ДЕПАРТАМЕНТ СМОЛЕНСКОЙ ОБЛАСТИ ПО ОБРАЗОВАНИЮ И НАУКЕ
областное государственное бюджетное профессиональное образовательное учреждение «Смоленская академия профессионального образования» (ОГБПОУ СмолАПО)

УТВЕРЖДАЮ
Директор ОГБПОУ СмолАПО
_____ М. В. Белокопытов

ПРОГРАММА ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«Методы, средства и технологии защиты информации»

Смоленск
2020 г.

1. Наименование программы повышения квалификации:

«Методы, средства и технологии защиты информации»

2. Общая характеристика образовательной программы

2.1. Цель реализации программы:

Программа повышения квалификации, направлена на формирование профессиональных компетенций, необходимых для профессиональной деятельности в области обеспечения информационной безопасности и комплексной защиты объектов информатизации.

Программа повышения квалификации адаптирована для лиц с особыми потребностями с целью развития их жизненных и профессиональных компетенций и успешной социализации. Одним из факторов социальной адаптации и развития компетенций слушателей из числа лиц с ОВЗ является повышение доступности образовательной среды за счет использования электронного обучения и дистанционных образовательных технологий.

Социальная адаптация и формирование профессиональных компетенций слушателей из числа лиц с ОВЗ достигается за счет индивидуального подхода, систематичности и поэтапного усложнения обучающего материала и учёта зоны ближайшего развития.

2.2. Программа разработана на основе требований профессиональных стандартов:

– «Специалист по защите информации в автоматизированных системах» (зарегистрировано в Минюсте России 28 сентября 2016 г. № 43857).

ОТФ: Обеспечение защиты информации в автоматизированных системах в процессе их функционирования,

– «Специалист по безопасности компьютерных систем и сетей» (зарегистрировано в Минюсте России 28 сентября 2016 г. № *N* 44464).

ОТФ: Обеспечение безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности.

2.3. Планируемые результаты обучения

Слушатель, освоивший программу повышения квалификации, должен обладать следующими компетенциями:

– осуществлять планирование и организацию выполнения мероприятий по защите информации,

– выявлять и анализировать возможные угрозы информационной безопасности объектов,

– применять программно-аппаратные и технические средства защиты информации на защищаемых объектах,

По итогам освоения программы слушатель должен:

Знать:

– основные понятия в области информационной безопасности,

– основы организационного и правового обеспечения информационной безопасности, основные правовые акты и нормативные методические в области защиты информации,

– виды и состав угроз информационной безопасности,

– критерии, условия и принципы отнесения информации к защищаемой,

– принципы и общие методы обеспечения информационной безопасности,

– классификацию видов, методов и средств защиты информации.

Уметь:

– применять правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;

– классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.

Владеть:

– профессиональной терминологией в области информационной безопасности;

– навыками рационального выбора средств и методов защиты информации объектов информатизации;

– организационными и техническими методами обеспечения безопасности объекта информатизации.

3. Учебный и учебно-тематический планы

УЧЕБНЫЙ ПЛАН

программы повышения квалификации
«Методы, средства и технологии защиты информации»

Требования к уровню образования поступающих на обучение	Обучение осуществляется на базе высшего и среднего профессионального образования
Категория слушателей	Для сотрудников предприятий и организаций, работающих в сфере ИТ, желающих повысить профессиональный уровень в рамках имеющейся квалификации. Лица, планирующие сменить деятельность на работу в сфере информационной безопасности
Срок обучения	12 дней
Форма обучения	очная, очно-заочная с применением электронного обучения и дистанционных образовательных технологий

№ п/п	Наименование модуля, темы	Всего часов трудоемкости	В том числе				Форма контроля
			Аудиторные занятия*			Самостоятельная работа*	
			Всего часов	из них			
				Лекции	Практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Модуль 1. Организационные и правовые основы информационной безопасности	24	18	2 6*	2 8*	6	Тестирование
2	Модуль 2. Угрозы информационной безопасности	18	14	2 2*	2 8*	4	Тестирование
3	Модуль 3. Способы и методы защиты информации	30	22	6*	8 8*	8	Тестирование
	Всего:	**72**	**54**	**18**	**36**	**18**	
	Итоговая аттестация						Накопительная система по промежуточной аттестации
	Общая трудоемкость программы:	**72**					

* **С применением дистанционных образовательных технологий и электронного обучения**

Учебно-тематический план программы повышения квалификации

№ п/п	Наименование модуля, темы	Всего часов трудоемкости	В том числе				Форма контроля
			Аудиторные занятия*			Самостоятельная работа*	
			Всего часов	из них			
				Лекции	Практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Модуль 1. Организационные и правовые основы ИБ	*24*	*18*	*8*	*10*	*6*	Тестирование
2	Тема 1.1 Понятие ИБ и её место в системе национальной безопасности	6	4	2*	2*	2	Практическое задание
3	Тема 1.2 Законодательство в области информационных технологий и защиты информации	10	8	2 2*	4*	2	Практическое задание
4	Тема 1.3. Классификация информации подлежащей защите	8	6	2*	2 2*	2	Практическое задание
5	Модуль 2. Угрозы информационной безопасности	*18*	*14*	*4*	*10*	*4*	Тестирование
6	Тема 2.1. Угрозы информационной безопасности	8	6	2*	4*	2	Практическое задание
7	Тема 2.2. Виды атак на информационную систему	10	8	2	2 4*	2	Практическое задание
8	Модуль 3. Способы и методы защиты информации	*30*	*22*	*6*	*16*	*8*	Тестирование
9	Тема 3.1 Способы и методы защиты информации	16	12	4*	4 4*	4	Практическое задание
10	Тема 3.2. Подходы к реализации и этапы построения систем защиты информации	14	10	2*	4 4*	4	Практическое задание
	Всего:	**72**	**54**	**18**	**36**	**18**	
	Итоговая аттестация						Накопительная система по промежуточной аттестации
	Общая трудоемкость программы:	**72**					

* **С применением дистанционных образовательных технологий и электронного обучения**

4. Календарный учебный график

Программа повышения квалификации *Методы, средства и технологии защиты информации*

Объем программы 72 час.

Продолжительность обучения 12 дней

Форма обучения – очная, очно-заочная с применением электронного обучения и дистанционных образовательных технологий

Образовательный процесс по программе может осуществляться в течение всего учебного года. Занятия проводятся по мере комплектования групп.

5. Содержание программы

Модуль 1. **Организационные и правовые основы информационной безопасности**

Тема 1.1 Понятие информационной безопасности и её место в системе национальной безопасности

Сущность информационной безопасности. Объекты информационной безопасности. Место информационной безопасности в системе национальной безопасности. Понятие и назначение доктрины информационной безопасности. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности.

Тема 1.2 Законодательство в области информационных технологий и защиты информации

Обзор законодательства России как основы для обеспечения интересов личности, общества и государства в информационной сфере. Характеристика стандартов в области информационной безопасности.

Тема 1.3. Классификация информации подлежащей защите

Свойства информации как предмета защиты. Основные виды конфиденциальной информации, нуждающейся в защите. Государственные органы в области защиты информации. Система безопасности РФ.

Модуль 2. **Угрозы информационной безопасности**

Тема 2.1. Угрозы информационной безопасности

Понятие угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия.

Тема 2.2. Виды атак на информационную систему

Основные способы несанкционированного доступа к конфиденциальной информации. Методы, используемые злоумышленниками для получения доступа к конфиденциальной информации либо вывода из строя информационной системы.

Модуль 3. **Способы и методы защиты информации**

Тема 3.1 Способы и методы защиты информации

Способы предупреждения возможных угроз. Способы обнаружения угроз. Способы пресечения или локализации угроз. Основные способы ликвидации последствий. Основные защитные действия при реализации способов защиты информации. Защита от разглашения. Защитные действия от утечки и от несанкционированных действий (НСД) к конфиденциальной информации. Мероприятия по технической защите информации.

Тема 3.2. Подходы к реализации и этапы построения систем защиты информации

Классификация автоматизированных систем и требования к обеспечению безопасности различных классов. Реализация системы защиты информации на основе встраиваемых и встроенных средств защиты. Организация безопасной среды для работы обработки конфиденциальной информации. Этапы проектирования и реализации систем защиты конфиденциальной информации.

6. Организационно-педагогические условия реализации программы

6.1. Материально-технические условия

Для реализации дополнительной профессиональной программы повышения квалификации «Методы, средства и технологии защиты информации» предусмотрена мастерская «Кибер-безопасности», оснащенная следующим оборудованием и программным обеспечением:

– Персональный компьютер в сборе: Processor - AMD Ryzen X8 R7-1700, DDR4 DIMM 32Гб, Видеокарта - ASUS GeForce GTX 1650 PHOENIX OC [PH-GTX1650-04G], SD накопитель A-DATA S11 Pro AGAMMIXS11P-512GT-C 512 Гб;

– Компьютерный монитор AOC 24" G2460VQ6;

– Клавиатура USB CBR KB 107;

– Компьютерная мышь USB CBR CM-302;

– Источник бесперебойного питания Powercom UPS RPT-800A EURO;

– Сервер [2U / 2 x Intel Xeon Silver 4210R (2.4GHz,10C) / 8 x 32Gb DDR4 2933, ECC R(24up) / 4x960Gb SSD SATA / 4 x 10GE / 2 x 800w;

– Управляемый Коммутатор Cisco WS-C2960L-48;

– Коммутатор L3 WS-C3650-24;

– Телевизор 50” LED Haier LE50K5500TF;

– Флипчат электронный SMART kapp 42;

– Интерактивная доска Screen Media;

– Проектор CASIO XJ-V110W с потолочным креплением и коммутацией;

– МФУ Canon i-SENSYS MF426dw;

– USB-токен JaCarta-2 PKI/ГОСТ (XL) JC-MediaKit-4 - "ПК JaCarta – MediaKit,

– Рутокен ЭЦП 2.0 64 кб;

– RDS-01 USB считывательключей Dallas Touch Memory (iButton);

– DS1996 с изогнутым брелоком - электронный ключ DallasTouchMemory (IButton);

– Findkey Hamster III (HFDU06S) - настольный биометрический считыватель;

– Установочный комплект. Средство защиты информации Secret Net Studio 8;

– Установочный комплект. Средство защиты информации vGate R2;

– Дистрибутив СКЗИ КриптоПро CSP версии 5.0 КС1 и КС2 на DVD;

– Формуляры Dallas Lock 8.0-К. Право на использование** (СЗИ НСД. СКН); Бессрочная лицензия Dallas Lock 8.0. Сертифицированный комплект для установки;

– Программное обеспечение клиентского доступа к виртуальным машинам Academic VMware Workstation 15 Pro for Linux and Windows;

– Система виртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;

– ПО операционная система Windows 10 с интегрированной программной платформой .NET Framework, 4.8;

– ПО для просмотра документов в формате PDF Adobe Reader DC;

– ПО для архивации 7-Zip;

– ПО офисный пакет Microsoft Office 2019;

– Система виртуализации VMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;

– Антивирусное программное обеспечение Kaspersky Endpoint Security.

Каждое рабочее место, оснащено персональным компьютером с высокоскоростным доступом к сети Интернет.

6.2. Учебно-методическое и информационное обеспечение программы (учебно-методические материалы)

Нормативно-правовые документы

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ (последняя редакция).

2. Федеральный закон «О коммерческой тайне» от 18.12.2006 г. № 231-ФЗ (последняя редакция).

3. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ (последняя редакция).

4. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.).

Основная литература

1. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: учеб. пособие / Е.В. Глинская, Н.В. Чичварин. М.: ИНФРА-М, 2018. 118 с.

2. Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие / Е.К. Баранова, А.В. Бабаш. 3-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2017. 322 с.

Дополнительная литература

1. Гришина Н.В. Информационная безопасность предприятия: учеб. пособие. 2-е изд., доп. М.: ФОРУМ: ИНФРА-М, 2017. 239 с.

2. Вдовенко Л.А. Информационная система предприятия: учеб. пособие. 2-е изд., пераб. и доп. М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. 304 с.

3. Партыка Т.Л. Информационная безопасность: учеб. пособие для сред. проф. образования / Т.Л. Партыка, И.И. Попов. 2-е изд., испр. и доп. М.: ФОРУМ: ИНФРА-М, 2015. 368 с.

4. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.

5. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

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

Программное обеспечение и интернет-ресурсы

1. Дистрибутивы антивирусных программ с официальных сайтов разработчиков.

2. Справочно-информационная система (СИС) «Гарант».

3. Справочно-информационная система «Консультант».

6.3. Реализация рабочей программы обеспечивается педагогическими кадрами, имеющими высшее и среднее профессиональное образование, соответствующее профилю преподаваемой темы.

6.4. Условия для функционирования электронной информационно-образовательной среды (при реализации программ с использованием электронного обучения и дистанционных образовательных технологий):

- наличие системы дистанционного обучения на основе Moodle - http://do.smolapo.ru/

- системы видеоконференцсвязи (ВКС) – Zoom, Discord.

7. Описание контроля качества освоения программы

При проведении текущего, промежуточного и итогового контроля для лиц с ОВЗ предусмотрено увеличение времени для подготовки ответа, оказание необходимой технической помощи, выбор формы предоставления заданий и ответов (устно, письменно на бумаге, письменно на компьютере, с использованием услуг ассистента (сурдопереводчика), использование специальных технических средств, предоставление дополнительных перерывов).

7.1. Формы текущей аттестации

Текущий контроль освоения программы включает в себя оценивание работы слушателя на практических занятиях и самостоятельной работы над домашним заданием. Оценки за работу на практических занятиях и самостоятельную работу слушателя вставляются в рабочую ведомость, а также результаты прохождения тестов с использованием электронного обучения и дистанционных образовательных технологий.

Практическое задание оценивается преподавателем по 4-балльной шкале. Отметки 5, 4 и 3 – положительные. Отметка 2 – неудовлетворительная и означает, что практическое задание считается невыполненным.

7.2. Формы промежуточной аттестации

Промежуточный контроль осуществляется после изучения каждого модуля курса с использованием электронного обучения и дистанционных образовательных технологий посредством тестирования по каждой теме.

Тест оценивается по шкале «зачтено – не зачтено» и считается успешно выполненным, если слушатель верно ответит на 60 и более процентов поставленных тестовых заданий. Для прохождения тестирования слушателю предоставляется две попытки, период прохождения тестирования – весь срок реализации программы. Взаимозависимости между прохождением промежуточной аттестации по предыдущей теме и допуском к прохождению следующей темы не устанавливается.

Примеры тестовых и практических заданий приведены в приложении А.

7.3. Форма итоговой аттестации

Итоговая аттестация освоения курса осуществляется по накопительной системе. Для прохождения итоговой аттестации слушатель должен выполнить с положительной отметкой одно задание по каждой теме и успешно пройти тестирование по всем модулям.

ПРИЛОЖЕНИЕ А

Примеры тестовых заданий

1. Что такое защита информации?

1) защита от несанкционированного доступа к информации;

2) выпуск бронированных коробочек для дискет;

3) комплекс мероприятий, направленных на обеспечение информационной безопасности.

2. К какой группе мер по защите информации относится шифрование информации?

1) организационным;

2) техническим;

3) аппаратным;

4) программным.

3. Укажите принципы создания комплексной системы защиты информации:

1) неизменности;

2) прозрачности;

3) модульности;

4) рациональности;

5) доступности.

4. Внешние техногенные угрозы информационной безопасности обусловлены:

1) средствами связи и помехами от них;

2) близко расположенными опасными производствами;

3) некачественными программными средствами;

4) взаимодействием технических средств.

5. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?

1) стихийные;

2) техногенные;

3) антропогенные.

6. Основные цели организационных мер защиты информации:

1) обеспечение правильности функционирования механизмов защиты;

2) предоставление бесперебойного доступа к необходимой информации авторизованным сотрудникам;

3) регламентация автоматизированной обработки информации;

4) шифрование информации.

7. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода:

1) макровирус;

2) троянский конь;

3) червь;

4) файловый вирус.

8. Самым слабым элементом в помещении с точки зрения звукоизоляции являются:

1) двери, стены, система заземления;

2) двери, пол, потолок;

3) двери, окна;

4) окна, система заземления, пол.

9. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?

1) организационное;

2) организационно-техническое;

3) техническо-организационное;

4) техническое.

10. Какие пункты относятся к активным методам защиты речевой информации?

1) создание маскирующих акустических и вибрационных помех;

2) выявление факта несанкционированного подключения к линии;

3) создание прицельных электромагнитных помех акустическим закладным устройствам;

4) выявление излучений акустических закладных устройств;

5) уничтожение средств несанкционированного подключения к телефонной линии.

11. В число основных принципов построения системы безопасности, с точки зрения её архитектуры, входят:

1) следование признанным стандартам;

2) применение нестандартных решений, не известных злоумышленникам;

3) разнообразие защитных средств.

12. Оценка рисков позволяет ответить на следующие вопросы:

1) Как спроектировать надежную защиту?

2) Какую политику безопасности предпочесть?

3) Какие защитные средства экономически целесообразно использовать?

13. Окно опасности появляется, когда:

1) становится известно о средствах использования уязвимости;

2) появляется возможность использовать уязвимость;

3) устанавливается новое программное обеспечение.

14. Окно опасности перестает существовать, когда:

1) администратор безопасности узнает об угрозе;

2) производитель программного обеспечения выпускает заплату;

3) заплата устанавливается в защищаемой информационной системе.

15. В число направлений физической защиты входят:

1) мобильная защита систем;

2) системная защита средств мобильной связи;

3) защита мобильных систем;

4) противопожарные меры;

5) межсетевое экранирование;

6) контроль защищенности;

7) физическая защита пользователей;

8) защита поддерживающей инфраструктуры;

9) защита от перехвата данных.

16. Политика безопасности:

1) строится на основе общих представлений об информационной системе организации;

2) строится на основе изучения политик родственных организаций;

3) строится на основе анализа рисков;

4) фиксирует правила разграничения доступа;

5) отражает подход организации к защите своих информационных активов;

6) описывает способы защиты руководства организации.

17. Оценка рисков позволяет ответить на следующие вопросы:

1) Как спроектировать надежную защиту?

2) Какую политику безопасности предпочесть?

3) Какие защитные средства экономически целесообразно использовать?

4) Чем рискует организация, используя информационную систему?

5) Чем рискуют пользователи информационной системы?

6) Чем рискуют системные администраторы?

7) Существующие риски приемлемы?

8) Кто виноват в том, что риски неприемлемы?

9) Что делать, чтобы риски стали приемлемыми?

18. В число принципов физической защиты входят:

1) беспощадный отпор;

2) непрерывность защиты в пространстве и времени;

3) минимизация защитных средств.

19. В число основных принципов архитектурной безопасности входят:

1) применение наиболее передовых технических решений;

2) применение простых, апробированных решений;

3) сочетание простых и сложных защитных средств.

20. Меры информационной безопасности направлены на защиту от:

1) нанесения неприемлемого ущерба;

2) нанесения любого ущерба;

3) подглядывания в замочную скважину.

21. Цели защиты информации от технических средств разведки:

а) предотвращение утечки, хищения, утраты, искажения, подделки информации;

б) предотвращение угроз безопасности личности, общества, государства;

в) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

г) предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

22. Что понимается под угрозой безопасности информации в компьютерной системе?

а) потенциально возможная уязвимость информации в компьютерной системе;

б) потенциально возможное событие, которое может привести к уничтожению, утрате целостности, конфиденциальности или доступности информации;

в) подготовка взлома компьютерной системы.

23. Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

а) несанкционированный доступ к информации, вредительские программы, ошибки при разработке компьютерной системы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур компьютерной системы;

в) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала.

24. Для защиты от случайных угроз компьютерной информации используют:

а) обучение пользователей правилам работы с КС, разрешительную систему доступа в помещение;

б) межсетевые экраны, идентификацию и аутентификацию пользователей;

в) дублирование информации, создание отказоустойчивых КС, блокировка ошибочных операций.

25. Несанкционированный доступ к информации в компьютерной системе это:

а) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники;

б) доступ к информации, нарушающий правила разграничения доступа с использованием технических средств разведки;

в) доступ к информации компьютерной системы без санкции администратора безопасности.

26. Построение модели злоумышленника при создании системы защиты информации необходимо для:

а) оптимизации системы защиты информации;

б) составления фоторобота злоумышленника;

в) составления базы данных потенциальных взломщиков.

27. Какие из перечня угроз относятся к преднамеренным угрозам компьютерной информации:

а) шпионаж и диверсии, несанкционированный доступ к информации, вредоносные программы;

б) ошибки при разработке компьютерной системы, ошибки в программном обеспечении, электромагнитные излучения и наводки;

в) стихийные бедствия и аварии, сбои и отказы технических средств,

ошибки пользователей и обслуживающего персонала.

28. Какие средства защиты фиксируют факт проникновения злоумышленника в компьютерную систему?

а) средства охранно-пожарной сигнализации;

б) средства биометрической идентификации;

в) пломбы, наклейки, замки на аппаратуре компьютерной системы.

29. Персональные данные:

а) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу;

б) данные, касающиеся состояния здоровья и религиозных взглядов человека;

в) информация о месте работы, паспортные данные, сведения о доходе.

30. Обработка персональных данных:

а) 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;

б) накопление, хранение и передача персональных данных;

в) размещение персональных данных в информационных системах.

31. Оператор:

а) 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;

б) юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных;

в) юридическое или физическое лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к персональным данным.

32. Контроль над выполнением требований в сфере защиты персональных данных выполняют

а) ФСБ РФ;

б) ФСТЭК России

в) Роскомнадзор;

в) все перечисленные организации.

33. За несоблюдение положений закона 152-ФЗ «О персональных данных» предусматривается:

а) гражданская, уголовная, административная ответственность;

б) дисциплинарная и другие виды ответственности;

в) все перечисленные виды ответственности.

34. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита:

а) речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов;

б) физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн;

в) всех видов информации.

35. Обезличивание персональных данных:

а) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность

персональных данных конкретному субъекту персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных;

в) все перечисленные действия.

36. Несанкционированный доступ (НСД) к информации:

а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС);

б) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств;

в) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа.

37. Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

а) несанкционированный доступ к информации, вредительские программы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур;

в) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала.

38. Идентификация это:

а) процесс предъявления пользователем идентификатора.

б) процесс подтверждения подлинности.

в) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов.

39. Что является организационной формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования,

модификации или уничтожения.

40. Что является правовой формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования,

модификации или уничтожения.

41. Что является инженерно-технической формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования,

модификации или уничтожения.

42. К числу определяющих признаков, по которым производится классификация информационных систем, относятся:

а) наличие в информационной системе информации различного уровня конфиденциальности;

б) уровень значимости информации и масштаб информационной системы;

в) режим обработки данных в информационной системе - коллективный или индивидуальный.

43. Для ИСПДн устанавливается:

а) два уровня защищенности персональных данных;

б) три уровня защищенности персональных данных;

в) четыре уровня защищенности персональных данных.

44. В общедоступные источники персональных данных (в том числе справочники, адресные книги) персональные данные включаются:

а) с письменного согласия субъекта персональных данных;

б) согласия субъекта персональных данных не требуется;

в) согласия субъекта персональных данных не требуется, но по требованию субъекта данные в любое время должны быть исключены из общедоступных источников персональных данных.

45. Уровень защищенности ПДн устанавливается в зависимости от:

а) типа угроз, актуальных для ИСПДн и категории обрабатываемых ПДн;

б) объема ПДн, обрабатываемых в ИСПДн;

в) типа угроз, актуальных для ИСПДн, категории обрабатываемых ПДн, объема ПДн, обрабатываемых в ИСПДн.

Примеры практических задач

1. Выделить нормативно-правовые акты, закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций).

2. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации).

3. Оценить действия сотрудника предприятия, приведшие к инциденту, связанному с угрозой информационной безопасности (в предлагаемой ситуации).

4. Установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла.

5. Разграничить доступ к файлу, директории и принтеру средствами операционной системы Windows.

6. Разграничить доступ к файлу, директории и принтеру средствами операционной системы LINUX.

7. Настроить аудит обращений к файлу от имени владельца средствами операционной системы Windows.

8. Настроить аудит обращений к файлу от имени владельца средствами операционной системы LINUX.

9. Настроить политику паролей средствами операционной системы Windows.

10. Настроить политику паролей средствами операционной системы LINUX.

11. Проверить компьютерную систему на наличие вредоносного программного обеспечения.

12. Установка и администрирование системы защиты информации SecretNet.

13. Установка и администрирование системы защиты информации DallasLock.

14. Настройка удаленного управления компьютером с помощью удаленного рабочего стола.