | 0 | |
| 16.2 | Организация и проведение работ по развёртыванию СЗПДн и настройке ее элементов в ИСПДн. | 0,5 | 0,5 | 0 | |
| 16.3 | Испытания СЗПДн в процессе развертывания и опытной эксплуатации ИСПДн. | 0,25 | 0,25 | 0 | |
| **17.** | **Закрытие технических каналов утечки ПДн в ИСПДн** | **2** | **2** | **0** | |
| 17.1 | Технические каналы утечки ПДн при их обработке в ИСПДн. | 1 | 1 | 0 | |
| 17.2 | Мероприятия по защите ПДн от утечки по техническим каналам для различных УЗ ИСПДн. | 1 | 1 | 0 | |
| **18.** | **Лицензирование деятельности по защите ПДн в ИСПДн** | **1** | **1** | **0** | |
| 18.1 | Техническая защита конфиденциальной инфомации и техническое обслуживание СКЗИ как лицензируемые виды деятельности. | 0,5 | 0,5 | 0 | |

| № п/п | Наименование разделов, дисциплин и тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практ. занятия | |
| 18.2 | Получение оператором лицензий ФСТЭК и ФСБ России. | 0,5 | 0,5 | 0 | |
| **19.** | **Контроль за соблюдением условий использования средств защиты информации** | **1** | **1** | **0** | |
| **20.** | **Итоговый контроль знаний** | **1** | **0** | **1** | **зачёт** |
| | **Итого** | **40** | **38** | **2** | |

### 9.2 Лабораторный практикум

Лабораторный практикум программой не предусмотрен.

| №№ п/п | № раздела учебной дисциплины | Наименование лабораторной работы | Количество отводимого времени (час.) |
|---|---|---|---|
| 1. | | | |

### 9.3 Семинары

Семинары программой не предусмотрены.

| № п/п | № раздела учебной дисциплины | Тематика семинаров | Количество отводимого времени (час.) |
|---|---|---|---|
| 1. | | | |

### 9.4 Практические занятия

| №№ п/п | № раздела учебной дисциплины | Тематика практического занятия | Количество отводимого времени (час.) |
|---|---|---|---|
| 1. | Модуль 2. Тема 3. Классификация информационных систем персональных данных (определение уровня защищенности) | Определение уровня исходной защищенности для заданной ИСПДн. Оформление соответствующих документов. | 1 |
| 2. | Модуль 2. Тема 4. Формирование модели угроз ПДн и модели нарушителей | Построение модели угроз для заданных параметров ИСПДн | 1 |
| 3. | Модуль 2. Тема 5. Разработка (проектирование) системы защиты персональных данных (СЗПДн) | Разработка проекта системы защиты с указанием основных видов средств защиты информации и (СЗИ) определения классов СЗИ. | 1 |

### 9.5 Учебно-методическое и информационное обеспечение

Каждый обучающийся (слушатель) перед началом занятий по Программе получает в постоянное пользование:

- оригинальное учебное пособие (руководство слушателя курса в печатном виде и возможность удалённого доступа к его электронному варианту на сервере СДО Учебного центра);
- справочные и вспомогательные материалы по изучаемым вопросам в электронном виде в системе дистанционного обучения.

Обеспеченность слушателей учебной литературой – 100%.

**а) основная литература:**

1. Защита персональных данных. Руководство слушателя курса КП32.- М.: УЦ Информзащита, 2016. – 251 с.

2. Техническая защита персональных данных. Руководство слушателя курса КП33. – М. УЦ Информзащита, 2016. – 260 с.

**б) дополнительная литература:**

3. «Конституция Российской Федерации», принята всенародным голосованием 12 декабря 1993г.

4. «О Декларации прав и свобод человека и гражданина», Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-1.

5. «Доктрина информационной безопасности Российской Федерации», утверждена

Президентом РФ 9 сентября 2000г. №Пр-1895.

**Кодексы:**

6. «Уголовный кодекс Российской Федерации», принят Федеральным законом от 13 июня 1996г. № 63-ФЗ.
7. «Кодекс Российской Федерации об административных правонарушениях», принят Федеральным законом от 30 декабря 2001г. №195-ФЗ.
8. «Гражданский кодекс Российской Федерации (часть первая)», принят Федеральным законом от 30 ноября 1994г. №51-ФЗ.
9. «Гражданский кодекс Российской Федерации (часть вторая)», принят Федеральным законом от 26 января 1996г. №14-ФЗ.
10. «Гражданский кодекс Российской Федерации (часть третья)», принят Федеральным законом от 26 ноября 2001г. №146-ФЗ.
11. «Гражданский кодекс Российской Федерации (часть четвертая)», принят Федеральным законом от 18 декабря 2006г. №230-ФЗ.
12. «Трудовой кодекс Российской Федерации», принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ.

**Федеральные законы:**

13. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
14. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
15. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».
16. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».
17. Федеральный закон от 2 декабря 1990г. № 395-1 «О банках и банковской деятельности».
18. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
19. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».
20. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».
21. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».
22. Федеральный закон от 3 апреля 1995г. № 40-ФЗ «О Федеральной службе безопасности».
23. Федеральный закон от 7 июля 2003г. № 126-ФЗ «О связи».

**Указы Президента Российской Федерации:**

24. Указ Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера».
25. Указ Президента Российской Федерации от 30 мая 2005г. № 609 «Об утверждении

Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

26. Указ Президента Российской Федерации от 3 апреля 1995г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

27. Указ Президента Российской Федерации от 16 августа 2004г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

**Постановления Правительства Российской Федерации:**

28. Постановление Правительства РСФСР от 5 декабря 1991г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

29. Постановление Правительства Российской Федерации от 16 марта 2009г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

30. Постановление Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

31. Постановление Правительства Российской Федерации от 1 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

32. Постановление Правительства Российской Федерации от 6 июля 2008г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

33. Постановление Правительства Российской Федерации от 4 марта 2010г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».

34. Постановление Правительства Российской Федерации от 16 апреля 2012г. № 313 «Об утверждении Положения о лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных

(криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

35. Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

36. Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).

37. Постановление Правительства Российской Федерации от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации».

38. Постановление Правительства Российской Федерации от 3 ноября 1994г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

39. Постановление Правительства Российской Федерации от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

**Нормативные документы ФСТЭК России:**

40. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.

41. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.

42. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

43. «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»,

утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

44. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

45. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

46. «Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», утвержден решением председателя Гостехкомиссии России от 30 марта 1992г.

47. «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 25 июля 1997г.

48. «Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования», утвержден решением председателя Гостехкомиссии России от 25 июля 1997г.

49. «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утвержден приказом председателя Гостехкомиссии России от 4 июня 1999г. № 114.

50. «Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1, Часть 2, Часть3», утвержден приказом председателя Гостехкомиссии России от 19 июня 2002г. №187.

51. «Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

52. «Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты», Гостехкомиссия России, 2003г.

53. «Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты», Гостехкомиссия России, 2003г.

54. «Руководство по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

55. Приказ ФСТЭК России № 21 от 18.02.2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

56. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

**Нормативные документы ФСБ России:**

57. Приказ ФСБ от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

58. Приказ ФСБ Российской Федерации от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

59. Приказ ФАПСИ Российской Федерации от 13 июня 2001г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г. № 2848.

60. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015)

61. Приказ Роскомнадзора от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных"

62. "Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 "Об утверждении требований и методов по обезличиванию персональных данных"

**Стандарты:**

63. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Москва, Стандартинформ, 2007, 11с.

64. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования». Москва, Стандартинформ, 2006, 8 с.

65. ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 814-ст). Москва, Стандартинформ, 2014, 56 с.

66. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. ... Часть 2. Функциональные компоненты безопасности. Москва, Стандартинформ, 161 с.

67. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Москва, Стандартинформ, 150 с.

68. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Москва, ИПК Изд-во стандартов, 1989, 28 с.

69. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Москва, Стандартинформ, 2012, 33 с.

70. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования». Москва, Стандартинформ, 2012, 35 с.

71. ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения». Москва, ИПК Изд-во стандартов, 1991, 27 с.

72. ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Москва, Стандартинформ, 2014. 106 с.

73. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Москва, Стандартинформ, 2009, 40 с.

**Учебные пособия:**

74. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев, ООО «ТИД ДС», 2001, 688 с.

75. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. Москва, Горячая линия - Телеком, 2000.

76. Петренко С.А., Курбатов В.А. Политики информационной безопасности. Москва, Компания АйТи, 2006, 400 с.

77. Петренко С.А., Петренко А.А. Аудит безопасности IntraNet. Москва, ДМК Пресс, 2002, 187 с.

78. Скот Бармен. Разработка правил информационной безопасности. Вильямс, 2002, 208 с.

79. Смит Р.Э. Аутентификация: от паролей до открытых ключей. Вильямс, 2002, 432 с.

80. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Москва, Издательство ТРИУМФ, 2002, 816 с.

81. Безопасность информационных технологий. Руководство слушателя курса БТ01. - М.: УЦ Информзащита, 2016. – 350 с.

82. Безопасность компьютерных сетей. Руководство слушателя курса БТ03.- Москва,

УЦ Информзащита, 2016, 367 с.

83. Основы TCP/IP. Руководство слушателя курса БТ05. Москва, УЦ Информзащита, 2012,108 с.

84. Безопасность ОС Windows 7/8.1/10/2012R2. Руководство слушателя курса БТ30.- М.: УЦ Информзащита, 2016. – 700 с.

85. Порядок применения системы защиты Secret Net (сетевая версия). Руководство слушателя курса Т005. Москва, УЦ Информзащита, 2016, 245 с.

86. Порядок применения системы защиты Secret Net (автономный вариант). Руководство слушателя курса Т005АВ. Москва, УЦ Информзащита, 2016, 138 с.

87. Реализация режима коммерческой тайны на предприятии. Руководство слушателя курса КП30. Москва, УЦ Информзащита, 2015, 85 с.

88. Организация конфиденциального делопроизводства. Руководство слушателя курса КП31. Москва, УЦ Информзащита, 2015, 218 с.

**Статьи:**

89. Станскова У.М. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа. Трудовое право в России и за рубежом, 2011, № 2.

90. Волков П.П. Экспертный анализ методов защиты информации от утечки по техническим каналам. Эксперт-криминалист, 2009, № 4.

91. Воротников В.Л. О правовой защите компьютерной информации. Администратор суда, 2009, № 2.

92. Забегайло Л.А., Назарова И.А. Актуальные вопросы охраны коммерческой тайны в отношениях с органами государства. Современное право, 2011, № 7.

93. Савчишкин Д.Б. Административная ответственность как средство обеспечения информационной безопасности. Административное и муниципальное право, 2011, № 6.

94. Чеботарева А.А. Электронное государственное управление как новая форма взаимоотношений личности, общества и государства. Государственная власть и местное самоуправление, 2011, № 6.

95. Маркарьян Р.В. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации. Международное публичное и частное право, 2011, № 4.

96. Кузнецова Т.В. Организация работы с персональными данными. Трудовое право, 2011, № 5.

97. Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных. Журнал российского права, 2011, №5.

98. Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации. Российский следователь, 2011, №4.

99. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция, 2011, №2.

100. Загузов Г.В. Административно-правовые средства обеспечения

информационной безопасности и защиты информации в Российской Федерации. Административное и муниципальное право, 2010, №5.

101. Палехова Е.А. Конфиденциальная информация и институт персональных данных в банковской деятельности. Предпринимательское право, 2010, №3.

**в) программное обеспечение:**

102. Microsoft Office (2003 или новее), броузеры (программы просмотра гипертекстов)

**г) базы данных, информационно-справочные и поисковые системы:**

103. Электронный ресурс Internet Security Glossary, Version 2. Режим доступа: http://www.ietf.org/rfc/rfc4949.txt.

104. Система дистанционного обучения (СДО) Учебного центра «Информзащита». Режим доступа: https://sdo.itsecurity.ru/view_doc.html?mode=default

105. Сайт Учебного центра «Информзащита». Режим доступа: http://itsecurity.ru/

106. Электронный ресурс Yandex.ru. Режим доступа: http://Yandex.ru

107. Электронный ресурс Google.com. Режим доступа: http://Google.com

## 9.6 Материально-техническое обеспечение учебного курса

Аудиторные занятия по дисциплине (модулю, курсу) включают лекции с демонстрацией презентаций на экране и практические работы (семинары) под руководством преподавателя.

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятий | Наименование оборудования, программного обеспечения |
|---|---|---|
| 1 | 2 | 3 |
| Лаборатория для изучения дисциплин по теме «Управление информационной безопасностью» | Лекции, практические занятия (семинары) | Для преподавателя<br>компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции (вебинара)<br>Для слушателей (на каждого, не менее) компьютер:<br>Процессор Core 2 Quad 2.50GHz<br>Память 2 Gb<br>Жесткий диск 500.0 Gb<br>DVD-ROM<br>Доступ в сеть интернет (сеть, броузер)<br>Доступ к СДО (системе тестирования)<br>Рассматриваемые аппаратно-программные средства защиты |

Необходимое оснащение класса. Столы, стулья по количеству обучаемых, оборудование кондиционирования и вентиляции воздуха.

Для преподавателя: компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции (вебинара).

В период очного обучения, каждому слушателю предоставляется компьютер с возможностью выхода в интернет, в том числе для доступа в «личный кабинет», где находится раздаточный материал по курсу (в электронном виде), а также к СДО Учебного центра для прохождения тестирования.

Тестирование слушателей в целях контроля усвоения материала по дисциплине (модулю, курсу), реализуется в системе дистанционного тестирования на базе сервера управления обучением и тестированием Учебного центра.

При использовании дистанционных образовательных технологий (онлайн-вебинаров) к компьютерам слушателей предъявляются такие же требования, как и компьютерам в аудитории.

### 9.7 Методические рекомендации по организации изучения учебного курса

Используются традиционные образовательные технологии на основе объяснительно-иллюстративного метода обучения, в форме информационной лекции и практических занятий в компьютерных классах.

Формирование профессиональных компетенций обеспечивается использованием в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

### 9.8 Оценочные материалы

Оценочные материалы по Программе включают наборы тестовых вопросов, используемые для контроля усвоения материала при проведении промежуточных аттестаций по каждой учебной дисциплине (курсу, модулю), а также скомпонованный из них пул тестов итоговой аттестации, реализуемые в рамках системы дистанционного тестирования на базе сервера управления обучением и тестированием Учебного центра.

Основные вопросы, включаемые в оценочные материалы промежуточных аттестаций приведены в соответствующих Рабочих программах по данным дисциплинам (модулям, курсам).

Перечень вопросов Итоговой аттестации (для экзамена) формируется из перечней основных вопросов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным дисциплинам (курсам, модулям) Программы.

Основные группы тестовых вопросов, выносимые на итоговую аттестацию:

Тест содержит 16 вопросов. К каждому вопросу предлагается по четыре варианта ответов, только один из которых правильный (полный). За каждый правильный ответ на вопрос теста слушатель получает один балл. Проходной бал зачёта 2/3 (11/16) правильных ответов.

На прохождение теста отводится один академический час.

Зачет принимает (тестирование организует) преподаватель, ведущий занятия по данной дисциплине (модулю, курсу).

**Оценочные материалы по модулю 1** программы включают следующие основные вопросы, выносимые на аттестацию (тестирование):

Персональные данные - это …

Возможность получения работодателем персональных данных работника у третьей стороны …

Кто является оператором персональных данных …

На что не распространяются требования Федерального закона "О персональных данных" …

Что включается в общедоступные источники персональные данные …

На кого возлагается обязанность предоставить доказательства получения согласия субъекта персональных данных на обработку его персональных данных …

Конфиденциальность персональных данных это …

Как производится уничтожение персональных данных …

Что является целью Федерального закона "О персональных данных": …

Когда согласие может быть только письменным …

Что относится к специальным категориям персональных данных …

Как осуществляется защита персональных данных работников работодателем …

Вправе ли работодатель получать и обрабатывать данные о частной жизни работника …

Уведомление об обработке персональных данных направляется оператором …

Кто является уполномоченным органом по защите прав субъектов персональных данных …

В каких случаях возможна обработка биометрических персональных данных …

Допуск к персональным данным лиц, которым они необходимы для выполнения служебных (трудовых) обязанностей …

Порядок определения уровня защищенности информационных систем персональных данных…

**Оценочные материалы по модулю 2** программы включают следующие основные вопросы, выносимые на аттестацию (тестирование):

Что такое Модель угроз безопасности персональных данных при их обработке в ИСПДн?

Что относится к специальным категориям персональных данных?

Как производится уничтожение персональных данных?

Какие значения может принимать показатель Y1 исходной защищённости ИСПДн?

Какие значения может принимать экспертная оценка "опасности конкретной угрозы" в методике актуализации угроз ФСТЭК России?

Для каких ИСПДн обязательно требуется формировать модель угроз?

Какое понятие является противоположным по смыслу понятию "общедоступная информация"?

Что такое "характеристики безопасности объекта защиты (объекта угроз)" в толковании документов ФСБ России по персональным данным?

Как "частная модель угроз" конкретной ИСПДн связана с уровнем защищенности?

Чем определяется требуемый уровень криптографической защиты ПДн (класс требуемых криптосредств)?

В каком кодексе предусмотрена ответственность за «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»?

С какого уровня защищенности необходимо назначить ответственного за обеспечение безопасности ПДн?

С какого уровня защищенности необходима автоматическая регистрация изменения полномочий сотрудника по доступу к ПДн?

В каких условиях разрешается техническое обслуживание криптосредств и смена криптоключей?

Где должны находиться печати, предназначенные для опечатывания хранилищ (при использовании криптосредств)?

Что необходимо сделать с ключом от хранилищ (при использовании криптосредств) по окончанию рабочего дня?

## 10. Перечень сведений, составляющих государственную тайну, используемых в учебном процессе

В учебном процессе по данной программе повышения квалификации сведения, составляющие государственную тайну, не рассматриваются.