МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования "Курский государственный университет"

УТВЕРЖДЕНО
Проректор по учебной работе
_____ Т.Н. Балабина
«___»_____2020 г.

Дополнительная профессиональная программа
повышения квалификации
«**Основы информационной безопасности**»

Документ о квалификации: удостоверение о повышении квалификации

Объем: 72 часа / 2 зачетные единицы

Курск 2020 г.

Дополнительная профессиональная программа повышения квалификации «Основы информационной безопасности» / сост. кандидат технических наук, и.о. заведующий кафедрой информационной безопасности Крыжевич Л.С., кандидат сельскохозяйственных наук, доцент, доцент кафедры информационной безопасности Глаголев Р.В., кандидат технических наук, доцент кафедры информационной безопасности Гордиенко В.В.; Курск. гос. ун-т. – Курск, 2020

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 06.032 «Специалист по безопасности компьютерных систем и сетей» утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года № 598н.

Дополнительная профессиональная программа повышения квалификации «Основы информационной безопасности» предназначена для для формирования первичных знаний, умений и навыков в сфере деятельности – техники по компьютерным сетям и системам. По итогам освоения программы начального уровня (обучения с уровня общих знаний) формируется профессиональная компетенция ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты, которая соответствует профессиональной функции - обслуживание программно-аппаратных средств защиты информации в операционных системах (А/01.5) профессионального стандарта 06.032 "Специалист по безопасности компьютерных систем и сетей" утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года N 598н.

Составители:
кандидат технических наук, и.о. заведующий кафедрой
информационной безопасности Крыжевич Л.С.,
кандидат сельскохозяйственных наук, доцент,
доцент кафедры информационной безопасности Глаголев Р.В.,
кандидат технических наук,доцент кафедры
информационной безопасности Гордиенко В.В.

Оглавление

1. Цель программы

Целью программы дополнительного профессионального образования «Основы информационной безопасности» изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах, обеспечивающие требования к освоению начального уровня деятельности по направлению цифровой экономики «Кибербезопасность и защита данных»

2. Планируемые результаты обучения

2.1.Знание (осведомленность в областях)

2.1.1. – Архитектура и пользовательские интерфейсы операционных систем;

2.1.2 – Порядок обеспечения безопасности информации при эксплуатации операционных систем;

2.1.3 – Источники угроз информационной безопасности и меры по их предотвращению;

2.1.4 – Сущность и содержание понятия информационной безопасности, характеристики ее составляющих;

2.1.5. – Типовые средства защиты информации в операционных системах;

2.1.6 – Программно-аппаратные средства и методы защиты информации;

2.1.7 – Порядок эксплуатации средств антивирусной защиты в операционных системах;

2.1.8 – Формы и методы инструктажа пользователей по порядку работы в операционных системах;

2.1.9 – Общие принципы функционирования программно-аппаратных средств криптографической защиты информации;

2.1.10 – Порядок оформления эксплуатационной документации;

2.1.11 – Нормативные правовые акты в области защиты информации;

2.1.12 – Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

2.1.13 – Организационные меры по защите информации.

2.2. Умение (способность к деятельности)

2.2.1. – Настраивать компоненты подсистем защиты информации операционных систем;

2.2.2 – Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;

2.2.3 – Применять программно-аппаратные средства защиты информации в операционных системах;

2.2.4 – Применять антивирусные средства защиты информации в операционных системах;

2.2.5 – Работать в операционных системах с соблюдением действующих требований по защите информации;

2.2.6 – Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;

2.2.7 – Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;

2.2.8 – Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;

2.2.9 – Контролировать целостность подсистем защиты информации операционных систем;

2.2.10 – Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации;

2.2.11 – Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации.

2.3.Навыки (использование конкретных инструментов)

2.3.1– Защиты текстовых документов;

2.3.2 – Тестирование безопасности операционной системы Windows;

2.3.3 – Подготовки персональных рабочих станций к внешней проверке;

2.3.4 – Подготовка персональных рабочих станций к эксплуатации в условиях потенциальных угроз;

2.3.5 – Передачи защищенной и маскированной информации;

2.3.6 – Преобразования данных посредствам криптосистемы RSA.

3. Категория слушателей

3.1 Среднее профессиональное или высшее образование

3.2 Квалификация – Нет требований

3.3 Наличие опыта профессиональной деятельности – Не требуется

4.4 Не требуется

4. Учебный план программы «Основы информационной безопасности»

№ п/п	Модуль	Всего, час	Виды учебных занятий		
			лекции	практические занятия	самостоятельная работа
1	Модуль 1 - Защита операционных систем, программ и данных	24	**6**	**6**	**12**
3	Модуль 2 – Криптографические и стеганографические методы защиты данных	22	**6**	**4**	**12**
3	Модуль 3 – Защищённый электронный документооборот	24	**6**	**6**	**12**
	Всего	70	**18**	**16**	**36**
Итоговая аттестация		**2**	**Зачет в форме тестирования**		
Итого		**72**			

5. Календарный план-график реализации образовательной программы

«Основы информационной безопасности»
(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

№ п/п	Наименование учебных модулей	Трудоёмкость (час)	Сроки обучения
1	Модуль 1 - Защита операционных систем, программ и данных	**24**	**01 -05**
2	Модуль 2 – Криптографические и стеганографические методы защиты данных	**22**	**06-10**
3	Модуль 3 – Защищённый электронный документооборот	**24**	**11-15**

Всего:	**70**	**01-15 (15 дней фактического взаимодействия)**

6. Учебно-тематический план программы «Основы информационной безопасности»

№ п/п	Модуль / Тема	Всего, час	Виды учебных занятий			Формы контроля
			лекции	практические (лабораторно - практические)занятия	самостоятельная работа	
1	**Модуль 1. Защита операционных систем, программ и данных**	**24**	**6**	**6**	**12**	**тестирование**
1.	Тема 1.1. Понятие информационной безопасности. Основные составляющие.	**8**	**2**	**2**	**4**	**практическое задание**
1.2	Тема 1.2. Защита операционных систем	**8**	**2**	**2**	**4**	**защита отчета по лабораторно-практическому занятию**
1.3	Тема 1.3. Защита программ и данных	**8**	**2**	**2**	**4**	**практическое задание**
2	**Модуль 2. Криптографические и стеганографические методы защиты данных**	**24**	**6**	**6**	**12**	**тест**

2.1	Тема 2.1. Криптографические основы безопасности	**8**	**2**	**2**	**4**	**защита отчета по лабораторно-практическому занятию**
2.2	Тема 2.2. Стеганографические основы безопасности	**6**		**2**	**4**	**защита отчета по лабораторно-практическому занятию**
2.3	Тема 2.3. Электронно-цифровая подпись, как основа безопасности	**8**	**2**	**2**	**4**	**защита отчета по лабораторно-практическому занятию**
3	**Модуль 2. Защищённый электронный документооборот.**	**24**	**6**	**6**	**12**	**тестирование**
3.1	Тема 2.1 Технология защиты документированной информации.	**12**	**2**	**4**	**6**	**защита отчета по лабораторно-практическому занятию**
3.2	Тема 2.2. Создание комплексной системы защиты конфиденциальной информации	**8**	**2**	**2**	**4**	**практическое задание**
3.3	Тема 2.3. Организационное направление работ по созданию КСЗИ	**6**	**2**		**2**	**практическое задание**

7. Учебная (рабочая) программа повышения квалификации «Основы информационной безопасности»

Модуль 1. Защита операционных систем, программ и данных (24 часа)

Тема 1.1. Понятие информационной безопасности. Основные составляющие (8 часов)

Содержание темы:

Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности. Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Вредоносное программное обеспечение. Основные угрозы конфиденциальности.

Тема 1.2. Защита операционных систем (8 часов).

Содержание темы:

Проблемы обеспечения безопасности операционных систем. Угрозы безопасности операционной системы. Подходы к построению защищенных операционных систем. Административные меры защиты**.** Основные функции подсистемы защиты операционной системы. Идентификация, аутентификация и авторизация субъектов доступа. Разграничение доступа к объектам операционной системы. Правила разграничения доступа. Полномочное разграничение доступа с контролем информационных потоков. Сравнительный анализ моделей разграничения доступа**.** Процедура аудита применительно к Операционной системе. Требования к аудиту. Политика аудита.

Тема 1.3. Защита программ и данных (8 часов)

Содержание темы:

Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире. Технологическая и эксплуатационная безопасность программ. Модель угроз и принципы обеспечения безопасности программного обеспечения. Формальные методы доказательства правильности программ и их спецификаций. Методы и средства анализа безопасности программного обеспечения. Методы обеспечения надежности программ для контроля их технологической безопасности. Методы идентификации программ и их характеристик. Методы и средства защиты программ от компьютерных вирусов. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок. Методы и средства обеспечения целостности и достоверности используемого программного кода. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.

Модуль 2. Криптографические и стеганографические методы защиты данных (22часа)

Тема 2.1. «Криптографические основы безопасности» (12 часов).

Содержание темы: Основные понятия и элементы криптографии (алгоритм, ключ, шифр).Симметричные криптосистемы. Криптосистемы с открытым ключом. Системы электронной подписи. Управление ключами. Симметричные и асимметричные криптосистемы-достоинства и недостатки. Перестановки. Гаммирование. Блочные шифры. Применение технологии шифрования с симметричным ключом. Алгоритм Диффи-Хеллмана.Хэш-функция. Алгоритм Message Digest 2 (MD2). Алгоритм Message Digest 4 (MD4). Алгоритм Message Digest 5 (MD5). Алгоритм безопасного хэша (Secure Hash Algorithm – SHA).Требования к криптосистемам.

Тема 2.2. «Стеганографические основы безопасности» (8 часов).

Содержание темы: Стеганографические методы защиты информации Основные понятия. Классификация стеганографических методов, стегосистем и методов сокрытия информации. Классификация стегосистем. Безключевые стегосистемы. Стегосистемы с секретным ключом. Стегосистемы с открытым ключом. Смешанные стегосистемы. Методы сокрытия информации. Текстовые стеганографы. Методы искажения формата текстового документа. Синтаксические методы лингвистической стеганографии. Семантические методы стеганографии. Методы генерации стеганограмм с помощью скрываемого сообщения. Сокрытие данных в изображении и видео. Методы замены во временной (пространственной) области. Методы сокрытия в частотной области изображения. Широкополосные методы. Статистические методы. Методы искажения. Структурные методы. Сокрытие информации в

звуковой среде. Метод наименьших значащих битов. Методы широкополосного кодирования. Метод сокрытия в эхо-сигнале. Фазовые методы сокрытия. Музыкальные стегосистемы.

Тема 2.3. «Электронно-цифровая подпись » (6 часов).

Содержание темы: Понятие электронного документа и электронной подписи. Назначение и применение ЭЦП. История возникновения ЭЦП. Алгоритмы и использование хеш-функций. Симметричная схема. Асимметричная схема. Виды асимметричных алгоритмов ЭЦП. Перечень алгоритмов ЭЦП. Подделка подписей. Модели атак и их возможные результаты. Подделка документа (коллизия первого рода) Получение двух документов с одинаковой подписью (коллизия второго рода).Социальные атаки. Управление ключами. Управление открытыми ключами. Хранение закрытого ключа. Использование ЭЦПВ России. Модели атак и их возможные результаты. Атака с использованием открытого ключа. Атака на основе известных сообщений. Адаптивная атака на основе выбранных сообщений. Полный взлом цифровой подписи. Получение закрытого ключа. Универсальная подделка цифровой подписи. Нахождение алгоритма, аналогичного алгоритму подписи. Выборочная подделка цифровой подписи. Экзистенциальная подделка цифровой подписи.

Модуль 3. Защищённый электронный документооборот (24час.)

Тема 3.1. Технология защиты документированной информации» (8 часов).

Содержание темы: Электронная документация: определение и особенности. Системы управления электронным документооборотом. Функции и задачи систем управления документами. Проблемы организации электронного документооборота. Методы и средства защиты документов в ИС. Кодирование экономической информации. Применение кодов в процессе решения задач. Защита текстовых документов.

Тема 3.2. «Создание комплексной системы защиты конфиденциальной информации» (8 часов).

Содержание темы: Методология построения комплексной системы защиты конфиденциальной информации и описание основных методов и принципов. Основные организационно-методические мероприятия по созданию и поддержанию функционирования комплексной системы защиты. Создание службы обеспечения конфиденциальности (СОК). Перечень основных нормативных и организационно-распорядительных документов, необходимых для организации комплексной системы защиты информации. Рекомендации по методологии построения матрицы конфиденциальности.

Определение объектов и субъектов информационных потоков. Определение характеристик и признаков объектов и субъектов информационных потоков (матрицы конфиденциальности). Построение правил разграничения доступа субъектов к объектам информационных потоков на основании матрицы конфиденциальности.

Тема 3.3. «Организационное направление работ по созданию КСЗИ» (8 часов).

Содержание темы: Анализ объекта и ресурсов, подлежащих защите. Выявление способов несанкционированного доступа и каналов утечки информации. Составление моделей угроз и способов их реализации. Выбор защитных мероприятий. Анализ риска. Формулирование политики безопасности. Составление плана инженерно-технических мероприятий комплексной защиты информации. Оценка эффективности принятых решений. Сущность комплексной системы защиты информации. Принципы построения комплексной системы защиты информации.

Описание практико-ориентированных заданий и кейсов

п/п	Номер темы/модуля	Наименование практического занятия	Описание
	Модуль 1. Защита операционных систем, программ и данных		
	Тема 1.1. Понятие информационной безопасности. Основные составляющие.	Практическая работа: «Моделирование угроз безопасности»	Порядок моделирования угроз безопасности информации и разработки моделей угроз безопасности информации. Определение возможных негативных последствий от реализации угроз безопасности информации. Оценка условий реализации угроз безопасности информации. Источники угроз безопасности информации и оценка возможностей нарушителей. Определение сценариев реализации угроз

			безопасности информации. Оценка уровней опасности угроз безопасности информации.
	Тема 1.2. Защита операционных систем	Лабораторно-практическое занятие №1 «Тестирование безопасности операционной системы Windows»	Исследование надежности пароля администратора. Очистка списков недавних мест и программ. Очистка списка USB-накопителей. Очистка кэша и истории браузеров. Удаление записи DNS. Удаление списка последних документов MS Office.
	Тема 1.3. Защита программ и данных	Практическая работа: «Работа с AVZ»	Работа с программой. Карантин и папка infected. Встроенные средства поиска. Встроенные утилиты. Функции анализа и восстановления. Подсистема AVZ Guard. Подсистема AVZ PM. Подсистема Boot Cleaner. Параметры командной строки.
	Модуль 2. Криптографические и стеганографические методы защиты данных		
	Тема 2.1. Криптографические основы безопасности	Лабораторно-практическое занятие №2 «Организация защищенного обмена данными»	Безключевое кодирование информации. Создание QR-кодов. Симметричное шифрование с помощью ресурса Crypt-online. Ассиметричное шифрование RSA с помощью ресурса Crypt-online. Передача зашифрованных сообщений.
	Тема 2.2. Стеганографические основы безопасности	Лабораторно-практическое занятие №3 «Маскировка передачи закрытых данных методом стеганографии»	Наиболее распространенные стеганографические

			программы. S-Tools. Steganos for Windows. JSTEG Shell. Шифрование и дешифрование с помощью сайта «Стеганография онлайн».
	Тема 2.3. Электронно-цифровая подпись, как основа безопасности	Практическая работа: «Шифрование и электронно-цифровая подпись в системе документооборота»	Программа шифрования информации с открытым исходным кодом PGP. Схемы шифрования электронной цифровой подписи. Цифровая подпись. Генерация ключа шифрования, шифрование и расшифровка сообщений. Экспорт открытого ключа. Шифрование файлов и установка под ними электронно-цифровой подписи. Расшифрование сообщений и идентификация подписи. PGP диск. Создание нового PGP диска. Смена парольной фразы.
	Модуль 3. Защищённый электронный документооборот		
	Тема 3.1 Технология защиты документированной информации.	Лабораторно-практическое занятие №4 «Защищенный документооборот. Защита текстовых документов» Лабораторно-практическое занятие №5 «Защищенный документооборот. Защита табличных документов»	Ограничение редактирования тестового документа в редакторе Microsoft Word. Пометить документ Microsoft Word как окончательный. Шифрование документа редактором Microsoft Word с использованием пароля. Добавление цифровой подписи в Microsoft Word. Защита данных в табличном редакторе MSExcel. Защита

			структуры и окон электронной таблицы. Скрытие и отображение дополнительных листов MSExcel.
	Тема 3.2. Создание комплексной системы защиты конфиденциальной информации	Практическая работа: «Настройка безопасности рабочей станции пользователя»	Отключение учетной записи Гость. Настройка получения автоматических обновлений. Настройка параметров брандмауэра Windows. Просмотр списка разрешенных программ. Настройка параметров брандмауэра для новой сети. Принудительное обновление антивирусной базы. Создаю пользователя без прав. Запуск сетевых приложений от имени учетной записи, настройка автоматического запуска при запуске Windows. Ограничение доступа к папке «Автозагрузка» Использование on-line GUID/UUID генераторы. Использование менеджера паролей в браузере. Создание резервных копий. Установка архиватора, с хорошей поддержкой командной строки. Восстановление текстовых документов.

8. Оценочные материалы по образовательной программе

8.1. Вопросы тестирования по модулям

№ модуля	Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
1		Модуль 1	

	которая хранится отдельной группой и имеет собственное имя? 2. Какие символы разрешается использовать в имени файла или имени директории в Windows? 3. Выберите имя файла anketa с расширением txt. 4. Какое наибольшее количество символов имеет имя файла или каталога в Windows? 5. Какое наибольшее количество символов имеет расширение имени файла? 6. Какое расширение у исполняемых файлов? 7. Какой символ заменяет любое число любых символов? 8. Как записать ? “Все файлы без исключения”? 9. Подкаталог SSS входит в каталог YYY. Как называется каталог YYY относительно каталога SSS? 10. Что выполняет компьютер сразу после включения POWER? 11. Могут ли быть несколько окон активными одновременно? 12. Какое окно считается активным? 13. Может ли каталог и файлы в нем иметь одинаковое имя? 14. Может ли в одном каталоге быть два	1.Учетная запись с ограниченными правами (О) отличается от учетной записи администратора (А) тем, что. 2 Если в окне «Выберите способ входа пользователя в систему» указать адрес собственной электронной почты, то после входа под такой учетной записью пользователь. 3 Зачем желательно указывать учетную запись Microsoft при создании учетной записи с ограниченными правами? 4 Как настроить ОС Windows 10 для автоматического входа по умолчанию в две учетные записи «user» и «user2»? 5 Какие диски можно разбивать на разделы? 6 Зачем нужно сжимать том? 7 Что можно делать с не распределенной областью? 8 Раздел нужно форматировать чтобы. 9 Ярлыки создают для. 10 Что позволяют делать антивирусные системы? 11 Программа дефрагментации Disk Defrag применяется в случае. 12 Установку программы Disk Defrag необходимо производить. 13 Фрагментированные участки диска это.	1. Основными рисками информационной безопасности являются? 2. Когда получен спам по e-mail с приложенным файлом, следует? 3. Наиболее распространены угрозы информационной безопасности корпоративной системы? 4. Наиболее распространены угрозы информационной безопасности сети? 5. Утечкой информации в системе называется ситуация, характеризуемая? 6. Под информационной безопасностью понимается… 7. Основные составляющие информационной безопасности? 8. Конфиденциальность – это.. 9. Угроза – это… 10. Основная масса угроз информационной безопасности приходится на? 11. Под какие системы распространение вирусов происходит наиболее динамично? 12. Какой подход к обеспечению безопасности имеет место? 13. Для чего создаются информационные системы? 14. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? 15. Когда целесообразно не предпринимать никаких

	файла с одинаковыми именами? 15. Может ли в разных каталогах быть два файла с одинаковыми именами. 16. Возможно ли восстановить стертую информацию на жестком диске? 17. Запись файлов на диске в виде разбросанных участков по всей поверхности диска называется… 18. Какое высказывание неверно? Дефрагментация проводят с целью … 19. Какая из программ предназначена для дефрагментации диска? 20. Что выполняет операционная система при удалении файла с диска? 21. Как можно удалить компьютерный вирус с диска? 22. Архивация файлов – это… 23. Какая из программ является архиватором? 24. Какая из программ является антивирусной программой? 25. Что собой представляет компьютерный вирус?	14 Программа Recuva Free применяется для. 15 Программу Recuva Free необходимо запускать. 16 После форматирования диска можно. 17 Программа Disk Wipe предназначена для….. 18 Если Вы забыли установленный пароль на открытие документа в формате .doc, то какой из вариантов даст действенный результат. 19 Если Вы пометили документ Word, как окончательный, то ... 20 Вы защитили документ Word паролем без шифрования, ограничив редактирование документа, и выложили в интернет. 21 Чтобы защитить документ Word от копирования данных необходимо воспользоваться инструментом. 22 Какие инструменты приводят к изменению архитектуры документа? 23 При создании цифровых подписей используются три компонента, какие из этих компонентов содержатся в самом документе. 24 Какие инструменты защиты в табличный редактор Excel перешли из текстового редактора Word?	действий в отношении выявленных рисков? 16. К конфиденциальной информации относятся документы, содержащие 17. Какая информация подлежит защите? 18. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? 19. Какими путями может быть получена информация? 20. Под непреднамеренным воздействием на защищаемую информацию понимают? 21. Шифрование информации это…….. 22. Можно выделить следующие направления мер информационной безопасности 23. Что можно отнести к организационным мерам ИБ? 24. Что можно отнести к техническим мерам ИБ? 25. Какие сбои оборудования бывают? 26. Какие потери информации бывают из-за некорректной работы программ? 27. Средства защиты данных, функционирующие в составе программного обеспечения. 28. Программное средство защиты информации? 29. В классификацию вирусов по способу заражения входят? 30. Вирусы, не связывающие свои

	26. Что не поможет удалить с диска компьютерный вирус? 27. Какое утверждение верно? 28. Архиваторы характеризуются… 29. Что не является каналом распространения вирусов? 30. Подсистема это? 31. Расширение файла, как правило, характеризует? 32. Производительность работы компьютера зависит от? 33. Озу это память в которой хранится? 34. Для выхода на поисковый сервер необходимо? 35. Процессор обрабатывает информацию? 36. При отключении компьютера информация? 37. Протокол маршрутизации ip обеспечивает? 38. Во время исполнения прикладная программа хранится 39. За минимальную единицу измерения количества информации принято считать? 40. Компьютер, подключенный к интернету, обязательно имеет?	25 Одним способом снятия защиты с листа Excel является копирование содержимого защищенного листа на новый лист Excel, при этом необходимое условие реализации процедуры. 26 Выделите ячейки, которые не надо защищать (если таковые есть), щелкните по ним правой кнопкой мыши и выберите в контекстном меню команду Формат ячеек (Format Cells). Будут защищены при включении защиты листа. 27 Как можно узнать количество скрытых листов в MS Excel? 28 Чтобы открыть Ваш зашифрованный PDF-файл, злоумышленнику потребуется. 29 Снять защиту на открытия pdf-файла в рамках правового поля можно, используя…… 30 С какой целью документ в формате Word сохраняют в файл формате PDF? 31 Как можно защитить pdf-файл от изменения авторский прав на документ 32 Вы зашифровали информацию и отправили ее контрагенту по защищенному каналу. 33 Существует объективная необходимость передачи большого	копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются? 31. Основными компонентами парольной системы являются…….. 32. К категории компьютерных вирусов НЕ относятся…….. 33. Как происходит заражение «почтовым» вирусом? 34. Как вирус может появиться в компьютере? 35. Руткит - это... 36. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется... 37. Компьютерные вирусы - это... 38. Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

		объема закрытой информации. 34 Вы работает с несколькими агентами, необходимо использовать ключи шифрования. 35 Наложение криптографических преобразований, подразумевает использование. 36 Выберите какой из пунктов не связан понятием электронная подпись.	
2		Модуль 2 1 Вы зашифровали информацию и отправили по защищенному каналу контрагенту. 2 Существует объективная необходимость передачи большого объема закрытой информации. Необходимые действия. 3 Вы работаете одновременно с несколькими агентами. Какую политику необходимо выбрать при использовании ключей шифрования. 4 Наложение криптографических преобразований, подразумевает использование. 5 Выберите какой из пунктов не связан понятием электронная подпись. 6. Какого этапа не было в истории криптографии?	

		7. Какой раздел не входит в современную криптографию? 8. Что такое ключ? 9. От какого слова пошло понятие «шифр»? 10. Сколько раз используется ключ при многоалфавитной замене. 11. Кратко опишите схему передачи сообщения. 12. Какие допущения не принимаются по отношении к нарушителю? 13. Что называют «криптоатакой». 14. Что понимают под симметричными криптографическими системами: 15. Какие методы могут называться стеганографическими? 16. Как расшифровывается метод LSB? 17. Какие типы данных можно использовать в качестве контейнеров для встраивания информации? 18. Выберете примеры использования методов стеганографии из истории 19. Сколько бит можно спрятать в изображение незаметно для человеческого взгляда?	
3		Модуль 3 1. Если Вы забыли установленный пароль на открытие документа в формате .doc, то	

		какой из вариантов даст действенный результат. 2. Если Вы пометили документ Word, как окончательный, то ... 3. Вы защитили документ Word паролем без шифрования, ограничив редактирование документа, и выложили в интернет. 4. Чтобы защитить документ Word от копирования данных необходимо воспользоваться инструментом. 5. Какие инструменты приводят к изменению архитектуры документа. 6. При создании цифровых подписей используются три компонента, какие из этих компонентов содержатся в самом документе. 7. Какие инструменты защиты в табличный редактор Excel перешли из текстового редактора Word? 8. Одним способом снятия защиты с листа Excel является копирование содержимого защищенного листа на новый лист Excel, при этом необходимое условие реализации процедуры. 9. Выделите ячейки, которые не надо защищать (если таковые есть), щелкните по ним правой кнопкой мыши	

		и выберите в контекстном меню команду Формат ячеек (Format Cells). Будут защищены при включении защиты листа. 10. Как можно узнать количество скрытых листов в MS Excel? 11. Чтобы открыть Ваш зашифрованный PDF-файл, злоумышленнику потребуется. 12. Используя какое программное обеспечение можно защитить PDF-документ от копирования? 13 Снять защиту на открытия pdf-файла в рамках правового поля можно, используя. 14 С какой целью документ в формате Word сохраняют в файл формате PDF? 15. Как можно защитить pdf-файл от изменения авторский прав на документ.	

8.2. Описание показателей и критериев оценивания, шкалы оценивания.

Показатели оценки результатов обучения

Результаты обучения(освоенные умения, усвоенные знания)	**Основные показатели оценки результата**
ПК-4 – способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Знает: – основные угрозы информационной безопасности и программное обеспечение для решения прикладных задач;	Эффективно применяет методы и средства защиты документов и программ для решения задач типовых мероприятий по обеспечению информационной

– классификацию информационных систем, структуру, конфигурацию информационных систем, общую характеристику процесса организации защиты информационных систем; – структуру состав и свойства информационных процессов, систем и технологий, методы анализа устойчивости информационных систем, модели представления угроз информационной безопасности; – структуру, принципы реализации и функционирования технологий, используемых при создании комплексной системы информационной безопасности, инструментальные средства информационной безопасности. Умеет: – использовать методы защиты информации в своей профессиональной деятельности; – использовать детализированные решения при разработке мероприятий по обеспечению информационной безопасности; – применять технологии информационной безопасности при обслуживании информационных систем.	безопасности структурного подразделения / организации.

Критерии оценивания

Дескриптор	**Начальный уровень** (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.)	**Базовый уровень** (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.)	**Продвинутый** (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)

Знать	Сущность и содержание понятия информационной безопасности, характеристики ее составляющих; Нормативные правовые акты в области защиты информации; Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;	Архитектура и пользовательские интерфейсы операционных систем; Порядок обеспечения безопасности информации при эксплуатации операционных систем; Источники угроз информационной безопасности и меры по их предотвращению; Типовые средства защиты информации в операционных системах; Порядок эксплуатации средств антивирусной защиты в операционных системах;	Программно-аппаратные средства и методы защиты информации; Формы и методы инструктажа пользователей по порядку работы в операционных системах; Общие принципы функционирования программно-аппаратных средств криптографической защиты информации; Порядок оформления эксплуатационной документации; Организационные меры по защите информации.
Уметь	Настраивать компоненты подсистем защиты информации операционных систем; Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей; Применять антивирусные средства защиты информации в операционных системах;	Применять программно-аппаратные средства защиты информации в операционных системах; Работать в операционных системах с соблюдением действующих требований по защите информации; Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;	Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; Контролировать целостность подсистем защиты информации операционных систем; Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации;

		Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;	Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации.
Владеть	Защитой текстовых документов; Подготовкой персональных рабочих станций к внешней проверке;	Тестированием безопасности операционной системы Windows; Методами подготовки персональных рабочих станций к эксплуатации в условиях потенциальных угроз;	Методами передачизащищенной и маскированной информации;

Шкала оценивания

Отметка	Уровень освоения компетенции
«зачтено»	Отметка «зачтено» выставляется в случае, если обучающийся продемонстрировал уровень освоения компетенции не ниже базового.
«не зачтено»	Отметка «не зачтено» выставляется в случае, если обучающийся продемонстрировал начальный уровень освоения компетенции.

.

Необходимым условием успешного освоения программы является прохождение текущего тестирования, которое позволяет оценить уровень подготовки слушателя.

В процентном соотношении оценки выставляются в следующих диапазонах:

«не зачтено» - менее 50%

«не зачтено» - 51% и выше

Вместе с вышеуказанным необходимым условием допуска к итоговому тестированию является предоставление отчетности по четырем лабораторно-практическим занятиям.

8.3. Примеры контрольных заданий по модулям или всей образовательной программе

Пример заданий итогового тестирования по курсу

Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его

Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

Утечкой информации в системе называется ситуация, характеризуемая:

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

Под информационной безопасностью понимается…

- защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
- программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
- нет правильного ответа

Основные составляющие информационной безопасности:

- целостность
- достоверность
- конфиденциальность

Конфиденциальность – это..

- защита от несанкционированного доступа к информации
- программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
- описание процедур

Угроза – это…

- потенциальная возможность определенным образом нарушить информационную безопасность

- система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
- процесс определения отвечает на текущее состояние разработки требованиям данного этапа

Основная масса угроз информационной безопасности приходится на:

- Троянские программы
- Шпионские программы
- Черви

Под какие системы распространение вирусов происходит наиболее динамично:

- Windows
- Mac OS
- Android

Какой подход к обеспечению безопасности имеет место:

- теоретический
- комплексный
- логический

Для чего создаются информационные системы:

- получения определенных информационных услуг
- обработки информации
- оба варианта верны

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:

- проведение тренингов по безопасности для всех сотрудников
- поддержка высшего руководства
- эффективные защитные меры и методы их внедрения

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:

- когда риски не могут быть приняты во внимание по политическим соображениям
- для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- когда стоимость контрмер превышает ценность актива и потенциальные потери

Информация

- не исчезает при потреблении
- становится доступной, если она содержится на материальном носителе
- подвергается только "моральному износу"
- характеризуется всеми перечисленными свойствами

К конфиденциальной информации относятся документы, содержащие

- государственную тайну
- законодательные акты
- "ноу-хау"
- сведения о золотом запасе страны

Какая информация подлежит защите?

- информация, циркулирующая в системах и сетях связи
- зафиксированная на материальном носителе информация с реквизитами,
- позволяющими ее идентифицировать
- только информация, составляющая государственные информационные ресурсы
- любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- Сотрудники

- Хакеры
- Атакующие
- Контрагенты (лица, работающие по договору)

Какими путями может быть получена информация?

- проведением научных исследований, покупкой и противоправным добыванием информации
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

Под непреднамеренным воздействием на защищаемую информацию понимают?

- Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Шифрование информации это

- Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
- Все ответы верны
- Технические

Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных

сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Какие сбои оборудования бывают?

- сбои работы серверов, рабочих станций, сетевых карт и тд
- потери при заражении системы компьютерными вирусами
- несанкционированное копирование, уничтожение или подделка информации
- ознакомление с конфиденциальной информацией

Какие потери информации бывают из-за некорректной работы программ?

- сбои работы серверов, рабочих станций, сетевых карт и тд
- перебои электропитания
- потеря или изменение данных при ошибках ПО
- ознакомление с конфиденциальной информацией

Средства защиты данных, функционирующие в составе программного обеспечения.

- Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

Программное средство защиты информации

- криптография
- источник бесперебойного питания
- резервное копирование
- дублирование данных

В классификацию вирусов по способу заражения входят

- опасные
- файловые
- резидентные
- загрузочные
- файлово -загрузочные
- нерезидентные

Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:

- компаньон - вирусами
- черви
- паразитические
- студенческие
- призраки
- стелс - вирусы
- макровирусы

Основными компонентами парольной системы являются

- интерфейс администратора
- хранимая копия пароля
- база данных учетных записей
- все варианты верны

К категории компьютерных вирусов НЕ относятся

- загрузочные вирусы
- type-вирусы
- сетевые вирусы
- файловые вирусы

Как происходит заражение «почтовым» вирусом?

- при получении с письмом, присланном по e-mail, зараженного файла
- при открытии зараженного файла, присланного с письмом по e-mail
- при подключении к почтовому серверу

– при подключении к web-серверу, зараженному «почтовым» вирусом

Как вирус может появиться в компьютере?

– при работе с макросами
– самопроизвольно
– при работе компьютера в сети
– при решении математической задачи

Руткит - это...

– вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю
– разновидность межсетевого экрана
– программа использующая для распространения Рунет (Российскую часть Интернета)
– программа для скрытого взятия под контроль взломанной системы
– вредоносная программа, маскирующаяся под макрокоманду

Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

– Макровирус
– Загрузочный вирус
– Сетевой червь
– Троян
– Файловый вирус

Компьютерные вирусы - это...

– Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы
– Вредоносные программы, наносящие вред данным.
– Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера
– Это скрипты, помещенные на зараженных интернет-страничках
– Программы, уничтожающие данные на жестком диске

Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

- Сетевой червь
- Файловый вирус
- Загрузочный вирус
- Макровирус
- Троян

8.4. Тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий

Вопросы входного тестирования

Как называется группа файлов, которая хранится отдельной группой и имеет собственное имя?

- Байт
- Каталог
- Дискета

Какие символы разрешается использовать в имени файла или имени директории в Windows?

- Цифры и только латинские буквы
- Латинские, русские букву и цифры
- Русские и латинские буквы

Выберите имя файла anketa с расширением txt.

- Anketa. txt.
- Anketa. txt
- Anketa/txt.

Какое наибольшее количество символов имеет имя файла или каталога в Windows?

- 255
- 10
- 8

Какое наибольшее количество символов имеет расширение имени файла?

- 3
- 8
- 2

Какое расширение у исполняемых файлов?

- exe, doc
- bak, bat

– exe, com, bat

Какой символ заменяет любое число любых символов?

– ?
– \
–

Как записать : “Все файлы без исключения”?

– ?.?
– .
– .?

Подкаталог SSS входит в каталог YYY. Как называется каталог YYY относительно каталога SSS?

– корневой
– дочерний
– родительский

Что выполняет компьютер сразу после включения POWER?

– перезагрузка системы
– проверку устройств и тестирование памяти
– загрузку программы

Могут ли быть несколько окон активными одновременно?

– да
– нет

Какое окно считается активным?

– первое из открытых
– любое
– то, в котором работаем.

Может ли каталог и файлы в нем иметь одинаковое имя?

– да
– нет

Может ли в одном каталоге быть два файла с одинаковыми именами?

– да
– нет

Может ли в разных каталогах быть два файла с одинаковыми именами.

– да
– нет

Возможно ли восстановить стертую информацию на жестком диске?

– возможно всегда
– возможно, но не всегда

Запись файлов на диске в виде разбросанных участков по всей поверхности диска называется…

– оптимизация диска
– фрагментация диска
– форматирование диска

Какое высказывание неверно? Дефрагментация проводят с целью …

- оптимизации дискового пространства
- ускорения процесса чтения и записи файлов
- сжатия информации

Какая из программ предназначена для дефрагментации диска?

- Smart Defrag
- NDD
- Unerase

Что выполняет операционная система при удалении файла с диска?

- Перемешивает в FAT его кластеры
- Уничтожает первый символ имени файла в каталоге
- Размагничивает участки диска, где располагался файл

Как можно удалить компьютерный вирус с диска?

- Перезагрузить систему
- Специальной программой
- Удалить вирус невозможно

Архивация файлов – это…

- Объединение нескольких файлов
- Разметка дисков на сектора и дорожки
- Сжатие файлов

Какая из программ является архиватором?

- NDD
- DRWEB
- RAR

Какая из программ является антивирусной программой?

- NDD
- DRWEB
- RAR

Что собой представляет компьютерный вирус?

- Небольшая по размерам программа
- Миф, которого не существует
- Название популярной компьютерной игры

Что не поможет удалить с диска компьютерный вирус?

- Дефрагментация диска
- Проверка антивирусной программой
- Форматирование диска

Какое утверждение верно?

- Все файлы сжимаются при архивации одинаково
- Файлы растровой графики сжимаются лучше всего
- Различные типы файлов сжимаются при архивации по - разному

Архиваторы характеризуются…

- Степенью и скоростью архивации
- Способом распространения

- Методом и скорость сжатия

Что не является каналом распространения вирусов?

- Устройства визуального отображения информации
- Компьютерные сети
- Внешние носители информации.

Подсистема это:

- Предопределенная рабочая среда, посредством которой система координирует выделение ресурсов и распределяет задачи
- Множество элементов, находящихся в отношениях и связях друг с другом, которые образуют определённую целостность
- Часть информационной системы, выделяемой при проектировании системной архитектуры.

Расширение файла, как правило, характеризует:

- Объем памяти
- Путь к папке, где хранятся данные
- Тип данных, хранящихся в файле

Производительность работы компьютера зависит от:

- От комплектующих системного блока
- От установленного ПО
- От скорости Интернет-соединения

Озу это память в которой хранится:

- Информация о файловой системе
- Выполняемый машинный код
- Кэшированные данные процессора

Для выхода на поисковый сервер необходимо:

- Зайти в браузер
- Ввести запрос в поисковом меню
- Вписать в адресную строку браузера адрес поискового сервиса

Процессор обрабатывает информацию:

- В текстовом формате
- В двоичном коде
- На языке Pascal

При отключении компьютера информация:

- Удаляется с HDD
- Сохраняется в кэше графического процессора
- Удаляется с памяти ОЗУ

Протокол маршрутизации ip обеспечивает:

- Пересылку информации в компьютерных сетях
- Возможность связи нескольких компьютеров и их данных в одну общую сеть
- Кодировку и дешифровку данных

Во время исполнения прикладная программа хранится

- в кэш-памяти ядра

- в памяти ОЗУ
- в памяти винчестера (жесткого диска)

За минимальную единицу измерения количества информации принято считать:

- Байт
- Килобит
- Бит

Компьютер, подключенный к интернету, обязательно имеет:

- Связь с удаленным сервером
- IP-адрес
- Доменное имя

Вопросы промежуточного тестирования

Модуль 1

Учетная запись с ограниченными правами (О) отличается от учетной записи администратора (А) тем, что:

- операционная система ограничивает доступ к некоторым важным файлам пользователю с учетной записью (О), а пользователю с учетной записью (А) разрешает;
- в учетной записи (О) указаны фамилия и инициалы, а в учетной записи (А) указаны полностью фамилия, имя, отчество пользователя;
- пользователь с учетной записью (А) может читать все файлы, созданные пользователем с учетной записью (О);
- пользователь с учетной записью (О) может читать все файлы, созданные пользователем с учетной записью (А);

Если в окне «Выберите способ входа пользователя в систему» указать адрес собственной электронной почты, то после входа под такой учетной записью пользователь:

- всем адресатам будет передаваться адрес своей электронной почты автоматически.
- увидит всю пришедшую по электронной почте корреспонденцию на рабочем столе;
- сможет пользоваться только указанным почтовым ящиком;

- сразу будет иметь возможность просматривать свою почту при входе в браузер;

Зачем желательно указывать учетную запись Microsoft при создании учетной записи с ограниченными правами?

- она защищает учетную запись с ограниченными правами от взлома;
- она используется для доступа к многочисленным устройствам и службам Майкрософт;
- она позволяет синхронизировать данные компьютера с другими устройствами;
- она следит за действиями пользователя.

Как настроить ОС Windows 10 для автоматического входа по умолчанию в две учетные записи «user» и «user2»?

- сразу две учетные записи настроит для автоматического входа невозможно.
- при настройке указать сразу два имени «user» и «user2»;
- сначала настроить вход от имени «user», а затем от имени «user2»;

Какие диски можно разбивать на разделы?

- удаленные диски через интернет.
- жесткие диски компьютера;
- любые диски компьютера;
- USB диски компьютера;

Зачем нужно сжимать том?

- чтобы сам том занимал как можно меньше места.
- чтобы освободить место для создания нового тома;
- чтобы туда можно было добавить новую информацию;
- чтобы предотвратить сбои на томе;

Что можно делать с не распределенной областью?

- добавить к другому тому.

- создать в ней новый том;
- оставить в резерве на всякий случай;
- использовать как системную область;

Раздел нужно форматировать чтобы:

- восстановить работоспособность раздела;
- создать один или несколько других разделов;
- удалить ненужную информацию с него;
- операционная система могла писать или считывать информацию.

Ярлыки создают для:

- утаивания настоящих файлов от посторонних глаз;
- надежного хранения файлов;
- удобства доступа к файлам или папкам;

Что позволяют делать антивирусные системы?

- защищают облачные хранилища
- проверку носителей на наличие вирусов;
- очищают реест от ненужных файлов
- создают резервные копии;

Программа дефрагментации Disk Defrag применяется в случае:

- наличия вирусов;
- получения угроз по электронной почте.
- замедления работы компьютера;
- получения синего экрана смерти;

Установку программы Disk Defrag необходимо производить:

- удаленно из интернета;
- из учетной записи администратора;
- предварительно выключив все антивирусные средства.
- из учетной записи с ограниченными правами;

Фрагментированные участки диска это:

- цветные метки на диске;
- части одного файла перепутанные с частями других файлов;
- участки диска не пригодные для хранения информации.
- сильно намагниченные части диска;

Программа Recuva Free применяется для:

- создания резервных копий;
- восстановления удаленных данных.
- создания красочных графических файлов;
- контроля целостности файловой системы;

Программу Recuva Free необходимо запускать:

- предварительно выключив все
- из учетной записи с ограниченными правами;
- удаленно из интернета;
- из учетной записи администратора;

После форматирования диска можно:

- проверять наличие удаленных файлов;
- разбивать диск на разделы.
- восстанавливать ранее записанные на него файлы;
- писать на него новые файлы;

Программа Disk Wipe предназначена для:

- надежного уничтожения данных;
- повышения отказоустойчивости компьютера.
- борьбы с вирусами;
- пересылки почтовых отправлений;

Если Вы забыли установленный пароль на открытие документа в формате .doc, то какой из вариантов даст действенный результат:

- Вы попробуете его открыть с использование OpenOffice, игнорируя настройки Word
- Вы прибегнете, к возможностям браузера просматривать документы он-лайн
- Вы откроете файл с использование Блокнот, пытаясь обойти настройки Word
- Вы постараетесь вспомнить пароль так, как знаете принцип создания своих паролей

Если Вы пометили документ Word, как окончательный, то ...

- Вы уверены, что данная информация уже никем не может быть изменена?
- Вы уверены в том, что данные не смог быть скопированы?
- Вы уверены в том, что Вы его не измените случайно при попытке редактирования или печати?

Вы защитили документ Word паролем без шифрования, ограничив редактирование документа, и выложили в интернет:

- Вы отдаете себе отчет, что эта информация доступна всем, установка пароля в данном случае лишь мера предосторожности, от случайных корректировок, которые Вы хотите предотвратить
- Вы полагаете, что специалистов, способных извлечь информацию крайне мало
- Вы больше не беспокоитесь о сохранности его содержимого документа

Чтобы защитить документ Word от копирования данных необходимо воспользоваться инструментом:

- Примечания
- Ввод данных в поля форм
- Только чтение
- Запись исправлений

Какие инструменты приводят к изменению архитектуры документа?

- Ограничения на редактирование и форматирование
- Шифрование документа
- Пометка "Окончательный"
- Установка электронной цифровой подписи

При создании цифровых подписей используются три компонента, какие из этих компонентов содержатся в самом документе:

- Шифрование с помощью ключа
- Сертификаты
- Хеширование

Какие инструменты защиты в табличный редактор Excel перешли из текстового редактора Word?

- Ограничить редактирование и форматирование
- Электронная цифровая подпись
- Пометка "Окончательный"
- Зашифровать документ

Одним способом снятия защиты с листа Excel является копирование содержимого защищенного листа на новый лист Excel, при этом необходимое условие реализации процедуры:

- Выделение заблокированных и не заблокированных ячеек будет разрешено автором файла
- Наличие версии Microsoft Excel не ниже 2016 года
- Возможность загрузки документа на он-лайн сервисы
- Использование многопользовательского режима в Office 365

Выделите ячейки, которые не надо защищать (если таковые есть), щелкните по ним правой кнопкой мыши и выберите в контекстном меню команду Формат ячеек (Format Cells). Будут защищены при включении защиты листа:

- Все ячейки, для которых этот флажок останется установленным
- Все подсвеченные цветом ячейки на текущем листе, при условии использовании соответствующего макроса
- Все ячейки которые будут помечены в ручном режиме

Как можно узнать количество скрытых листов в MS Excel?

- В контекстном меню включить режим "Отобразить листы"
- Открыть документ через архиватор
- В опции "Защитить лист"

Чтобы открыть Ваш зашифрованный PDF-файл, злоумышленнику потребуется:

- Наличие современного оборудование, как минимум современные видеокарты NVIDIA/AMD для GPU ускорения, и временной ресурс
- Использование общих возможностей распределенной ЭВМ, с внедренным алгоритмом, для получения доступа к ресурсу пользовательского персонального компьютера
- Наличие специально программного обеспечения типа Accent OFFICE Password Recovery, Passcovery Suite

Используя какое программное обеспечение можно защитить PDF-документ от копирования?

- Защифровать в Word или Excel и пересохранить в формате PDF
- Виртуальные принтеры (например, PDF Creator, Adobe PDF)
- Собрать постранично в программах для сканирования и распечатать в PDF.
- Он-лайн сервисы, аналоигчные pdf.io, pdf2go.com, ilovepdf.com, smallpdf.com

Снять защиту на открытия pdf-файла в рамках правового поля можно, используя

- специальное программное обеспечение, использующее методологию brute force
- в ручную, подбирая пароль
- онлайн сервисы, если знаешь пароль

С какой целью документ в формате Word сохраняют в файл формате PDF?

- Чтобы его можно было открыть на компьютерах, где установлены MacOs или Linux
- Чтобы исключить изменения текста и других данных документа
- Чтобы исключить, что "поедут" некоторые строчки или картинки

Как можно защитить pdf-файл от изменения авторский прав на документ

- Добавить рукописную подпись
- Установить электронную цифровую подпись
- Наложить поверх документа водяной знак

Вы зашифровали информацию и отправили ее контрагенту по защищенному каналу:

- Вы полагаетесь на техническое совершенство средств передачи данных
- Вы полностью уверены в недоступности и безопасности передаваемых данных
- Вы обеспечиваете сохранность данных, используя критерий времени
- Вы по каналам связи передаете только оперативные данные, ограничиваясь критерием актуальности информации

Существует объективная необходимость передачи большого объема закрытой информации:

- Вы организуете передачу ключа по каналам, использующим ассиметричный алгоритм, а остальныеданные передаете посредствам симметричных алгоритмов шифрования
- Вы прибегаете к использованию открытого канала ограничивая время передачи информации
- Вы маскируете передачу информации посредствам использования методов стеганографии
- Вы организуете передачу по каналу использующему исключительно RSA алгоритм

Вы работает с несколькими агентами, необходимо использовать ключи шифрования:

- Вы максимально сократите объем информации и перешлете ее с использованием ассиметричного алгоритма
- Вы используете общий открытый ключ шифрования
- Вы постоянно будете менять открытый ключ после работы с каждым агентом
- Вы создадите уникальные открытые ключи по количеству агентов

Наложение криптографических преобразований, подразумевает использование:

- Алгоритмов шифрования
- Методов внедрения и скрытия информации
- Кодирование азбукой Морзе
- Средств хэширования

Выберите какой из пунктов не связан понятием электронная подпись

- Сертификат
- Ассиметричное шифрование
- QR-код
- Хэширование

Модуль 2

Вы зашифровали информацию и отправили по защищенному каналу контрагенту:

- Вы по каналам связи передаете только оперативные данные, ограничиваясь критерием актуальности информации
- Вы уверены, что любой алгоритм шифрования обеспечивает недоступность и безопасность передаваемых данных
- Вы полагаетесь на техническое совершенство современных средств передачи данных
- Вы обеспечиваете сохранность данных, используя критерий времени

Существует объективная необходимость передачи большого объема закрытой информации. Необходимые действия:

- Вы организуете передачу данных, используя ассиметричный алгоритма RSA
- Вы организуете передачу ключа по каналам, использующим ассиметричный алгоритм, а остальныеданные передаете посредствам симметричных алгоритмов шифрования
- Вы прибегаете к использованию открытого канала связи, ограничивая время передачи информации
- Вы маскируете передачу информации посредствам использования методов стеганографии

Вы работаете одновременно с несколькими агентами. Какую политику необходимо выбрать при использовании ключей шифрования:

- Вы используете общий открытый ключ шифрования
- Вы постоянно будете менять открытый ключ после работы с каждым агентом
- Вы создадите уникальные ключи для каждого агента
- Вы максимально сократите объем информации и перешлете ее с использованием ассиметричного алгоритма

Наложение криптографических преобразований, подразумевает использование:

- Алгоритмов шифрования
- Методов внедрения и скрытия информации
- Кодирование азбукой Морзе
- Средств хэширования

Выберите какой из пунктов не связан понятием электронная подпись

- Сертификат
- QR-код
- Хэширование
- Ассиметричное шифрование

Какого этапа не было в истории криптографии?

- Философская криптография.
- Научная криптография.
- Компьютерная криптография
- Наивная криптография.

Какой раздел не входит в современную криптографию?

- Системы электронной подписи.
- Управление ключами.
- Криптосистемы с закрытым ключом.
- Симметричные криптосистемы.

Что такое ключ?

- секретная последовательность букв
- пароль
- сочетание цифр
- аутентификация субъектов

От какого слова пошло понятие «шифр»?

- Цифра
- Знак
- Звук
- Символ

Сколько раз используется ключ при многоалфавитной замене:

- 1
- 2
- много
- ни разу

Кратко опишите схему передачи сообщения:

- источник->шифрование->дешифрование-> приёмник;
- источник->шифрование->расшифровывание-> взлом
- источник->шифрование->расшифровывание->приёмник;
- источник->шифрование->дешифрование->взлом

Какие допущения не принимаются по отношении к нарушителю?

- нарушитель знает секретный ключ
- нарушителю доступны все зашифрованные тексты
- нарушитель знает алгоритм шифрования
- нарушитель имеет в своем распоряжении вычислитель¬ные, людские, временные и иные ресурсы

Что называют «взломом»:

- дешифрование
- ввод пароля
- удачная криптоатака
- знание ключа

Что называют «криптоатакой»:

- подделки зашифрованного сообщения
- перехват зашифрованного сообщения
- прочтения зашифрованного сообщения
- вычисления ключа

Что понимают под симметричными криптографическими системами:

- в которых для шифрования и расшифровывания ключи не используется.
- в которых для шифрования и расшифровывания используется один и тот же ключ
- в которых для шифрования и расшифровывания используется два разных ключа
- в которых для шифрования и расшифровывания используется множество ключей

Какие методы могут называться стеганографическими?

- встраивание бита информации в младший бит данных
- прикрепление к файлу дополнительной информации
- установка прозрачных водяных знаков
- кодировка текста в QR-код

Как расшифровывается метод LSB?

- Lenovo Service Bridge
- Linux Standard Base
- Least Significant Bit

Какие типы данных можно использовать в качестве контейнеров для встраивания информации?

- Музыка
- Документы
- Изображения
- Таблицы

Выберете примеры использования методов стеганографии из истории

- портрет Моны Лизы
- квадрат Малевича
- письмо молоком
- татуировка на голове раба

Сколько бит можно спрятать в изображение незаметно для человеческого взгляда?

- 16
- 2
- 8
- 4

Модуль 3

Если Вы забыли установленный пароль на открытие документа в формате .doc, то какой из вариантов даст действенный результат:

- Вы откроете файл с использование Блокнот, пытаясь обойти настройки Word
- Вы прибегнете, к возможностям браузера просматривать документы он-лайн
- Вы постараетесь вспомнить пароль так, как знаете принцип создания своих паролей
- Вы попробуете его открыть с использование OpenOffice, игнорируя настройки Word

Если Вы пометили документ Word, как окончательный, то ...

- Вы уверены в том, что данные не смог быть скопированы?
- Вы уверены, что данная информация уже никем не может быть изменена?
- Вы уверены в том, что Вы его не измените случайно при попытке редактирования или печати?

Вы защитили документ Word паролем без шифрования, ограничив редактирование документа, и выложили в интернет:

- Вы больше не беспокоитесь о сохранности его содержимого документа
- Вы отдаете себе отчет, что эта информация доступна всем, установка пароля в данном случае лишь мера предосторожности, от случайных корректировок, которые Вы хотите предотвратить
- Вы полагаете, что специалистов, способных извлечь информацию крайне мало

Чтобы защитить документ Word от копирования данных необходимо воспользоваться инструментом:

- Примечания
- Запись исправлений
- Только чтение
- Ввод данных в поля форм

Какие инструменты приводят к изменению архитектуры документа?

- Установка электронной цифровой подписи
- Ограничения на редактирование и форматирование
- Пометка "Окончательный"
- Шифрование документа
- Защита документов в формате .xls
- обеспечение безопасности табличных документов, созданных в программе MS Excel и других табличных процессорах

При создании цифровых подписей используются три компонента, какие из этих компонентов содержатся в самом документе:

- хеширование
- сертификаты
- шифрование с помощью ключа

Какие инструменты защиты в табличный редактор Excel перешли из текстового редактора Word?

- зашифровать документ
- электронная цифровая подпись
- пометка "окончательный"

– ограничить редактирование и форматирование

Одним способом снятия защиты с листа Excel является копирование содержимого защищенного листа на новый лист Excel, при этом необходимое условие реализации процедуры:

– выделение заблокированных и не заблокированных ячеек будет разрешено автором файла
– возможность загрузки документа на он-лайн сервисы
– наличие версии microsoft excel не ниже 2016 года
– использование многопользовательского режима в Office 365

Выделите ячейки, которые не надо защищать (если таковые есть), щелкните по ним правой кнопкой мыши и выберите в контекстном меню команду Формат ячеек (Format Cells). Будут защищены при включении защиты листа:

– все ячейки, для которых этот флажок останется установленным
– все подсвеченные цветом ячейки на текущем листе, при условии использовании соответствующего макроса
– все ячейки которые будут помечены в ручном режиме

Как можно узнать количество скрытых листов в MS Excel?

– в контекстном меню включить режим "отобразить листы"
– открыть документ через архиватор
– в опции "защитить лист"
– защита документов в формате .pdf
– обеспечение безопасности документов, созданных в on-line редакторах

Чтобы открыть Ваш зашифрованный PDF-файл, злоумышленнику потребуется:

– наличие современного оборудование, как минимум современные видеокарты nvidia/amd для gpu ускорения, и временной ресурс
– наличие специально программного обеспечения типа accent office password recovery, passcovery suite

- использование общих возможностей распределенной эвм, с внедренным алгоритмом, для получения доступа к ресурсу пользовательского персонального компьютера

Используя какое программное обеспечение можно защитить PDF-документ от копирования?

- он-лайн сервисы, аналоигчные pdf.io, pdf2go.com, ilovepdf.com, smallpdf.com
- защифровать в word или excel и пересохранить в формате pdf
- собрать постранично в программах для сканирования и распечатать в pdf.
- виртуальные принтеры (например, PDF Creator, Adobe PDF)

Снять защиту на открытия pdf-файла в рамках правового поля можно, используя

- специальное программное обеспечение, использующее методологию brute force
- онлайн сервисы, если знаешь пароль
- в ручную, подбирая пароль

С какой целью документ в формате Word сохраняют в файл формате PDF?

- чтобы его можно было открыть на компьютерах, где установлены macos или linux
- чтобы исключить, что "поедут" некоторые строчки или картинки
- чтобы исключить изменения текста и других данных документа

Как можно защитить pdf-файл от изменения авторский прав на документ

- наложить поверх документа водяной знак
- установить электронную цифровую подпись
- добавить рукописную подпись

Вопросы итогового тестирования

Как называется группа файлов, которая хранится отдельной группой и имеет собственное имя?

- байт
- каталог
- дискета

Какие символы разрешается использовать в имени файла или имени директории в Windows?

- цифры и только латинские буквы
- латинские, русские букву и цифры
- русские и латинские буквы

Выберите имя файла anketa с расширением txt.

- Anketa. txt.
- Anketa. txt
- Anketa/txt.

Какое наибольшее количество символов имеет имя файла или каталога в Windows?

- 255
- 10
- 8

Какое наибольшее количество символов имеет расширение имени файла?

- 3
- 8
- 2

Какое расширение у исполняемых файлов?

- exe, doc
- bak, bat
- exe, com, bat

Какой символ заменяет любое число любых символов?

- ?
- \
- *

Как записать : “Все файлы без исключения”?

- ?.?
- *.*
- *.?

Подкаталог SSS входит в каталог YYY. Как называется каталог YYY относительно каталога SSS?

- корневой
- дочерний
- родительский

Что выполняет компьютер сразу после включения POWER?

- перезагрузка системы
- проверку устройств и тестирование памяти
- загрузку программы

Могут ли быть несколько окон активными одновременно?

- да
- нет

Какое окно считается активным?

- первое из открытых
- любое
- то, в котором работаем.

Может ли каталог и файлы в нем иметь одинаковое имя?

- да
- нет

Может ли в одном каталоге быть два файла с одинаковыми именами?

- да
- нет

Может ли в разных каталогах быть два файла с одинаковыми именами.

- да
- нет

Возможно ли восстановить стертую информацию на жестком диске?

- возможно всегда
- возможно, но не всегда

Запись файлов на диске в виде разбросанных участков по всей поверхности диска называется…

- оптимизация диска
- фрагментация диска
- форматирование диска

Какое высказывание неверно? Дефрагментация проводят с целью …

- оптимизации дискового пространства
- ускорения процесса чтения и записи файлов
- сжатия информации

Какая из программ предназначена для дефрагментации диска?

- Smart Defrag
- NDD
- Unerase

Что выполняет операционная система при удалении файла с диска?
- перемешивает в fat его кластеры
- уничтожает первый символ имени файла в каталоге
- размагничивает участки диска, где располагался файл

Как можно удалить компьютерный вирус с диска?
- перезагрузить систему
- специальной программой
- удалить вирус невозможно

Архивация файлов – это…
- объединение нескольких файлов
- разметка дисков на сектора и дорожки
- сжатие файлов

Какая из программ является архиватором?
- NDD
- DRWEB
- RAR

Какая из программ является антивирусной программой?
- NDD
- DRWEB
- RAR

Что собой представляет компьютерный вирус?
- небольшая по размерам программа
- миф, которого не существует
- название популярной компьютерной игры

Что не поможет удалить с диска компьютерный вирус?
- дефрагментация диска
- проверка антивирусной программой
- форматирование диска

Какое утверждение верно?
- все файлы сжимаются при архивации одинаково
- файлы растровой графики сжимаются лучше всего

– различные типы файлов сжимаются при архивации по - разному

Архиваторы характеризуются…
– степенью и скоростью архивации
– способом распространения
– методом и скорость сжатия

Что не является каналом распространения вирусов?
– устройства визуального отображения информации
– компьютерные сети
– внешние носители информации.

Подсистема это:
– предопределенная рабочая среда, посредством которой система координирует выделение ресурсов и распределяет задачи
– множество элементов, находящихся в отношениях и связях друг с другом, которые образуют определённую целостность
– часть информационной системы, выделяемой при проектировании системной архитектуры.

Расширение файла, как правило, характеризует:
– объем памяти
– путь к папке, где хранятся данные
– тип данных, хранящихся в файле

Производительность работы компьютера зависит от:
– от комплектующих системного блока
– от установленного по
– от скорости Интернет-соединения

ОЗУ это память в которой хранится:
– информация о файловой системе
– выполняемый машинный код
– кэшированные данные процессора

Для выхода на поисковый сервер необходимо:
– зайти в браузер
– ввести запрос в поисковом меню
– вписать в адресную строку браузера адрес поискового сервиса

Процессор обрабатывает информацию:
– в текстовом формате
– в двоичном коде

– на языке Pascal

При отключении компьютера информация:
– удаляется с HDD
– сохраняется в кэше графического процессора
– удаляется с памяти ОЗУ

Протокол маршрутизации ip обеспечивает:
– пересылку информации в компьютерных сетях
– возможность связи нескольких компьютеров и их данных в одну общую сеть
– кодировку и дешифровку данных

Во время исполнения прикладная программа хранится
– в кэш-памяти ядра
– в памяти ОЗУ
– в памяти винчестера (жесткого диска)

За минимальную единицу измерения количества информации принято считать:
– байт
– килобит
– бит

Компьютер, подключенный к интернету, обязательно имеет:
– связь с удаленным сервером
– IP-адрес
– доменное имя

Практикоориентированная работа состоит из заданий, выполняемых в рамках практических и лабораторно-практических занятий.

Практические занятия

Практическое занятие №1 «Моделирование угроз безопасности»

1. Порядок моделирования угроз безопасности информации и разработки моделей угроз безопасности информации.
2. Определение возможных негативных последствий от реализации угроз безопасности информации.
3. Оценка условий реализации угроз безопасности информации.
4. Источники угроз безопасности информации и оценка возможностей нарушителей.

5. Определение сценариев реализации угроз безопасности информации.
6. Оценка уровней опасности угроз безопасности информации.

Практическое занятие №2 «Работа с AVZ»

1. Работа с программой.
2. Карантин и папка infected.
3. Встроенные средства поиска.
4. Встроенные утилиты.
5. Функции анализа и восстановления.
6. Подсистема AVZ Guard.
7. Подсистема AVZ PM.
8. Подсистема Boot Cleaner.
9. Параметры командной строки.

Практическое занятие №3 «Шифрование и электронно-цифровая подпись в системе документооборота»

1. Программа шифрования информации с открытым исходным кодом PGP.
2. Схемы шифрования электронной цифровой подписи.
3. Цифровая подпись.
4. Генерация ключа шифрования, шифрование и расшифровка сообщений.
5. Экспорт открытого ключа.
6. Шифрование файлов и установка под ними электронно-цифровой подписи. Расшифрование сообщений и идентификация подписи.
7. PGP диск.
8. Создание нового PGP диска.
9. Смена парольной фразы.

Практическое занятие №4 «Настройка безопасности рабочей станции пользователя»

1. Отключение учетной записи Гость.
2. Настройка получения автоматических обновлений.
3. Настройка параметров брандмауэра Windows.
4. Просмотр списка разрешенных программ.
5. Настройка параметров брандмауэра для новой сети.
6. Принудительное обновление антивирусной базы.
7. Создание пользователя без прав.

8. Запуск сетевых приложений от имени учетной записи, настройка автоматического запуска при запуске Windows.
9. Ограничение доступа к папке «Автозагрузка».
10. Использование on-line GUID/UUID генераторы.
11. Использование менеджера паролей в браузере.
12. Создание резервных копий.
13. Установка архиватора, с хорошей поддержкой командной строки.
14. Восстановление текстовых документов.

Лабораторно-практические занятий

Лабораторно-практическое занятие №1: «Тестирование безопасности операционной системы Windows»

1. Исследование надежности пароля администратора.
2. Очистка списков недавних мест и программ.
3. Очистка списка USB-накопителей.
4. Очистка кэша и истории браузеров.
5. Удаление записи DNS.
6. Удаление списка последних документов MS Office.

Лабораторно-практическое занятие №2: «Организация защищенного обмена данными»

1. Безключевое кодирование информации.
2. Создание QR-кодов.
3. Симметричное шифрование с помощью ресурса Crypt-online.
4. Ассиметричное шифрование RSA с помощью ресурса Crypt-online.
5. Передача зашифрованных сообщений.

Лабораторно-практическое занятие №3: «Маскировка передачи закрытых данных методом стеганографии»

1. Наиболее распространенные стеганографические программы.

2. S-Tools.
3. Steganos for Windows.
4. JSTEG Shell.

5. Шифрование и дешифрование с помощью сайта «Стеганография онлайн».

Лабораторно-практическое занятие №4: «Защищенный документооборот. Защита текстовых документов»

1. Ограничение редактирования тестового документа в редакторе Microsoft Word.
2. Пометить документ Microsoft Word как окончательный.
3. Шифрование документа редактором Microsoft Word с использованием пароля.
4. Добавление цифровой подписи в Microsoft Word.

Лабораторно-практическое занятие №5: «Защищенный документооборот. Защита табличных документов»

1. Защита данных в табличном редакторе MSExcel.
2. Защита структуры и окон электронной таблицы.
3. Скрытие и отображение дополнительных листов MSExcel.

8.5. Описание процедуры оценивания результатов обучения.

Реализация дополнительной профессиональной программы повышения квалификации «Основы информационной безопасности» завершается итоговой аттестацией в форме тестирования.

К тестированию допускаются лица, успешно выполнившие все лабораторные работы и показавшие удовлетворительные и более результаты при прохождении промежуточного тестирования.

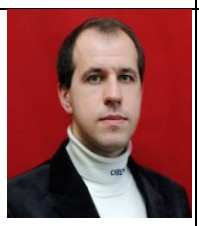
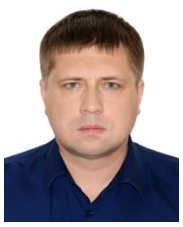
На выполнение итогового задания отводится 90 минут. Обучающиеся в отвечают на поставленные вопросы в режиме он-лайн. Результат тестирования выводится на экран слушателя и сохраняется в базе.

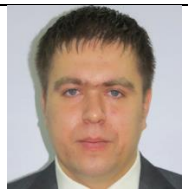
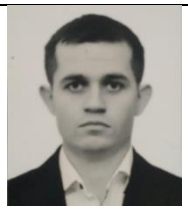
Отметка «зачтено» ставится в том случае, если обучающиеся выполнили итоговой тест на 51% и более.

Отметка «не зачтено» ставится в случае выполнения теста менее чем на 50 %.

9. Организационно-педагогические условия реализации программы

9.1. Кадровое обеспечение программы

№ п/п	Фамилия, имя, отчество (при наличии)	Место основной работы и должность, ученая степень и ученое звание (при наличии)	Ссылки на веб-страницы с портфолио (при наличии)	Фото в формате jpeg	Отметка о полученном согласии на обработку персональных данных
1	**Крыжевич Леонид Святославович**	ФГБОУ ВО "Курский государственный университет",кафедра информационной безопасности к.т.н., заведующий кафедрой	https://my.kursksu.ru/#/person/4690		**согласен**
2	**Бабкин Геннадий Викторович**	ФГБОУ ВО "Курский государственный университет",кафедра информационной безопасности, к.т.н., доцент кафедры	https://my.kursksu.ru/#/person/4241		**согласен**
3	**Глаголев Роман Владимирович**	ФГБОУ ВО "Курский государственный университет",кафедра информационной безопасности, к.т.н., доцент,доцент кафедры	https://my.kursksu.ru/#/person/18577		**согласен**

4.	**Гранкин Александр Николаевич**	ФГБОУ ВО "Курский государственный университет",кафедра информационной безопасности, к.т.н., доцент,доцент кафедры	https://my.kursksu.ru/#/person/18471		**согласен**
	Гордиенко Виктория Викторовна	ФГБОУ ВО "Курский государственный университет",кафедра информационной безопасности, к.т.н., доцент,доцент кафедры	https://my.kursksu.ru/#/person/23981		**согласна**
5.	**Лисицин Александр Леонидович**	ФГБОУ ВО "Курский государственный университет", кафедра информационной безопасности,старший преподаватель кафедры	https://my.kursksu.ru/#/person/37937		**согласен**

9.2. Учебно-методическое обеспечение и информационное сопровождение

Учебно-методические материалы	
Методы, формы и технологии	**Методические разработки, материалы курса, учебная литература**
Технологии обучения: технологии проблемного обучения, технологии дистанционного обучения, технология проектного обучения	

Методы обучения: проблемного изложения; репродуктивный; исследовательский; интерактивные методы; методы индивидуальной и дифференцированной работы.	
Формы обучения: индивидуально-групповые	
Лекционные занятия	**Основная литература** 1 Нестеров С. А. - Информационная безопасность: Учебник и практикум - М.: Издательство Юрайт, 2017. 2 Кияев В., Граничин О. - Безопасность информационных систем: курс - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. **Дополнительная литература** Рогозин В.Ю., Галушкин И.Б., Новиков В.К., Вепрев С.Б. - Основы информационной безопасности: учебник - Москва: ЮНИТИ-ДАНА, 2017. Сычев Ю.Н - Основы информационной безопасности: учебно-методическое пособие - Москва: Евразийский открытый институт, 2012.
Практические занятия	1 Крыжевич Л.С., Глаголев Р.В., Гордиенко В.В. Методические указания к практической работа: «Моделирование угроз безопасности» [Электронный документ]– Курск: 2020. – 16с. 2 Крыжевич Л.С., Глаголев Р.В., Гордиенко В.В. Методические указания к практической работа: «Работа с AVZ» [Электронный документ]– Курск: 2020. – 20 с. 3 Крыжевич Л.С., Глаголев Р.В., Гордиенко В.В. Методические указания к практической работа: «Шифрование и электронно-цифровая подпись в системе документооборота»[Электронный документ] – Курск: 2020. – 16с. 4 Крыжевич Л.С., Глаголев Р.В., Гордиенко В.В. Методические указания к практической работа: «Настройка безопасности рабочей станции пользователя» [Электронный документ]– Курск: 2020. – 16с.
Лабораторно – практические занятия	1 Крыжевич Л.С., Глаголев Р.В., Бабкин Г.В., Гордиенко В.В. Методические указания к лабораторно практическому занятию №1: «Тестирование безопасности операционной системы Windows» [Электронный документ]– Курск: 2020. – 16с.

	2 Крыжевич Л.С., Глаголев Р.В., Бабкин Г.В., Гордиенко В.В. Методические указания к лабораторно практическому занятию №2: «Организация защищенного обмена данными» [Электронный документ]– Курск: 2020. – 20 с. 3 Крыжевич Л.С., Глаголев Р.В., Бабкин Г.В., Гордиенко В.В. Методические указания к лабораторно практическому занятию №3: «Маскировка передачи закрытых данных методом стеганографии» [Электронный документ]– Курск: 2020. – 12 с. 4 Крыжевич Л.С., Глаголев Р.В., Бабкин Г.В., Гордиенко В.В. Методические указания к лабораторно практическому занятию №4: «Защищенный документооборот. Защита текстовых документов» [Электронный документ]– Курск: 2020. – 12 с. 5 Крыжевич Л.С., Глаголев Р.В., Бабкин Г.В., Гордиенко В.В. Методические указания к лабораторно практическому занятию №4: «Защищенный документооборот. Защита табличных документов» [Электронный документ]– Курск: 2020. – 16 с.

Информационное сопровождение	
Электронные образовательные ресурсы	Электронные информационные ресурсы
course.secsem.ru — спецкурс «Современная криптография» и «Безопасность приложений» (факультет ВМК МГУ имени М. В. Ломоносова и компании Яндекс)	https://fstec.ru/
http://window.edu.ru/resource/775/77775 – учебная литература по информационной безопасности	xssed.com - сборник в уязвимостей
https://intuit.ru/studies/courses/10/10/info курс основы информационной безопасности	https://www.anti-malware.ru/ - информационно-аналитический портал

9.3. Материально-технические условия реализации программы

Вид занятий	Наименование оборудования, программного обеспечения
Лекционные (теоретические) занятия	ПК с доступом в Интернет; платформа Zoom, платформа Moodle
Практические занятия	ПК с доступом в Интернет; операционная система Windows; платформа Zoom;

	платформа Moodle; свободно распространяемое программное обеспечение с открытым исходным кодом программа шифрования PGP, S-Tools. Steganos for Windows. JSTEG Shell, антивирусная программа AVZ
Лабораторно-практические	ПК с доступом в Интернет; операционная система Windows; платформа Zoom; платформа Moodle;, MS Office

Приложение

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«КУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа повышения квалификации по дисциплине: «Основы информационной безопасности»

(**72 час**)

1.	Наименование компетенции		ПК-4 – способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
	Указание типа компетенции	профессиональная	Обеспечивает способность сотрудника выполнять задачи в соответствии с существующими стандартами информационной безопасности.
3.	Определение, содержание и основные сущностные характеристики компетенции		Под компетенцией ПК-4 понимается способность постановки и нахождения путей решения прикладных задач информационной безопасности с использованием современных технических и программных средств. Слушатель курсов должен: знать: – основные угрозы информационной безопасности и программное обеспечение для решения прикладных задач; – классификацию информационных систем, структуру, конфигурацию информационных систем, общую характеристику процесса организации защиты информационных систем; – структуру состав и свойства информационных процессов, систем и технологий, методы анализа устойчивости информационных систем, модели представления угроз информационной безопасности; – структуру, принципы реализации и функционирования технологий, используемых при создании комплексной системы информационной безопасности, инструментальные средства информационной безопасности. уметь: – использовать методы защиты информации в своей профессиональной деятельности; – использовать детализированные решения при разработке мероприятий по обеспечению информационной безопасности; – применять технологии информационной безопасности при обслуживании информационных систем. владеть: – навыками использования программного обеспечения для решения прикладных задач; – моделями и средствами разработки мероприятий по обеспечению информационных систем;

		– методами и средствами использования технологий информационной безопасности при обслуживании информационных систем.	
	Дескриптор знаний, умений и навыков по уровням	Уровни сформированности компетенции обучающегося	Индикаторы
		Начальный уровень Знает: базовые принципы обеспечения информационной безопасности, а также наиболее распространенные типы угроз и основные возможности стандартного программного обеспечения при решении профессиональных задач. Умеет: применять математические методы, технические и программные средства для решения стандартных задач в области профессиональной деятельности.	Демонстрирует знания: – Сущность и содержание понятия информационной безопасности, характеристики ее составляющих; – Нормативные правовые акты в области защиты информации; – Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; Демонстрирует умения: – Настраивать компоненты подсистем защиты информации операционных систем; – Управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей; – Применять антивирусные средства защиты информации в операционных системах; Подтверждает владение навыками: – Защиты текстовых документов; – Подготовки персональных рабочих станций к внешней проверке;

		Владеет: навыками использования программного обеспечения для решения прикладных задач.	
		Базовый уровень Знает: основные виды уязвимостей, а также большинство типов внешних угроз и основные возможности прикладных пакетов при решении профессиональных задач. Умеет: применять математические методы, технические и программные средства для решения задач информационной безопасности в области профессиональной деятельности, строить траекторию защиты информационной целостности	Демонстрирует знания: - Архитектура и пользовательские интерфейсы операционных систем; – Порядок обеспечения безопасности информации при эксплуатации операционных систем; – Источники угроз информационной безопасности и меры по их предотвращению; – Типовые средства защиты информации в операционных системах; – Порядок эксплуатации средств антивирусной защиты в операционных системах; Демонстрирует умения: – Применять программно-аппаратные средства защиты информации в операционных системах; – Работать в операционных системах с соблюдением действующих требований по защите информации; – Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации; – Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации; Подтверждает владение навыками: – Тестирования безопасности операционной системы Windows;

		структурного подразделения. Владеет: методами планирования организации защиты информационных систем с использованием штатных средств обеспечения информационной безопасности	– Подготовки персональных рабочих станций к эксплуатации в условиях потенциальных угроз;
		Продвинутый уровень Знает: принципы идентификации основных видов уязвимостей и внешних угроз, а также область применения прикладных пакетов при решении профессиональных задач. Умеет: применять математические методы, технические и программные средства для решения задач	Демонстрирует знания: – Программно-аппаратные средства и методы защиты информации; – Формы и методы инструктажа пользователей по порядку работы в операционных системах; – Общие принципы функционирования программно-аппаратных средств криптографической защиты информации; – Порядок оформления эксплуатационной документации; – Организационные меры по защите информации. Демонстрирует умения: – Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; – Контролировать целостность подсистем защиты информации операционных систем; – Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации;

		информационной безопасности в области профессиональной деятельности, строить траекторию защиты информационной целостности структурного подразделения, подбирать методы и средства обеспечения информационной безопасности. Владеет: методами интеграции спланированных мероприятий по обеспечению информационной безопасности в деятельность структурных подразделений, с использованием программных средств обеспечения информационной безопасности	– Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации. Подтверждает владение навыками: – Передачи защищенной и маскированной информации; – Преобразования данных посредствам криптосистемы RSA.
5.	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими	Настоящий курс ориентирован на обеспечение начального уровня подготовки для деятельности в профессиональной сфере, таким образом для его освоения достаточно знаний полученных в процессе среднего профессионального или высшего (не профильного образования), в свою очередь настоящая компетенция является необходимой для освоения	

	компетенциями для формирования данной компетенции	ряда трудовых функций из профессионального стандарта06.032 "Специалист по безопасности компьютерных систем и сетей" утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года N 598н, а именно: администрирование средств защиты информации в компьютерных системах и сетях; оценивание уровня безопасности компьютерных систем и сетей; разработка программно-аппаратных средств защиты информации компьютерных систем и сетей
6.	Средства и технологии оценки	Оценка уровня подготовки, проходит на основании предоставления отчетности по практическим и лабораторно-практическим занятиям, оформленные по типовому шаблону и реализованных в форме электронного документа. Тестирование является универсальным средством готовности обучающегося по освоению материала, как отдельного модуля, так и итоговой подготовки.

Иная информация о качестве и востребованности образовательной программы

Качество настоящей программы дополнительного профессионального образования в настоящий подтверждается:

- номинальным соответствием результатов освоения дополнительной профессиональной программы «Основы информационной безопасности» заявленным целям и планируемым результатам обучения;

- соответствия процедуры (процесса) организации и осуществления дополнительной

профессиональной программы «Основы информационной безопасности» установленным требованиям к структуре, порядку и

условиям реализации программ;

- способности организации результативно и эффективно выполнять деятельность по предоставлению дополнительных образовательных услуг.

Рекомендаций к программе от работодателей

Программа дополнительного профессионального образования «Основы информационной безопасности» рекомендована к реализации в рамках Государственной системы предоставления ПЦС по направлению цифровой экономики «Кибербезопасность и защита данных» двумя организациями, испытывающими потребность в специалистах высокого в сфере обеспечения информационной безопасности, и соответственно являющиеся потенциальными работодателями в настоящей сфере Курской области – ООО Центр системной безопасности «Щит-информ» и Комитет социального обеспечения, материнства и детства Курской области

Указание на возможные сценарии профессиональной траектории граждан по итогам освоения образовательной программы

По итогам освоения программы слушатель может выполнять обязанности по должности (профессии):

– Техник по защите информации;

– Техник по безопасности компьютерных систем и сетей.

Сценарии профессиональной траектории граждан

Цели получения персонального цифрового сертификата	
текущий статус	цель
Трудоустройство	
состоящий на учете в Центре занятости безработный	трудоустроенный
Развитие компетенций в текущей сфере занятости	
работающий по найму в организации, на предприятии	развитие профессиональных качеств, смена работы без изменения сферы профессиональной деятельности
Переход в новую сферу занятости	
освоение новой сферы занятости	расширение кругозора
освоение смежных профессиональных областей	расширение профессиональной деятельности

Дополнительная информация

Программа дополнительного профессионального образования «Основы информационной безопасности» обеспечивает формирование у слушателей осознание принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения. Способствует формированию навыков, связанных с обеспечением защиты информации; творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности объектов

информатизации; создание представления об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.

Процесс обучения по программе дополнительного профессионального образования проводится с использованием дистанционных технологий в очной (контактной) форме взаимодействия, реализуемых посредствам организации он-лайн лекционных, практических и лабраторно-практических занятий, вместе с этим широко используя технологию дистанционного тестирования слушателей.

Программа охватывает круг вопросов, связанных с обеспечением информационной безопасности информационных систем. Освоение программы позволит получить знания в областях:

- защиты операционных систем, программ и данных;
- реализации защищённого электронного документооборота;
- криптографические и стеганографические методы защиты данных.

Общество с ограниченной ответственностью «ТЕХНО-ЩИТ»
Юридический адрес: 305001, Курская обл., г. Курск, ул. Александра Невского, д. 7, литер А, офис 42, ОГРН 1114632004475, ИНН 4632152654, КПП 463201001
тел. +7 (4712) 26-99-99 e-mail: info@tehshield.ru

№ 074-20/ТЩ/П

08 . 010 . 2020

Рекомендательное письмо
о реализации в рамках Государственной системы предоставления ПЦС программы дополнительного профессионального образования «Основы информационной безопасности»

Программа дополнительного профессионального образования «Основы информационной безопасности» по направлению цифровой экономики «Кибербезопасность и защита данных» представляет собой систему документов, разработанную на основе Профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей» утвержденного приказом Министерством труда и социального развития РФ от 1 ноября 2016 года №598н.

Программа дополнительного профессионального образования отвечает основной цели вида профессиональной деятельности – обеспечение защиты информации в компьютерных системах и сетях в условиях существования киберугроз. Ее структура включает следующие модули: защита операционных систем, программ и данных; защищенный электронный документооборот; криптографические и стеганографические методы защиты информации, итоговая аттестация.

Качество содержательной составляющей программы дополнительного профессионального образования «Основы информационной безопасности» направлено на формирование профессиональных функций. Структура программы логична и последовательна.

Контрольно-оценочные средства соответствуют целям и задачам программы дополнительного профессионального образования «Основы информационной безопасности» и обеспечивают оценку качества компетенций, приобретаемых слушателем.

Разработанная программа дополнительного профессионального образования «Основы информационной безопасности» имеет достаточный уровень подготовки слушателей, по итогам успешного освоения, которого возможна перспектива прохождения стажировки на базе ООО «ТЕХНО-ЩИТ», что может послужить существенным аргументом при последующем

трудостройстве в сфере обеспечения информационной безопасности и смежных отраслях.

Программа дополнительного профессионального образования «Основы информационной безопасности» рекомендована к реализации в рамках Государственной системы предоставления ПЦС по направлению цифровой экономики «Кибербезопасность и защита данных».

Директор по информационной безопасности _____ И.В. Волобуева

М.П.

АДМИНИСТРАЦИЯ
КУРСКОЙ ОБЛАСТИ
КОМИТЕТ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ,
МАТЕРИНСТВА И ДЕТСТВА КУРСКОЙ ОБЛАСТИ
(КОМИТЕТ СОЦОБЕСПЕЧЕНИЯ,
МАТЕРИНСТВА И ДЕТСТВА КУРСКОЙ ОБЛАСТИ)

305007, г. Курск, ул. Моковская, д. 2-г,
тел.: +7 (4712) 35-75-23, факс +7 (4712) 35-17-59
e-mail: kso@rkursk.ru;
www.ksokursk.ru

№ 083-07/9869 от 12.10.2020

Рекомендательное письмо
о реализации в рамках Государственной системы предоставления
ПЦС программы дополнительного профессионального образования
«Основы информационной безопасности»

Программа дополнительного профессионального образования «Основы информационной безопасности» по направлению цифровой экономики «Кибербезопасность и защита данных» представляет собой систему документов, разработанную на основе Профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей» утвержденного приказом Министерством труда и социального развития РФ от 1 ноября 2016 года N 598н.

Программа дополнительного профессионального образования отвечает основной цели вида профессиональной деятельности – обеспечение защиты информации в компьютерных системах и сетях в условиях существования киберугроз. Ее структура включает следующие модули: защита операционных систем, программ и данных; защищенный электронный документооборот; криптографические и стеганографические методы защиты информации, итоговая аттестация.

Качество содержательной составляющей программы дополнительного профессионального образования «Основы информационной безопасности» направлено на формирование профессиональных функций. Структура программы логична и последовательна. Контрольно-оценочные средства соответствуют целям и задачам программы дополнительного профессионального образования «Основы информационной безопасности» и обеспечивают оценку качества компетенций, приобретаемых слушателем.

Разработанная программа дополнительного профессионального образования «Основы информационной безопасности» имеет достаточный уровень подготовки

слушателей, по итогам успешного освоения, которого возможна перспектива прохождения стажировки на базе комитета социального обеспечения, материнства и детства Курской области, что может послужить существенным аргументом при последующем трудостройстве в сфере обеспечения информационной безопасности и смежных отраслях.

Программа дополнительного профессионального образования «Основы информационной безопасности» рекомендована к реализации в рамках Государственной системы предоставления ПЦС по направлению цифровой экономики «Кибербезопасность и защита данных».

Председатель комитета  Т.А. Сукновалова