

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


УТВЕРЖДАЮ
Документов
Директор ОГБПОУ СмолАПО
М. В. Белокопытов

**ПРОГРАММА ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ**

«Кибер-безопасность и защита данных»

Смоленск
2020 г.

1. Наименование программы профессиональной переподготовки:

Кибер-безопасность и защита данных

2. Общая характеристика образовательной программы

2.1. Цель реализации программы:

Формирование общих представлений о безопасности в информационном обществе, технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам, понимание технологий информационной безопасности и умения применять правила кибер-безопасности во всех сферах деятельности.

Программа адаптирована для лиц с особыми потребностями с целью развития их 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.

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

По итогам обучения слушателям, освоившим программу *«Кибер-безопасность и защита данных»* и прошедшим итоговую аттестацию, выдаются дипломы установленного образца, которые удостоверяют право (соответствие квалификации) специалиста на ведение профессиональной деятельности в области «Информационной безопасности».

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 профессиональной переподготовки, должен обладать следующими компетенциями:

– способность к выполнению работ по обеспечению функционирования телекоммуникационного оборудования корпоративных сетей с учетом требований информационной безопасности,

– выявлять и анализировать возможные угрозы информационной безопасности объектов,

– способность проводить анализ проектных решений по обеспечению безопасности компьютерных систем и сетей,

– способность эксплуатировать системы и средства обеспечения информационной безопасности компьютерных систем и сетей,

– способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов телекоммуникационных систем.

По итогам освоения программы слушатель должен:

Знать:

– объекты компьютерных технологий, используемые в обеспечении кибер-безопасности,

– понятийный аппарат информационных технологий и особенности терминологии кибер-безопасности,

– базовые составляющие в области развития систем информационной безопасности,

– объекты компьютерно-технической экспертизы.

Уметь:

- ставить цели, формулировать задачи, связанные с обеспечением кибер-безопасности,
- анализировать тенденции развития систем обеспечения кибер-безопасности,
- применять знания о кибер-безопасности в решении поставленных задач.

Владеть:

- знаниями о современных технологиях, применяемых в области кибер-безопасности;
- методами проведения анализа в области обеспечения кибер-безопасности.

3. Учебный и учебно-тематический планы

УЧЕБНЫЙ ПЛАН

программы профессиональной переподготовки

«Кибер-безопасность и защита данных»

Требования к уровню образования поступающих на обучение	Обучение по настоящей программе 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	16 недель
Форма обучения	очная, очно-заочная с применением дистанционных образовательных технологий

№№ п/п	Наименование дисциплины (модуля)	Всего часов трудоемкости	В том числе				Самостоятельная работа*	Форма контроля
			Аудиторные занятия*					
			Всего, часов	из них				
Лекции	Практические занятия							
1	2	3	4	5	6	7	8	
1	Организационные и правовые основы профессиональной деятельности по защите информации	30	24	12	12	6	Зачет	
2	Кибер-безопасность: основные понятия и определения	14	10	6	4	4	Зачет	
3	Кибер-безопасность: защита сетевой системы и данных. Виды защищаемой	32	26	14	12	6	Зачет	

* С применением дистанционных образовательных технологий и электронного обучения

	информации						
4	Хакерские атаки и кибертерроризм. Кибервойны.	24	20	10	10	4	Зачет
5	Проблемы безопасности инфраструктуры Интернета	26	20	8	12	6	Зачет
6	Уязвимости системы безопасности и эксплойты. Внутренние и внешние угрозы.	32	26	14	12	6	Зачет
7	Типы и симптомы вредоносного ПО. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	32	26	14	12	6	Зачет
8	Защита данных и конфиденциальности	30	26	14	12	4	Зачет
9	Организация и проведение работ по технической защите информации в компьютерных сетях и системах	32	26	14	12	6	Зачет
	Всего:	252	204	106	98	48	
	Итоговая аттестация		4				Итоговая аттестация
	Общая трудоемкость программы	256					

Учебно-тематический план программы профессиональной переподготовки

№ № п/п	Наименование дисциплины (модуля)	Трудо- емкость В часах	В том числе				Самостоятель- ная работа*	Форма контроля
			Аудиторные занятия *			Практи- ческие занятия		
			Всего, часов	из них				
		Лек- ции						
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	
1	Модуль 1. Организационные и правовые основы профессиональной деятельности по защите информации	30	24	12	12	6	Зачет	
2	Тема 1.1 Понятие информационной безопасности и её место в системе национальной безопасности	14	10	6*	4*	2	Тестиро- вание Практичес- кое задание	

* С применением дистанционных образовательных технологий и электронного обучения

3	<i>Тема 1.2</i> Законодательство в области информационных технологий и защиты информации	18	14	6*	8*	4	Тестирование Практическое задание
4	<i>Модуль 2.</i> Кибер-безопасность: основные понятия и определения	14	10	6	4	4	Зачет
5	<i>Тема 2.1.</i> Кибер-безопасность: основные понятия и определения	12	10	6*	4*	2	Тестирование Практическое задание
6	<i>Модуль 3.</i> Кибер-безопасность: защита сетевой системы и данных. Виды защищаемой информации	32	26	14	12	6	Зачет
7	<i>Тема 3.1</i> Виды защищаемой информации	16	14	2 6*	6*	2	Тестирование Практическое задание
8	<i>Тема 3.2</i> Защита данных	14	12	2 4*	6	2	Тестирование Практическое задание
9	<i>Модуль 4.</i> Хакерские атаки и кибертерроризм. Кибервойны.	24	20	10	10	4	Зачет
10	<i>Тема 4.1</i> Хакерские атаки и кибертерроризм. Кибервойна	24	20	4 6*	4 6*	4	Тестирование Практическое задание
11	<i>Модуль 5.</i> Проблемы безопасности инфраструктуры Интернета	26	20	8	12	6	Зачет
12	<i>Тема 5.1</i> Проблемы безопасности инфраструктуры Интернета	12	10	2 2*	4 2*	2	Тестирование Практическое задание
13	<i>Тема 5.2</i> Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	12	10	4*	6*	2	Тестирование Практическое задание
14	<i>Модуль 6.</i> Уязвимости системы безопасности и эксплойты. Внутренние и внешние угрозы.	32	26	14	12	6	Зачет
15	<i>Тема 6.1</i> Внутренние и внешние угрозы	14	12	6*	2 4*	2	Тестирование

* С применением дистанционных образовательных технологий и электронного обучения

* С применением дистанционных образовательных технологий и электронного обучения

							Практическое задание
16	Тема 6.2 Уязвимости системы безопасности и эксплойты	16	14	4 4*	4 2*	2	Тестирование Практическое задание
17	Модуль 7. Типы и симптомы вредоносного ПО. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	32	26	14	12	6	Зачет
18	Тема 7.1 Методы обеспечения безопасности ПК и интернета	16	14	2 6*	2 4*	2	Тестирование Практическое задание
19	Тема 7.2 Вирусы и антивирусы	14	12	6*	4 2*	2	Тестирование Практическое задание
20	Модуль 8. Защита данных и конфиденциальности	30	26	14	12	4	Зачет
21	Тема 8.1 Защита данных и конфиденциальности	14	12	6*	2 4*	2	Тестирование Практическое задание
22	Тема 8.2 Устройства безопасности	16	14	4 4*	2 4*	2	Тестирование Практическое задание
23	Модуль 9. Организация и проведение работ по технической защите информации в компьютерных сетях и системах	32	26	14	12	6	Зачет
24	Тема 9.1 Система защиты информации и требования, предъявляемые к ней	14	12	6*	6*	2	Тестирование Практическое задание
25	Тема 9.2 Организационно-технические мероприятия по защите информации	16	14	2 4*	2 4*	2	Тестирование Практическое задание
	Всего:	252	204	106	98	48	
	Итоговая аттестация		4				Итоговая аттестация
	Общая трудоемкость программы	256					

* С применением дистанционных образовательных технологий и электронного обучения

4. Календарный учебный график

Программа профессиональной переподготовки *«Кибер-безопасность и защита данных»*

Объем программы 256 часов.

Продолжительность обучения 16 недель

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.

. Содержание программы

Модуль 1. Организационные и правовые основы профессиональной деятельности по защите информации

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.

Тема 1.2 Законодательство в области информационных технологий и защиты информации

Обзор законодательства России в области информационной безопасности. Характеристика стандартов в области информационной безопасности.

Модуль 2. Кибер-безопасность: основные понятия и определения

Тема 2.1. Кибер-безопасность: основные понятия и определения

Кибер-безопасность (информационная безопасность): основные стандарты, понятия, определения. Обзор основных проблем, связанных с кибер-безопасностью; основные угрозы и уязвимости в сфере кибер-безопасности.

Модуль 3. Кибер-безопасность: защита данных. Виды защищаемой информации

Тема 3.1 Виды защищаемой информации

Свойства информации как предмета защиты. Основные виды конфиденциальной информации, подлежащих защите.

Тема 3.2 Защита данных

Составляющие информационной безопасности: целостность, доступность конфиденциальность. Персональные данные. Организационные данные.

Модуль 4. Хакерские атаки и кибертерроризм. Кибервойна.

Тема 4.1 Хакерские атаки и кибертерроризм. Кибервойна

Характеристики и мотивы злоумышленников. Типы злоумышленников. Кибервойна. Конфликты в киберпространстве.

Модуль 5. Проблемы безопасности инфраструктуры Интернета

Тема 5.1 Проблемы безопасности инфраструктуры Интернета

Протоколы маршрутизации сети, система доменных имен, средства маршрутизации. Проверка подлинности (аутентификация) в Интернете. Меры безопасности для пользователя WiFi. Настройка безопасности.

Тема 5.2 Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости

Понятие безопасности персонального компьютера. Настройка компьютера для безопасной работы. Ошибки пользователя. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях

Модуль 6. Внутренние и внешние угрозы. Уязвимости системы безопасности и эксплойты

Тема 6.1 Внутренние и внешние угрозы

Особенности современных информационных систем как объекта защиты информации. Классификация угроз безопасности информации. Характеристика основных угроз НСД и способов их реализации.

Тема 6.2 Уязвимости системы безопасности и эксплойты

Уязвимости программного и аппаратного обеспечения. Типы уязвимостей системы безопасности. Характеристика основных классов атак, реализуемых в сетях общего пользования. Методы оценки опасности угроз.

Модуль 7. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы

Тема 7.1 Методы обеспечения безопасности ПК и интернета

Технологии защиты. Стратегии снижения рисков. Аудит безопасности. Мониторинг инцидентов кибер-безопасности. Реагирование на инциденты кибер-безопасности.

Тема 7.2 Вирусы и антивирусы

Вредоносное программное обеспечение. Типы и симптомы вредоносного ПО. Способы проникновения. Антивирусные программы.

Модуль 8. Защита данных и конфиденциальности

Тема 8.1 Защита данных и конфиденциальности

Защита персональных данных в сети. Защита устройств и сети. Ведение данных.

Тема 8.2 Устройства безопасности

Устройства безопасности. Обнаружение атак в реальном времени, обнаружение вредоносного ПО. Инструменты для предотвращения и обнаружения инцидентов

Модуль 9. Организация и проведение работ по технической защите информации в компьютерных сетях и системах

Тема 9.1 Система защиты информации и требования, предъявляемые к ней

Особенности современных информационных систем как объекта защиты информации. Практические методики по информационной безопасности

Тема 9.2 Организационно-технические мероприятия по защите информации

Организационно-технические мероприятия по защите информации. Вопросы проектирования, внедрения и эксплуатации АС и их систем защиты 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 карт 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 считыватель ключей 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 виртуализации VMWare 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

Нормативно-правовые документы

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

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

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

4. Федеральный закон «О государственной тайне» от 21.07.1993 г. № 5485-1 (последняя редакция).

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

6. ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (утвержден и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст)

Основная литература

1. Олифер В. Г. Безопасность компьютерных сетей. Издательство: Горячая линия- Телеком. 2016.

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

3. *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. *Петренко С. А., Смирнов М. Б.* Безопасность АСУТП и критической информационной инфраструктуры // СПб.: ООО «ИД «Афина». – 2018. ISBN 978-5-9909868-1-7. Учебно-методическое пособие [Электронная версия]

2. - *Марков А.С., Цирлов В.Л.* Руководящие указания по кибербезопасности в контексте ISO 27032. Вопросы кибербезопасности № 1(12) 2014. С. 28-35

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.

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. Формы текущего контроля успеваемости

При проведении всех форм 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.

Преподаватель оценивает работу слушателя на практических занятиях и самостоятельную работу над домашним заданием. Оценки за работу на практических занятиях и самостоятельную работу слушателя преподаватель выставляет в рабочую ведомость, а также результаты прохождения тестов с использованием электронного обучения и дистанционных образовательных технологий.

Практическое задание оценивается преподавателем по 5-балльной шкале. Оценки 5, 4 и 3 – положительные. Оценки 1, 2 – неудовлетворительные и означают, что практическое задание считается невыполненным.

На текущем контроле знаний, в объеме изученного материала, слушатель должен продемонстрировать знание:

- основных понятий в области кибер-безопасности; основных угроз, рисков и уязвимостей в сфере кибер-безопасности,
- основных протоколов передачи данных и аутентификации,
- положений основных нормативных актов, регулирующих сферу кибер-безопасности Российской Федерации,
- архитектуры основных подсистем обеспечения ИБ.
- основных определений системы менеджмента информационной безопасности.

При выполнении домашних заданий и самостоятельной работы слушатель должен продемонстрировать знание:

- основных средств обеспечения кибер-безопасности (принципы построения);
- принципов проектирования систем безопасности,
- состава и способов организации деятельности сил обеспечения кибер-безопасности,
- основных требований к специалистам в области кибер-безопасности,
- целей обеспечения кибер-безопасности,
- классификации и примеров угроз, уязвимостей, рисков,
- основных рисков и проблем кибер-безопасности,

7.2. Формы промежуточной аттестации

Промежуточная аттестация осуществляется по накопительной системе. Для получения зачета по каждому модулю слушатель должен выполнить с положительной отметкой одно задание по каждой теме и успешно пройти тестирование.

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.

Наличие зачетов по всем модулям программы является условием допуска к итоговой аттестации.

Примеры тестовых заданий и примерный перечень вопросов к различным формам промежуточной аттестации приведены в приложении А.

7.1. Форма итоговой аттестации

Итоговая аттестация по программе профессиональной переподготовки «Кибер-безопасность и защита данных» в форме защиты итоговой аттестационной работы.

Примерные темы для подготовки аттестационной работы:

- задачи и уровни обеспечения защиты киберпространства, аспекты кибер-безопасности,
- национальные стандарты России в области кибер-безопасности,
- проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации),
- характеристика современного вредоносного программного обеспечения и виды кибератак,
- новые технологии и новые угрозы информационной безопасности,
- особенности современных информационных систем как объекта защиты информации,
- основные угрозы, риски и уязвимости в сфере кибер-безопасности и критической информационной инфраструктуры,
- положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации,
- архитектура основных подсистем обеспечения информационной безопасности объектов,
- основные определения системы менеджмента информационной безопасности и особенности построения системы менеджмента информационной безопасности;
- основные средства обеспечения кибер-безопасности (архитектура, принципы построения),
- принципы проектирования систем безопасности значимых объектов критической информационной инфраструктуры,

- состав и способы организации деятельности сил обеспечения кибербезопасности объектов,
- основные риски и проблемы усовершенствования системы кибербезопасности
- состав и классификация систем безопасности, критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз,
- хакерские атаки и кибертерроризм, последствия кибератак,
- уязвимости системы безопасности, основные внутренние и внешние угрозы,
- типы и симптомы современного вредоносного программного обеспечения и методы борьбы с ними,
- современные угрозы социальных сетей, меры личной безопасности при сетевом общении,
- риски интернета (контентные, электронные, коммуникационные, потребительские),
- виды хакерских атак и способы защиты от них,
- кибертерроризм: понятие, приемы, способы предотвращения,
- информационное противоборство в бизнесе и кибер-безопасность,
- конфиденциальность информации, угрозы конфиденциальной безопасности,
- механизмы обеспечения конфиденциальности данных и требования к ним,
- характеристика основных угроз НСД и способов их реализации,
- характеристика основных классов атак, реализуемых в сетях общего пользования.

В процессе подготовки аттестационной работы слушателю следует:

- изучить отечественную и зарубежную научную литературу, и аналитические материалы по теме исследования, имеющиеся статистические данные;

- определить современные разработки в научной литературе
- провести анализ основных научно-теоретических концепций по изучаемой проблеме;
- раскрыть возможности применения полученных решений к решению практических задач в сфере информационной безопасности сформулировать выводы и предложения.

ПРИЛОЖЕНИЕ А

Примеры тестовых заданий

1. *Постоянная работа по защите подключенных к Интернету сетевых систем и всех данных от несанкционированного использования или причинения вреда ... (кибербезопасность),*

2. *Компоненты тройки CIA... (Конфиденциальность (confidentiality), целостность (integrity) и доступность (availability)),*

3. *Неприкосновенность данных или приватностью, что означает, что доступ к данным ограничен только авторизованным персоналом ... (конфиденциальность),*

4. *Шифрование данных, идентификация по имени пользователя и паролю, двухфакторная аутентификация и т. д. ... (способы обеспечения конфиденциальности),*

5. *Термин, обозначающий точность, согласованность данных и доверие к ним ... (целостность),*

6. *Права доступа к файлам, контроль доступа пользователей, контроль версий и контрольная сумма ... (способы обеспечения целостности),*

7. *Термин, описывающий качественное обслуживание сервисов и данных и возможность доступа к ним в любой момент ... (доступность),*

8. *Люди или организации, которые взламывают сети или компьютерные системы, чтобы выявить их недостатки с целью повысить безопасность этих систем ... (белые хакеры),*

9. *Люди или организации, которые используют любые уязвимости для получения личной, финансовой или политической выгоды незаконным путем ... (черные хакеры),*

10. *Интернет-конфликт, связанный с проникновением в компьютерные системы и сети других стран ... (кибервойна),*

11. *Аппаратный или программный дефект, которым злоумышленники могут воспользоваться для взлома системы ... (уязвимость),*

12. Программа, написанная с целью воспользоваться известной уязвимостью системы безопасности ... (эксплойт),

13. Действие по использованию эксплойта для уязвимости с целью взлома выбранной системы... (кибератака),

14. Недостатки системы безопасности, связанные с упущениями в конструкции вычислительных устройств и компонентов. Обычно относятся к определенным моделям устройств и используются в целевых атаках ... (уязвимости аппаратного обеспечения),

15. Уязвимость программного обеспечения, которая происходит, когда данные записываются за пределами областей памяти, выделенных для приложения. Эта уязвимость может позволить приложению обращаться к памяти, выделенной другим процессам ... (переполнение буфера),

16. 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.

17. 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.

18. Оценка рисков позволяет ответить на следующие вопросы:

- 1) Как спроектировать надежную защиту?
- 2) Какую политику безопасности предпочесть?
- 3) Какие защитные средства экономически целесообразно использовать?

19. Окно опасности появляется, когда:

- 1) становится известно о средствах использования уязвимости;
- 2) появляется возможность использовать уязвимость;
- 3) устанавливается новое программное обеспечение.

20. Окно опасности перестает существовать, когда:

- 1) администратор безопасности узнает об угрозе;
- 2) производитель программного обеспечения выпускает заплату;
- 3) заплатка устанавливается в защищаемой информационной системе.

21. 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.

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. 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.

27. 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.

28. 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.

29. 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.

30. Идентификация это:

а) процесс предъявления пользователем идентификатора.

б) процесс подтверждения подлинности.

в) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов.

Примерный перечень вопросов к различным формам текущего контроля и промежуточной аттестации:

- основные понятия в области кибер-безопасности,
- основные угрозы, риски и уязвимости в сфере кибер-безопасности,
- основные протоколы передачи данных и аутентификации,
- положения основных нормативных актов, регулирующих сферу безопасности Российской Федерации;
- архитектура основных подсистем обеспечения ИБ;
- основные определения системы менеджмента информационной безопасности,
- положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения информационной безопасности,
- основные средства обеспечения кибер-безопасности (архитектура, принципы построения),
- принципы проектирования систем безопасности,
- состав и способы организации деятельности сил обеспечения кибер-безопасности,
- основные требования к специалистам в области кибер-безопасности,
- определение персональных данных, характеристики и ценность персональных данных,
- характеристики и ценность данных в организации,
- последствия нарушения безопасности,
- характеристики и мотивы злоумышленников,
- характеристики и цель кибервойн,
- уязвимости системы безопасности и их использование,
- типы вредоносного ПО и его признаки, способы проникновения и методики, используемые для отказа в обслуживании,
- защита устройств и сети от угроз,
- процедуры безопасности для ведения данных,

- способы аутентификации и правила безопасного поведения в сети,
- типы межсетевых экранов и устройств безопасности,
- способы обнаружения вредоносного ПО и атак в реальном времени,
- практические методики для организации,
- определение ботнета, убийственной цепочки и безопасности на основе поведения,
- цель сборника сценариев по информационной безопасности,
- инструменты, используемые для обнаружения и предотвращения инцидентов.

Примерный перечень заданий к различным формам текущего контроля и промежуточной аттестации:

- поиск своих персональных данных,
- сравнение данных с помощью хэш-функции,
- поиск информации о нескольких последних случаях нарушения безопасности (на примерах организаций),
- создание и хранение надежных паролей,
- резервное копирование данных во внешнее хранилище,
- изучение юридических соглашений о принадлежности ваших данных, когда они не хранятся в локальной системе,
- анализ своих действий в Интернете, которые могут скомпрометировать Вашу безопасность или конфиденциальность,
- выявление угроз информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации),
- идентификация угроз, изучение угроз, исходящих от кибератак,
- выявление уязвимостей, связанных с данными,
- усиление безопасности вашей учетной записи,
- установка виртуальной машины на ПК,
- выбор соответствующих методов аутентификации, авторизации или разграничения доступа для заданного сценария,

- использование лучших практик установки и настройки средств контроля безопасности при управлении учетными записями,
- обнаружение угроз и уязвимостей,
- демонстрация использования цифровых подписей, демонстрация проверки цифровых подписей,
- повышение надежности системы Linux,
- установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла,
- разграничение доступа к файлу, директории и принтеру средствами операционной системы Windows,
- разграничение доступа к файлу, директории и принтеру средствами операционной системы Linux,
- настройка аудита обращений к файлу от имени владельца средствами операционной системы Windows,
- настройка аудита обращений к файлу от имени владельца средствами операционной системы Linux,
- настройка политики паролей средствами операционной системы Windows,
- настройка политики паролей средствами операционной системы Linux,
- проверка компьютерной системы на наличие вредоносного программного обеспечения,
- проверка целостности файлов и данных,
- повышение надежности конфигурации IOS.