ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ ИМ. Б.Л. РОЗИНГА
(ФИЛИАЛ) СПбГУТ
(АКТ (ф) СПбГУТ)

СОГЛАСОВАНО
Зам. директора по учебной работе
_____Н.В. Калинина
«24» 09 2020 г.

УТВЕРЖДАЮ
Директор АКТ (ф) СПбГУТ
_____А.П. Топанов
«__» _____ 2020 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

Архангельск 2020

Составитель:

А.А. Зубарев, преподаватель высшей квалификационной категории АКТ (ф) СПбГУТ.

Программа рассмотрена и одобрена цикловой комиссией Информационной безопасности инфокоммуникационных систем

Протокол № 1 от 24 января 2020г.

Председатель_____ А.А. Зубарев

2

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

1.1 Пояснительная записка

В условиях формирования инновационной экономики к системе профессионального образования предъявляют такие требования, как постоянное обновление технологий, ускоренное освоение инноваций, быстрая адаптация к запросам и требованиям. В этой связи активно внедряются стандарты WorldSkills в образовательный процесс.

Настоящая программа предназначена для повышения квалификации слушателей в области реализация образовательным программ с применением стандартов WorldSkills по направлению защита персональных данных (которое является составляющей частью компетенции WorldSkills «Кибер-безопасность»).

Нормативно-правовой основой для разработки программы являются:

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

– Приказ Минобрнауки России от 01.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утверждены Министром образования и науки Российской Федерации 22.01.2015 г. № ДЛ-1/05вн).

1.2 Целевая аудитория

Программа предназначена для слушателей ведущих свою деятельность в области информационной безопасности (имеющих высшее или среднее профессиональное образование), а также преподавателей учебных дисциплин и МДК общепрофессиональных и профессиональных циклов, мастеров производственного обучения, учителей информатики образовательных организаций.

1.3 Цель программы и планируемые результаты обучения

Целью реализации программы является совершенствование профессиональной компетенции сотрудников организации в части сопровождение системы защиты информации в ходе её эксплуатации, проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации, проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации, а также педагогических работников системы

профессионального образования, учителей информатики в области реализации образовательных программ.

В результате успешного освоения программы слушатель должен

уметь:

– применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– контролировать соблюдение персоналом требований режима защиты информации;

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

знать:

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспертному контролю в данной области;

– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

– правовые нормы и стандарты по лицензированию в области защиты государственной тайны и сертификации средств защиты информации;

– принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности на предприятиях.

1.4 Нормативный срок освоения программы повышения квалификации

Нормативный срок освоения программы повышения квалификации составляет 42 часов, в том числе дистанционно – 12 часов.

1.5 Порядок аттестации слушателей

Текущий контроль знаний проводится по результатам выполнения практических работ, прохождения тестов.

Итоговая аттестация

Повышение квалификации завершается итоговой аттестацией, которая проходит в форме сдачи зачёта.

По завершении обучения слушателям выдается удостоверение о повышении квалификации.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

2.1 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный график формируется непосредственно при реализации программы повышения квалификации «Защита персональных данных». Календарный учебный график представлен в форме расписания занятий при наборе группы на обучение.

2.2 УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

№ п/п	Наименование разделов, модулей	Трудоемкость, ч.	Всего, ч.	в том числе					Самостоятельная работа, ч.	Форма аттестации
				Аудиторные занятия, ч.			Занятия с использованием ДОТ, ч			
				лекции	лабораторные занятия	практические занятия	лекции	практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
1	**Модуль 1 Основные понятия защиты информации (ЗИ)**	**2**	**2**	0	0	0	2	0	**0**	Тест
2	**Модуль 2 Правовое обеспечение ЗИ**	**7**	**6**	0	0	4	2	0	**1**	Практические работы №№1-2
3	**Модуль 3 Организационное обеспечение ЗИ**	**7**	**6**	0	0	4	2	0	**1**	Практические работы №№3-4
4	**Модуль 4 Виды тайн**	**2**	**2**	0	0	0	2	0	**0**	Тест
5	**Модуль 5 Правовые обеспечения защиты персональных данных**	**11**	**10**	0	0	8	2	0	**1**	Практические работы №№5-8

1	2	3	4	5	6	7	8	9	10	11
6	**Модуль 6 Организационное обеспечение защиты персональных данных.**	**13**	**12**	0	0	10	2	0	**1**	Практическая работа №9-12 Итоговый тест
	Итого:	**42**	**38**	0	0	26	12	0	**4**	**Зачёт**

2.3 УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

№ п/п	Наименование разделов, модулей	Всего часов, ч.	Из них						Форма аттестации
			Аудиторные занятия, ч.			Занятия с использованием ДОТ, ч		Самостоятельная работа, ч.	
			лекции	лабораторные занятия	практические занятия	лекции	практические занятия		
1	2	3	4	5	6	7	8	9	10
1	**Модуль 1 Основные понятия защиты информации (ЗИ)**	**2**	**0**	**0**	**0**	**2**	**0**	**0**	
1.1	Тема 1.1 Введение. Структура модуля. Основные понятия защиты информации.	2	0	0	0	2	0	0	Тест
2	**Модуль 2 Правовое обеспечение ЗИ**	**7**	**0**	**0**	**4**	**2**	**0**	**1**	
2.1	**Тема 2.1** Правовое обеспечение ЗИ. Основные правовые документы. Принципы, методы и способы правового регулирования защиты информации.	7	0	0	4	2	0	1	Практические работы №№1-2
2.2	**Практическая работа №1** Работа в программе Консультант Плюс.								
2.3	**Практическая работа №2** Поиск правовых документов в программе Консультант Плюс.								

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
2.4	**Самостоятельная работа** в подготовке к практическим занятиям: работа с конспектом лекций, работа с литературой.								
3	**Модуль 3 Организационное обеспечение ЗИ**	**7**	**0**	**0**	**4**	**2**	**0**	**1**	
3.1	**Тема 3.1** Система обеспечения информационной безопасности Российской Федерации. Государственная информационная политика. Государственная система защиты информации, состав, структура и функции. Функции и задачи органов исполнительной власти, уполномоченных в области ИБ (ФСО, ФСБ, ФСТЭК, Роскомнадзор).	7	0	0	4	2	0	1	Практические работы №№3-4
3.2	**Практическая работа №3** Изучение ФЗ №149-ФЗ «Об информации, информационных технологиях и о защите информации»								
3.3	**Практическая работа №4** Изучение функций и задач органов исполнительной власти, уполномоченных в области ИБ.								
3.4	**Самостоятельная работа** в подготовке к практическим занятиям: работа с конспектом лекций, работа с литературой.								
4	**Модуль 4 Виды тайн**	**2**	**0**	**0**	**0**	**2**	**0**	**0**	
4.1	Тема 4.1 Основные понятия служебной и конфиденциальной информации. Конфиденциальная информация.	2	0	0	0	2	0	0	Тест
5	**Модуль 5 Правовые обеспечения защиты персональных данных**	**11**	**0**	**0**	**8**	**2**	**0**	**1**	

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
5.1	Тема 5.1 Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации предприятия по защите персональных данных. Требование к документации юридических лиц по защите персональных данных. Требования к документации по обработке персональных данных работников. Типовые документы, регламентирующие получение, обработку, хранение и передачу персональных данных. Планирование мероприятий по защите персональных данных. Угрозы безопасности персональных данных. Классификация информационных систем персональных данных (ИСПДн).	11	0	0	8	2	0	1	Практические работы №№5-8
5.2	**Практическая работа №5** Изучение ФЗ № 152-ФЗ «О персональных данных»								
5.3	**Практическая работа №6** Изучение порядка работы с персональными данными работника.								
5.4	**Практическая работа №7** Планирование мероприятий по защите персональных данных.								
5.5	**Практическая работа №8** Изучение методов обезличивания персональных данных.								

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
5.6	**Самостоятельная работа** в подготовке к практическим занятиям: работа с конспектом лекций, работа с литературой.								
6	**Модуль 6 Организационное обеспечение ЗИ**	**13**	**0**	**0**	**10**	**2**	**0**	**1**	
6.1	Тема 6.1 Основы организации и обеспечения комплексной защиты персональных данных при их обработке в ИСПДн. Порядок создания и эксплуатации ИСПДн. Методы работы с постоянными сотрудниками. Административно-правовые нарушения в области связи и информации. Ответственность за нарушение требований по защите персональных данных. Система государственного надзора и контроля в области персональных данных. Проверка персонала при приеме на работу.	11	0	0	8	2	0	1	Практические работы №№9-12
6.2	**Практическая работа №9** Риск-подход к моделированию угроз ИБ.								
6.3	**Практическая работа №10** Подготовка объекта к аттестации. Типовые формы документов.								
6.4	**Практическая работа №11** Изучение моделей угроз безопасности персональных данных при их обработке в информационных системах.								

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
6.5	**Практическая работа №12** Изучение типовых форм документов, предполагающих или допускающих содержание персональных данных.								
6.7	**Самостоятельная работа** в подготовке к практическим занятиям: работа с конспектом лекций, работа с литературой.								
6.8	Итоговая аттестация	2	0	0	2	0	0	0	Итоговый тест
	Итого:	**42**	**0**	**0**	**26**	**12**	**0**	**4**	**Зачёт**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

3.1 Для реализации программы повышения квалификации должны быть предусмотрены следующие специальные помещения:

Мастерская по компетенции Кибер-безопасность, оснащенная оборудованием и техническими и программными средствами обучения:

доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., противошумовые наушники - 10 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт.

Кабинет информационной безопасности: учебная доска, рабочее место преподавателя - ПК 1 шт.; рабочие места обучающихся - ПК 14 шт. Программное обеспечение: LibreOffice; Linux; Консультнат +; Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y; программные межсетевые экраны для маршрутизаторов Cisco 1700 (Cisco 1721); программные межсетевые экраны для маршрутизаторов Cisco 2800; коммутатор Cisco Catalyst 2960- 3 шт.

3.2 Информационное обеспечение реализации программы

3.2.1. Печатные или электронные издания

1. Баранова, Е. К. Основы информационней безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - Москва : РИОР : ИНФРА-М, 2019. – 202 с. – URL: https://doi.org/10.29039/01806-4. - ISBN 978-5-16-107531-9. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1014830

2. Бубнов, А.А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Москва: Академия, 2020.

3. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. – Москва : ФОРУМ : ИНФРА-М, 2020. – 368 с. – Текст : электронный. - URL: https://new.znanium.com/catalog/product/1082470

4. Зверева, В. П. Организация и технология работы с конфиденциальными документами : учебное пособие / В.П. Зверева, А.В. Назаров. – Москва : КУРС: ИНФРА-М, 2020. – 320 с. – Текст : электронный. - URL: https://new.znanium.com/catalog/product/1078083

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурин. – Москва : Юрайт, 2020.

3.2.2. Дополнительные источники:

1. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. –Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. –Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/52209.html – Режим доступа: для авторизир. пользователей

2. Ищейнов, В. Я. Основные положения информационной безопасности : учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. – Москва : ФОРУМ : ИНФРА-М, 2018. – 208 с. – Текст : электронный. - URL: https://new.znanium.com/catalog/product/927190

4 ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Форма итоговой аттестации – итоговое тестирование.

Результаты итоговой аттестации оцениваются исходя из следующего количества полученных баллов:

30-38 баллов – «зачтено»;

менее 30 баллов – «не зачтено».

Типовые задания Итогового теста:

1 Основные угрозы доступности информации:

Выберите несколько вариантов ответа:

1) непреднамеренные ошибки пользователей;
2) злонамеренное изменение данных;
3) хакерская атака;
4) отказ программного и аппаратного обеспечения;
5) разрушение или повреждение помещений;
6) перехват данных.

2 Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

Выберите один вариант ответа:

1) С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создаёт информационных угроз для элементов самой системы и внешней среды;
2) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации;
3) способна противостоять только информационным угрозам, как внешним так и внутренним;
4) способна противостоять только внешним информационным угрозам.

3 Методы повышения достоверности входных данных:

Выберите несколько вариантов ответа:

1) замена процесса ввода значения процессом выбора значения из предлагаемого множества;
2) отказ от использования данных;
3) проведение комплекса регламентных работ;
4) использование вместо ввода значения его считывание с машиночитаемого носителя;
5) введение избыточности в документ первоисточник;
6) многократный ввод данных и сличение введенных значений.

4 Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):

Выберите один вариант ответа:

1) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения;

2) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты;

3) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом.

5 Сервисы безопасности:

Выберите несколько вариантов ответа:

1) идентификация и аутентификация;
2) шифрование;
3) инверсия паролей;
4) контроль целостности;
5) регулирование конфликтов;
6) экранирование;
7) обеспечение безопасного восстановления;
8) кэширование записей.

6 Под угрозой удаленного администрирования в компьютерной сети понимается угроза…

Выберите один вариант ответа:

1) несанкционированного управления удаленным компьютером;
2) внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
3) перехвата или подмены данных на путях транспортировки;
4) вмешательства в личную жизнь;
5) поставки неприемлемого содержания.

7 Причины возникновения ошибки в данных:

Выберите несколько вариантов ответа:

1) погрешность измерений;
2) ошибка при записи результатов измерений в промежуточный документ;
3) неверная интерпретация данных;
4) ошибки при переносе данных с промежуточного документа в компьютер;
5) использование недопустимых методов анализа данных;
6) неустранимые причины природного характера;
7) преднамеренное искажение данных;
8) ошибки при идентификации объекта или субъекта хозяйственной деятельности.

8 К формам защиты информации не относится…

Выберите несколько вариантов ответа:

1) аналитическая;
2) правовая;

3) организационно-техническая;
4) страховая.

9 Наиболее эффективное средство для защиты от сетевых атак:
Выберите один вариант ответа:
1) использование сетевых экранов или «firewall»;
2) использование антивирусных программ;
3) посещение только «надёжных» Интернет-узлов;
4) использование только сертифицированных программ-браузеров при доступе к сети Интернет.

10 Информация, составляющая государственную тайну не может иметь гриф…
Выберите один вариант ответа:
1) «для служебного пользования»;
2) «секретно»;
3) «совершенно секретно»;
4) «особой важности».

11 Разделы современной криптографии:
Выберите несколько вариантов ответа:
1) Симметричные криптосистемы
2) Криптосистемы с открытым ключом
3) Криптосистемы с дублированием защиты
4) Системы электронной подписи
5) Управление паролями
6) Управление передачей данных
7) Управление ключами

12 Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:
Выберите один вариант ответа:
1) рекомендации X.800;
2) оранжевая книга;
3) закон «Об информации, информационных технологиях и о защите информации».

13 Утечка информации – это …
Выберите один вариант ответа:
1) несанкционированный процесс переноса информации от источника к злоумышленнику;
2) процесс раскрытия секретной информации;
3) процесс уничтожения информации;
4) непреднамеренная утрата носителя информации.

14 Основные угрозы конфиденциальности информации:

Выберите несколько вариантов ответа:

1) «маскарад»;
2) «карнавал»;
3) переадресовка;
4) перехват данных;
5) блокирование;
6) злоупотребления полномочиями.

15 Элементы знака охраны авторского права:

Выберите несколько вариантов ответа:

1) буквы С в окружности или круглых скобках;
2) буквы Р в окружности или круглых скобках;
3) наименования (имени) правообладателя;
4) наименование охраняемого объекта;
5) года первого выпуска программы.

16 Защита информации обеспечивается применением антивирусных средств:

Выберите один вариант ответа:

1) да;
2) нет;
3) не всегда.

17 Средства защиты объектов файловой системы основаны на…

Выберите один вариант ответа:

1) определении прав пользователя на операции с файлами и каталогами;
2) задании атрибутов файлов и каталогов, независящих от прав пользователей.

18 Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза.

Выберите один вариант ответа:

1) активная;
2) пассивная.

19 Преднамеренная угроза безопасности информации

Выберите один вариант ответа:

1) кража;
2) наводнение;
3) повреждение кабеля, по которому идет передача, в связи с погодными условиями;
4) ошибка разработчика.

20 Концепция системы защиты от информационного оружия не должна включать…

Выберите один вариант ответа:

1) средства нанесения контратаки с помощью информационного оружия;
2) механизмы защиты пользователей от различных типов и уровней угроз для национальной;
3) информационной инфраструктуры;
4) признаки, сигнализирующие о возможном нападении;
5) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей.

21 В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

Выберите несколько вариантов ответа:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
реализацию права на доступ к информации»;
2) соблюдение норм международного права в сфере информационной безопасности;
3) выявление нарушителей и привлечение их к ответственности;
4) соблюдение конфиденциальности информации ограниченного доступа;
5) разработку методов и усовершенствование средств информационной безопасности.

22 Какие законы существуют в России в области компьютерного права?

Выберите несколько вариантов ответа:

1) о государственной тайне;
2) об авторском праве и смежных правах;
3) о гражданском долге;
4) о правовой охране программ для ЭВМ и БД;
5) о правовой ответственности;
6) об информации, информатизации, защищенности информации.

23 Какие существуют основные уровни обеспечения защиты информации?

Выберите несколько вариантов ответа:

1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный

6) процедурный
7) распределительный

24 Физические средства защиты информации

Выберите один вариант ответа:

1) средства, которые реализуются в виде автономных устройств и систем;
2) устройства, встраиваемые непосредственно в аппаратуру АС или;
3) устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;
4) это программы, предназначенные для выполнения функций, связанных с защитой информации;
5) средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

25 В чем заключается основная причина потерь информации, связанной с ПК?

Выберите один вариант ответа:

1) с глобальным хищением информации;
2) с появлением интернета;
3) с недостаточной образованностью в области безопасности;

26 Технические средства защиты информации

Выберите один вариант ответа:

1) средства, которые реализуются в виде автономных устройств и систем;
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;
3) это программы, предназначенные для выполнения функций, связанных с защитой информации;
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

27 К аспектам информационной безопасности относятся:

Выберите несколько вариантов ответа:

1) дискретность;
2) целостность;
3) конфиденциальность;
4) актуальность;
5) доступность.

28 Что такое криптология?

Выберите один вариант ответа:

1) защищенная информация;
2) область доступной информации;
3) тайная область связи.

29 Что такое несанкционированный доступ (НСД)?

Выберите один вариант ответа:

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;
2) Создание резервных копий в организации;
3) Правила и положения, выработанные в организации для обхода парольной защиты;
4) Вход в систему без согласования с руководителем организации;
5) Удаление не нужной информации.

30 Что такое целостность информации?

Выберите один вариант ответа:

1) свойство информации, заключающееся в возможности ее изменения любым субъектом;
2) свойство информации, заключающееся в возможности изменения только единственным пользователем;
3) свойство информации, заключающееся в ее существовании в виде единого набора файлов;
4) свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

31 Кто является знаковой фигурой в сфере информационной безопасности?

Выберите один вариант ответа:

1) Митник;
2) Шеннон;
3) Паскаль;
4) Беббидж.

32 В чем состоит задача криптографа?

Выберите один вариант ответа:

1) взломать систему защиты;
2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений.

33 Под информационной безопасностью понимают:

Выберите один вариант ответа:

1) защиту от несанкционированного доступа;
2) защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера;
3) защиту информации от компьютерных вирусов.

34 Что такое аутентификация?

Выберите один вариант ответа:

1) проверка количества переданной и принятой информации;

2) нахождение файлов, которые изменены в информационной системе несанкционированно;

3) проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа);

4) определение файлов, из которых удалена служебная информация.

35 "Маскарад"- это:

Выберите один вариант ответа:

1) осуществление специально разработанными программами перехвата имени и пароля;

2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

36 Верификация – …

Выберите один вариант ответа:

1) это проверка принадлежности субъекту доступа предъявленного им идентификатора;

2) проверка целостности и подлинности инф, программы, документа;

3) это присвоение имени субъекту или объекту.

37 Кодирование информации – …

Выберите один вариант ответа:

1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.

2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

38 Утечка информации:

Выберите один вариант ответа:

1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;

2) ознакомление постороннего лица с содержанием секретной информации;

3) потеря, хищение, разрушение или неполучение переданных данных.