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
«24» 09 2020 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

технической направленности

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

Возраст обучающихся: 14-18 лет
Срок реализации: 1 год

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 ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ «ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

1.1 Пояснительная записка

Дополнительная общеобразовательная программа технической направленности «Защита персональных данных».

Актуальность данной программы обусловлена современными требованиями к цифровой гигиене, к знаниям в области информационной безопасности, к умениям использовать процессы информационной безопасности в повседневной деятельности человека. Навык использования процессов защиты информации необходим для современного человека, так как угрозы в информационном обществе являются повседневными процессами передачи персональных данных, их обработки и уничтожения. Знания в области защиты персональных данных является неотъемлемой частью современного гражданина РФ.

Предлагаемая программа обучения разработана с учетом требований регуляторов в области информационной безопасности, интересов общества и школы. Школьникам предлагаемая программа будет интересна с точки зрения принципов определения состава персональных данных, знания основных нормативных правовых актов в области информационной безопасности и защиты информации, применения знаний в области защиты персональных данных в открытых компьютерных сетях.

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»;

– Концепцией развития дополнительного образования детей (распоряжение Правительства Российской Федерации от 4 сентября 2014 г. № 1726-р);

– Приказ Министерства Просвещения РФ от 9 ноября 2018 г. №196 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

– Письмо департамента государственной политики в сфере воспитания детей и молодежи от 18 ноября 2015 № 09-3242 «Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»;

– Постановление Главного государственного санитарного врача РФ от 04.07.2014 № 41 "Об утверждении СанПиН 2.4.4.3172-14 "Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей".

1.2 Целевая аудитория

К освоению дополнительных общеобразовательных программ допускаются любые лица без предъявления требований к уровню образования.

1.3 Цель программы и планируемые результаты обучения

Целью реализации программы является формирование и развитие творческих способностей детей, удовлетворение их индивидуальных потребностей в интеллектуальном, нравственном совершенствовании, формирование культуры здорового и безопасного образа жизни, укрепление здоровья, организацию их свободного времени.

Освоение содержания программы обеспечивает достижение слушателями следующих результатов:

личностных:

– осознание своего места в информационном обществе;

– готовность и способность к самостоятельной и ответственной творческой деятельности с использованием информационно-коммуникационных технологий;

– умение использовать достижения современных информационно-коммуникационных технологий для повышения собственного интеллектуального развития в выбранной профессиональной деятельности, самостоятельно формировать новые для себя знания в профессиональной области, используя для этого доступные источники информации;

– умение выстраивать конструктивные взаимоотношения в командной работе по решению общих задач, в том числе с использованием современных средств сетевых коммуникаций;

– умение управлять своей познавательной деятельностью, проводить самооценку уровня собственного интеллектуального развития, в том числе с использованием современных электронных образовательных ресурсов;

– умение выбирать грамотное поведение при использовании разнообразных средств информационно-коммуникационных технологий как в профессиональной деятельности, так и в быту;

– готовность к продолжению образования и повышению квалификации в избранной профессиональной деятельности на основе развития личных информационно-коммуникационных компетенций;

метапредметных:

– умение определять цели, составлять планы деятельности и определять средства, необходимые для их реализации;

– использование различных видов познавательной деятельности для решения информационных задач, применение основных методов

познания (наблюдения, описания, измерения, эксперимента) для организации учебно-исследовательской и проектной деятельности с использованием информационно-коммуникационных технологий;

– использование различных информационных объектов, с которыми возникает необходимость сталкиваться в профессиональной сфере в изучении явлений и процессов;

– использование различных источников информации, в том числе электронных библиотек, умение критически оценивать и интерпретировать информацию, получаемую из различных источников, в том числе из сети Интернет;

– умение использовать средства информационно-коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

– умение публично представлять результаты собственного исследования, вести дискуссии, доступно и гармонично сочетая содержание и формы представляемой информации средствами информационных и коммуникационных технологий;

предметных:

В результате успешного освоения программы слушатель должен

уметь:

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

– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

– классифицировать основные угрозы безопасности 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;

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

1.4 Нормативный срок освоения дополнительной общеобразовательной программы

Нормативный срок освоения программы повышения квалификации составляет 46 часов, в том числе дистанционно – 10 часов.

1.5 Порядок аттестации слушателей

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

Итоговая аттестация

Программа завершается итоговой аттестацией, которая проходит в форме сдачи зачёта.

По завершении обучения слушателям выдаётся сертификат.

2 СТРУКТУРА И СОДЕРЖАНИЕ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1 КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

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

2.2 УЧЕБНЫЙ ПЛАН ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ «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**	2	0	0	0	0	**0**	Тест
2	**Модуль 2 Правовое обеспечение ЗИ**	**9**	**8**	0	0	6	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**	**4**	**4**	0	0	2	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**	Практические работы №№9-12
	Итого:	**46**	**42**	2	0	30	10	0	**4**	**Зачёт**

2.1 УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ «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
	Стартовый уровень								
1	**Модуль 1 Основные понятия защиты информации (ЗИ)**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	
1.1	Тема 1.1 Введение. Основные понятия защиты информации.	2	2	0	0	0	0	0	Тест
2	**Модуль 2 Правовое обеспечение ЗИ**	**9**	**0**	**0**	**6**	**2**	**0**	**1**	
2.1	**Тема 2.1** Правовое обеспечение ЗИ. Основные правовые документы.	7	0	0	4	2	0	1	Практические работы №№1-2
2.2	**Практическая работа №1** Поиск правовых документов в программе Консультант Плюс.								
2.3	**Практическая работа №2** Категорирование персональных данных.								

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.								
2.5	Тема 2.2 Итоговая аттестация	2	0	0	2	0	0	0	Итоговый тест 1
	Базовый уровень								
3	**Модуль 3 Организационное обеспечение ЗИ**	**7**	**0**	**0**	**4**	**2**	**0**	**1**	
3.1	**Тема 3.1** Система обеспечения информационной безопасности Российской Федерации. 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**	**4**	**0**	**0**	**2**	**2**	**0**	**0**	
4.1	Тема 4.1 Основные понятия служебной и конфиденциальной информации. Конфиденциальная информация. Принципы использования информации как конфиденциальная информация третьими лицами.	2	0	0	0	2	0	0	Тест
4.2	Тема 4.2 Итоговая аттестация	2	0	0	2	0	0	0	Итоговый тест 2

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
	Продвинутый уровень								
5	**Модуль 5 Правовые обеспечения защиты персональных данных**	**11**	**0**	**0**	**8**	**2**	**0**	**1**	
5.1	Тема 5.1 Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных.	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** Принципы реализации обработки персональных.								
5.5	**Практическая работа №8** Изучение методов обезличивания персональных данных.								
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	11	0	0	8	2	0	1	Практические работы №№9-12

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
6.2	**Практическая работа №9** Принципы использование информации в общедоступных местах.								
6.3	**Практическая работа №10** Угрозы в открытых компьютерных сетях.								
6.4	**Практическая работа №11** Принципы построения системы безопасности домашних локальных сетей.								
6.5	**Практическая работа №12** Изучение УК РФ в области обработки информации и информационной безопаснсоти.								
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:	**46**	**2**	**0**	**30**	**10**	**0**	**4**	**Зачёт**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1 Для реализации дополнительной общеобразовательной программы 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:

Итоговый Тест 1
6-8 баллов – «зачтено»;
менее 6 баллов – «не зачтено».

Итоговый Тест 2
6-8 баллов – «зачтено»;
менее 6 баллов – «не зачтено».

Итоговый Тест 3
7-9 баллов – «зачтено»;
менее 7 баллов – «не зачтено».

Итоговый Тест 1

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.

Итоговый тест 2

1 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.

2 Основные угрозы конфиденциальности информации:

Выберите несколько вариантов ответа:

1) «маскарад»;

2) «карнавал»;

3) переадресовка;

4) перехват данных;

5) блокирование;

6) злоупотребления полномочиями.

3 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.

4 Защита информации обеспечивается применением антивирусных средств:

Выберите один вариант ответа:

1) да;
2) нет;
3) не всегда.

5 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.

6 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.

7 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.

8 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.

Итоговый тест 3

1 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.

2 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.

3 "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.

4 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.

5 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

6 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.

7 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.

8 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).

9 Кто является знаковой фигурой в сфере информационной безопасности?

Выберите один вариант ответа:

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