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

«Разработка системы информационной безопасности»

Смоленск
2020 г.

1. Наименование программы повышения квалификации:

Разработка системы информационной безопасности

2. Общая характеристика образовательной программы

2.1. Цель реализации программы:

Настоящая программа предназначена для повышения квалификации работников профессиональных образовательных организаций, реализующих подготовку обучающихся по укрупненным группам специальностей10.00.00 «Информационная безопасность» и 09.00.00 «Информатика и вычислительная техника».

Цель программы – повышение уровня профессиональной компетентности, формирование и закрепление на практике профессиональных знаний и умений, необходимых для организации образовательной деятельности при реализации ФГОС.

2.2. Программа разработана на основе требований:

– Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– профессионального стандарта «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования» (утв. приказом Минтруда и социальной защиты России от 08 сентября 2015 № 608н);

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

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

2.3. Планируемые результаты обучения

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

– выявлять и анализировать возможные угрозы информационной безопасности объектов,

– осуществлять планирование и организацию выполнения мероприятий по защите информации,

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

По итогам освоения программы слушатель должен:

Знать:

– виды и состав угроз информационной безопасности,

– критерии, условия и принципы отнесения информации к защищаемой,

– 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
«Разработка системы информационной безопасности»

Требования к уровню образования поступающих на обучение	Обучение осуществляется на базе высшего и среднего профессионального образования.
Категория слушателей	Работники профессиональных образовательных организаций, реализующих подготовку обучающихся по укрупненным группам специальностей10.00.00 «Информационная безопасность» и 09.00.00 «Информатика и вычислительная техника»
Срок обучения	8-12 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. Концепция информационной безопасности	6	4	2	2	2	Тестирование
2	Модуль 2. Анализ существующей системы защиты информации. Определение угроз информационной безопасности	18	14	8	6	4	Тестирование, практическое задание
3	Модуль 3. Разработка системы информационной безопасности	24	20	8	12	4	Тестирование, практическое задание
	Всего:	**48**	**38**	**18**	**20**	**10**	
	Итоговая аттестация	Накопительная система по промежуточной аттестации					
	Общая трудоемкость программы:	**48**					

* **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. Концепция информационной безопасности	6	4	2	2	2	
2	Тема 1.1 Цели и задачи системы информационной безопасности	6	4	2	2*	2	Тестирование
3	Модуль 2. Анализ существующей системы защиты информации. Определение угроз информационной безопасности	18	14	8	6	4	
4	Тема 2.1. Обследование существующей инфраструктуры и определение исходных данных	6	4	2	2*	2	Тестирование, практическое задание
5	Тема 2.2. Анализ конфиденциальной информации организации	2	2	2*	-	-	Тестирование, практическое задание
6	Тема 2.3. Определение угроз информационной безопасности	4	4	2*	2*	-	Тестирование, практическое задание
7	Тема 2.4. Характеристика существующих мер по защите информации организации.	6	4	2	2	2	Тестирование, практическое задание
8	Модуль 3. Разработка системы информационной безопасности	24	20	8	12	4	
9	Тема 3.1 Организационное обеспечение информационной безопасности	6	4	2*	2*	2	Тестирование, практическое задание
10	Тема 3.2. Инженерно-техническое обеспечение системы информационной	8	6	2	4*	2	Тестирование, практическое задание

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

	безопасности						
11	Тема 3.3. Программно-аппаратное обеспечение системы информационной безопасности	10	10	2 2*	6	-	Тестирование, практическое задание
	Всего:	**48**	**38**	**18**	**20**	**10**	
	Итоговая аттестация						Накопительная система по промежуточной аттестации
	Общая трудоемкость программы:	**48**					

4. Календарный учебный график

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

Объем программы 48 час.

Продолжительность обучения 8-12 дней

Форма обучения – очная, очно-заочная с применением 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. Концепция информационной безопасности

Тема 1.1 Цели и задачи системы информационной безопасности

Цели и задачи информационной безопасности. Концепция информационной безопасности. Основные аспекты, решаемые при разработке системы ИБ. Правовое обеспечение системы защиты информации.

Модуль 2. Анализ существующей системы защиты информации. Определение угроз информационной безопасности

Тема 2.1. Обследование существующей инфраструктуры и определение исходных данных

Определение исходных данных для проектирования системы ИБ. Описание

организации. Общая характеристика деятельности и организационная структура. Сведения о зданиях и помещениях. Информационная система.

Тема 2.2. Анализ конфиденциальной информации организации

Информационные активы организации. Перечень конфиденциальной информации.

Тема 2.3. Определение угроз информационной безопасности

Классификация угроз безопасности информации. Определение угроз информационной безопасности. Систематизация угроз ИБ

Тема 2.4. Характеристика существующих мер по защите информации организации

Характеристика систем контроля управления доступом, инженерно-технического и программно-аппаратного обеспечения системы защиты информации. Определение каналов несанкционированного доступа. Оценка и анализ рисков ИБ.

Выделение недостатков существующей СЗИ.

Модуль 3. Разработка системы информационной безопасности

Тема 3.1 Организационное обеспечение информационной безопасности

Плановые мероприятия и документы для усовершенствования существующей системы информационной безопасности. Основные направления политики ИБ.

Тема 3.2. Инженерно-техническое обеспечение системы информационной безопасности

Особенности разработки системы охраны периметра, охранно-пожарной сигнализации, системы видеонаблюдения. Выбор аппаратуры поста управления

Тема 3.3. Программно-аппаратное обеспечение системы информационной безопасности

Разработка подсистем идентификации и аутентификации, защиты от вредоносного ПО, резервного копирования и архивирования, обнаружения сетевых атак, защиты информации в ЛВС, обеспечения целостности данных.

Анализ рисков разработанной системы информационной безопасности.

Оценка контроля качества освоения программы повышения квалификации

Промежуточный контроль осуществляется после изучения каждой темы курса с использованием дистанционных образовательных технологий посредством тестирования по каждой теме и решения практической задачи на материале организации.

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.

Практическое задание оценивается преподавателем.

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

Примеры тестовых и практических заданий приведены в приложении А.

6. Организационно-педагогические условия реализации программы

6.1. Материально-технические условия

Для реализации дополнительной профессиональной программы повышения квалификации «Разработка системы информационной безопасности» 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

7.1. Форма итоговой аттестации

Итоговая аттестация осуществляется по накопительной системе. Для прохождения итоговой аттестации слушатель должен по каждой теме выполнить с положительной отметкой одно практическое задание и пройти тестирование (процент выполнения не меньше 60).

ПРИЛОЖЕНИЕ А

Примеры тестовых заданий

1. Комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных

a) Система защиты информации
b) Защита информации
c) Информационная безопасность
d) Информационная система

2. Конфиденциальная информация – это

a) документированная и не документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
b) **документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации**
c) документированная информация, доступ к которой ограничивается каждым владеющим ею субъектом по своему выбору
d) не документированная информация

3. Информация о гражданах (персональные данные) – это

a) любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу
b) информация о проведении гражданином собственного досуга
c) сведения о физическом состоянии гражданина, полученные в установленном законом порядке
d) сведения о психологическом состоянии гражданина, полученные в установленном законом порядке

4. Документированная информация - это

a) информация, записанная на бумаге
b) зафиксированная на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать
c) информация, записанная на материальный носитель и хранящаяся под грифом "Совершенно секретно"
d) нет правильного ответа

5. Подразделение предприятия, специально созданное для обеспечения безопасности его законных прав и интересов от криминальной конкуренции со стороны социальных организаций и физических лиц, называется

a) Система безопасности предприятия
b) Служба безопасности предприятия
c) Служба режима и охраны предприятия
d) Отдел работы с конфиденциальной информацией

6. Обследование защищаемых помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования - это задачи отдела

a) режима и охраны
b) инженерно-технической безопасности
c) информационно-аналитической деятельности
d) по работе с конфиденциальной безопасностью

7. Соглашение с сотрудником (обязательство сотрудника) о неразглашении КИ предприятия, подписываемое сотрудником при приеме на работу должно содержать

a) Обязательство о сохранении конфиденциальной информации
b) Право сотрудника на служебное произведение
c) Ответственность сотрудника за нарушение данного обязательства
d) Право на засекречивание информации

8. Органы, государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований ФЗ "О персональных данных" ...

a) регуляторы
b) операторы
c) контролеры
d) надзорные органы

9. Категория персональных данных можно отнести сведения о национальной принадлежности человека…

a) специальные
b) биометрические
c) дополнительные
d) общедоступные

10. Автоматизированные системы обработки информации (АС) классифицируются по следующим признакам

a) **уровень полномочий субъектов доступа АС к конфиденциальной** информации
b) средства защиты информации, которые используются в АС
c) режим обработки данных в АС
d) наличие в АС информации различного уровня конфиденциальности

11. Персональные данные, для которых не требуется обеспечение безопасности в соответствии с ФЗ “О персональных данных”

a) биометрические
b) специальные
c) обезличенные
d) общедоступные

12. Вид атаки направленный на получение конфиденциальной информации путем прослушивания сети

a) анализ сетевого трафика
b) сканирование сети
c) навязывание ложного маршрута
d) внедрение ложного объекта

13. Документ, отражающий полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПД – чтение, запись, корректировка, удаление

a) матрица доступа
b) частная модель угроз
c) список лиц, допущенных к обработке ПД
d) положение по обеспечению безопасности персональных

14. Персональные данные при их обработке в ИСПД должны быть защищены (выберите несколько вариантов ответа)

a) от передачи на носителях, открытых на запись
b) от стихийных бедствий
c) от несанкционированного доступа, в том числе случайного
d) от утечки по техническим каналам утечки

15. Критическая информационная инфраструктура - это ...

a) объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов

b) информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

c) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры

d) комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами

16. С целью снижения вероятности несанкционированного доступа как на территорию предприятия, так и в отдельные подразделения используется

a) метод создания рубежей защиты

b) программно-аппаратные средства защиты

c) метод парольной защиты

d) метод защиты от НСД

17. Совокупность документированных решений, принимаемых руководством организации и направленных на обеспечение информационной безопасности называется

a) Концепция безопасности

b) Политика безопасности

c) Доктрина безопасности

d) Система безопасности

18. Модель нарушителя информационной безопасности определяет

a) категории лиц, в числе которых может оказаться нарушитель

b) мотивационные основания и преследуемые цели нарушителя

c) возможности по осуществлению тех или иных угроз

d) наиболее вероятные способы действий нарушителя

19. К основным средствам инженерно-технической защиты информации относятся

a) физические средства защиты

b) аппаратные средства защиты
c) программные средства защиты
d) математические методы защиты

20. DoS-атака - это

a) Изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.
b) Создание таких условий, при которых правомерные пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам).
c) Пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа.
d) Попытка одного субъекта выдать себя за другого.

21. Совокупностью объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал, называют

a) Техническое средство обнаружения
b) Технический канал утечки информации
c) Информационное поле
d) Программно-аппаратная закладка

22. Организация и поддержание пропускного и внутри объектного режима; организация и установление мер физической и технической защиты зданий и помещений; организация, разработка и контроль системы безопасности в повседневных и в особых условиях - это задачи отдела

a) режима
b) режима и охраны
c) охраны
d) внешней деятельности

23. Защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования называется

a) криптографическая защита конфиденциальной информации
b) техническая защита конфиденциальной информации
c) организационная защита конфиденциальной информации

d) правовая защита конфиденциальной информации

24. Различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа

a) аппаратные средства защиты информации
b) программные средства защиты информации
c) физические средства защиты информации
d) математические средства защиты информации

25. Предотвращает доступ к системе нежелательных лиц, разрешает вход для легальных пользователей

a) аутентификация
b) авторизация
c) идентификация
d) программное обеспечение

26. Позволяет субъекту-пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя

a) аутентификация
b) авторизация
c) идентификация
d) протоколирование

27. Процесс фиксации и анализа накопленной информации, связанной с доступом к защищаемым системным ресурсам

a) транзакция
b) авторизация
c) аудит
d) идентификация

28. Процесс предоставления определённому лицу или группе лиц прав на выполнение определённых действий

a) аутентификация
b) авторизация
c) аудит
d) протоколирование

29. Плохие, слабые пароли обладают следующими признаками:

a) Содержат менее восьми символов

b) Содержат фамилию, кличку животного, имена друзей, сотрудников, вымышленных персонажей

c) Содержат даты рождения и иную личную информацию, например, адреса и номера телефонов

d) Содержат сочетание букв верхнего и нижнего регистров

30. Для назначения разрешений пользователям и локальным группам для общей папки следует воспользоваться

a) Вкладкой **Настройки** диалогового окна свойств общей папки.

b) Вкладкой **Доступ** диалогового окна свойств общей папки.

c) Вкладкой **Общие** диалогового окна свойств общей папки.

d) Вкладкой Безопасность диалогового окна свойств общей папки.

31. Выберите методы усиления механизмов парольной системы защиты

a) ключи i-button

b) смарт-карты

c) идентификаторы e-token

d) идентификаторы ru-token

32. По умолчанию межсетевой экран должен

a) запретить весь входящий трафик

b) разрешить весь исходящий трафик

c) разрешить весь входящий трафик

d) запретить весь исходящий трафик

33. Политика межсетевого экрана определяет

a) как межсетевой экран будет обрабатывать сетевой трафик для определенных IP-адресов и диапазонов адресов, протоколов, приложений и типов содержимого

b) как межсетевой экран будет обеспечивать балансировку нагрузки

c) как межсетевой экран будет обеспечивать качество обслуживания

d) как межсетевой экран будет маршрутизировать пакеты

34. Выберите физические биометрические характеристики, которые могут быть использованы при аутентификации пользователя

a) геометрическая форма руки

b) радужная оболочка глаза

c) геометрическая форма лица

d) голос

Примеры практических задач

1. Выделить нормативно-правовые акты, которыми руководствуется организация для обеспечения информационной безопасности (законы, ГОСТы, РД, Указы …)

2. Выявить угрозы информационной безопасности организации.

3. Составить перечень конфиденциальной информации организации.

4. Провести анализ защищенности ЛВС.

5. Разработка плана по установке, настройка антивируса, проверки его работоспособности.

6. Разработка подсистемы разграничения доступа к файлу, директории и принтеру средствами операционной системы Windows (демонстрация).

7. Разработка подсистемы разграничения доступа к файлу, директории и принтеру средствами операционной системы LINUX (демонстрация)..

8. Разработка парольной политики и настроить её средствами операционной системы Windows.

9. Разработка парольной политики и настроить её средствами операционной системы LINUX.

12. Разработка подсистемы защиты от НСД. Установка и администрирование системы защиты информации SecretNet.

13. Разработка подсистемы защиты от НСД. Установка и администрирование системы защиты информации DallasLock.

14. Разработка основных направлений политики информационной безопасности.

15. Разработка системы контроля управления доступом в организацию.