АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»
Факультет экономики и управления
Кафедра «Бизнес-информатика»

УТВЕРЖДАЮ
Проректор по учебно-
методической работе
_____ С.С. Скараник
«01» сентября 2020г.

Рабочая программа дисциплины
Информационная безопасность и защита информации

Направление подготовки
38.03.05 Бизнес-информатика

Квалификация выпускника
Бакалавр

Для всех
форм обучения

Симферополь 2020

Содержание

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 3

2. Место дисциплины в структуре ОПОП бакалавриата 4

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся 4

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий 4

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 7

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине 8

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 22

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины * 23

9. Методические указания для обучающихся по освоению дисциплины 24

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости) 24

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине 25

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины обучающийся должен овладеть следующими знаниями, умениями и навыками:

<table>
<tr><th>Коды компетенций</th><th>Результаты освоения ОПОП</th><th>Перечень планируемых результатов обучения по дисциплине</th></tr>
<tr><td>ОК-4</td><td>способность использовать основы правовых знаний в различных сферах деятельности</td><td rowspan="4"><u>Знать:</u>
• основы правовых знаний в различных сфере информационной безопасности;
• Основные принципы самоорганизации и самообразования
• методы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;
• способы организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью;
• права на интеллектуальную собственность.
<u>Уметь:</u>
• использовать основы правовых знаний в различных сферах деятельности;
• Организовать свое время, самостоятельно критически мыслить, формулировать свою точку зрения
• решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности;
• организовывать взаимодействие с клиентами и партнерами в процессе решения задач ;
• защищать права на интеллектуальную собственность.
<u>Владеть:</u>
• способностью использовать основы правовых знаний в различных сферах деятельности;
• Методами повышения квалификации,</td></tr>
<tr><td>ОК-7</td><td>способностью к самоорганизации и самообразованию</td></tr>
<tr><td>ОПК-1</td><td>способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</td></tr>
<tr><td>ПК-9</td><td>организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия</td></tr>
</table>

Коды компетенций	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-11	умение защищать права на интеллектуальную собственность	навыками накопления, обработки и использования информации • способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; • организация взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; • умение защищать права на интеллектуальную собственность.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.06 «Информационная безопасность» входит в вариативную часть дисциплин. Для успешного изучения необходимо предварительное овладения такими дисциплинами как: информатика; вычислительные системы, сети и телекоммуникации; стандартизация, сертификация и управление качеством программного обеспечения. Изучение дисциплины необходимо для таких предметов как: Архитектура и ИТ-инфраструктура предприятия; основы цифровой экономики; проектирование ИС.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144
Контактная работа	78
Аудиторная работа (всего):	72
Лекции	18
Семинары, практические занятия	54
Самостоятельная работа обучающихся	68

(всего)	
Дифф.зачет	4

Для заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	**Всего часов**
Общая трудоемкость дисциплины	144
Контактная работа	20
Аудиторная работа (всего):	14
Лекции	8
Семинары, практические занятия	6
Самостоятельная работа обучающихся (всего)	126
Дифф.зачет	4

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ темы	Наименование темы	Всего		Количество часов					
		ОФО	ЗФО	Контактная работа (аудиторная работа)				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
1	Тема 1. Общие вопросы информационной безопасности	14	14	2	1	2	1	10	12
2	Тема 2. Государственная система информационной безопасности	12	14	2	1	2	1	8	12
3	Тема 3. Угрозы безопасности	10	12	2	1	2	1	6	10
4	Тема 4. Теоретические основы методов защиты информационных систем	14	13	2	1	4		8	12
5	Тема 5. Методы защиты средств вычислительной техники	14	14	2	1	4	1	8	12
6	Тема 6. Основы криптографии	32	29	2	1	22	2	8	26
7	Тема 7. Архитектура защищенных экономических систем	14	15	2	1	6		6	14

8	Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению	14	15	2	1	6		6	14
9	Тема 9. Алгоритмы безопасности в компьютерных сетях	16	14	2		6		8	14
	Всего по дисциплине	140	140	18	8	54	6	68	126
	Дифф.зачет	4	4						
	Итого	**144**	**144**	**18**	**8**	**54**	**6**	**68**	**126**

4.2 Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Общие вопросы информационной безопасности

Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.

Тема 2. Государственная система информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Тема 3. Угрозы безопасности

Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Тема 4. Теоретические основы методов защиты информационных систем

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-Ла-Падулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.

Тема 5. Методы защиты средств вычислительной техники

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

Тема 6. Основы криптографии

Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации.

Тема 7. Архитектура защищенных экономических систем

Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.

Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению

Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода.

Тема 9. Алгоритмы безопасности в компьютерных сетях

Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

4.3. Темы практических занятий.

Практическая работа 1. Определение требований к защите информации

Практическая работа 2. Определение классов защищенности средств вычислительной техники от несанкционированного доступа

Практическая работа 3. Обзор нормативных документов в области обеспечения информационной безопасности ИСПДН и ГИС

Практическая работа 4. Работа с ГОСТами в области информационной безопасности

Практическая работа 5. Составление инструкции по обработке и хранению конфиденциальных документов

Практическая работа 6. Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации

Практическая работа 7. Оценка уязвимости информации

Практическая работа 8. Проведение анализа информации на предмет целостности

Практическая работа 9. Настройка BIOS, политик авторизации и аудита в

Windows

Практическая работа 10. Управление учетными записями в Windows

Практическая работа 11. Настройка прав доступа пользователей к объектам в Windows

Практическая работа 12. Настройка аудита доступа пользователей к объектам в Windows

Практическая работа 13. Ограничение запуска программ и использования съемных носителей в Windows

Практическая работа 14. Наследование разрешений в NTFS

Практическая работа 15. Настройка параметров безопасности Интернет

Практическая работа 16. Использование технологии шифрования Bitlocker

Практическая работа 17. Использование СКЗИ VipNet Safedisk

Практическая работа 18. Использование СКЗИ TrueCrypt

Практическая работа 19. Использование МЭ VipNet Personal Firewall

Практическая работа 20. Использование МЭ TrustAccess

Практическая работа 21. Использование САВЗ Dr. Web Security Space

Практическая работа 22. Использование ПАК «Соболь

Практическая работа 23. Анализ рисков на основе РискМенеджер

Практическая работа 24. Анализ рисков на основе Digital Security КОНДОР

Практическая работа 25. Анализ рисков на основе модели угроз и уязвимостей

Практическая работа 26. Оценка безопасности информации на объектах ее обработки

Практическая работа 27. Анализ и управление рисками информационной системы

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№ темы	Содержание заданий, выносимых на СРС	Кол-во часов ОФО	Кол-во часов ЗФО	Учебно-методическое обеспечение
1	Тема 1. Общие вопросы информационной безопасности	10	12	Учебно-методическое пособие
2	Тема 2. Государственная система информационной безопасности	10	12	Учебно-методическое пособие
3	Тема 3. Угрозы безопасности	6	8	Учебно-методическое пособие
4	Тема 4. Теоретические основы методов защиты информационных систем	8	13	Учебно-методическое пособие
5	Тема 5. Методы защиты средств вычислительной техники	8	12	Учебно-методическое пособие
6	Тема 6. Основы криптографии	9	30	Учебно-методическое пособие
7	Тема 7. Архитектура	7	14	Учебно-методическое

№ темы	Содержание заданий, выносимых на СРС	Кол-во часов ОФО	Кол-во часов ЗФО	Учебно-методическое обеспечение
	защищенных экономических систем			пособие
8	Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению	7	14	Учебно-методическое пособие
9	Тема 9. Алгоритмы безопасности в компьютерных сетях	7	15	Учебно-методическое пособие

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Паспорт фонда оценочных средств по дисциплине

Компетенция ОК-4

способность использовать основы правовых знаний в различных сферах деятельности		
Этапы формирования компетенции		
Знает	Умеет	Владеет
основы правовых знаний в различных сфере информационной безопасности; 6.2.1 (1-10, 19)	использовать основы правовых знаний в различных сферах деятельности 6.2.1 (1-10, 19), 6.2.2 (1-30), 6.2.3 (20-31)	способностью использовать основы правовых знаний в различных сферах деятельности 6.2.1 (1-10, 19), 6.2.2 (1-30), 6.2.3 (20-31)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-10, 19) Умеет, если выполнил 6.2.1 (1-10, 19), 6.2.2 (1-30) Владеет, если выполнил 6.2.1 (1-10, 19), 6.2.2 (1-30), 6.2.3 (20-31)		

Компетенция ОК-7

способностью к самоорганизации и самообразованию		
Этапы формирования компетенции		
Знает	Умеет	Владеет
Основные принципы самоорганизации и самообразования; Знает, если выполнил 6.2.1 (1-9, 14-22, 23-25), 6.2.2(1-15, 17-26), 6.2.3(1-13,25-31)	Организовать свое время, самостоятельно критически мыслить, формулировать свою точку зрения; Умеет, если выполнил 6.2.1 (10-13, 22-30, 6.2.2(14-20), 6.2.3(14-21)	Методами повышения квалификации, навыками накопления, обработки и использования информации; Владеет, если выполнил 6.2.1 (24-30), 6.2.4(1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-9, 14-22, 23-25), 6.2.2(1-15, 17-26), 6.2.3(1-13,25-31) Умеет, если выполнил 6.2.1 (10-13, 22-30, 6.2.2(14-20), 6.2.3(14-21) Владеет, если выполнил 6.2.1 (24-30), 6.2.4(1-5)		

Компетенция ОПК-1

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
Этапы формирования компетенции		
Знает	Умеет	Владеет
методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности 6.2.1 (1-30)	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности 6.2.2 (1-20), 6.2.3 (1-31)	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 – (1-30) Умеет, если выполнил 6.2.2 – (1-20), 6.2.3 – (1-31) Владеет, если выполнил 6.2.4 – (1-5)		

Компетенция ПК-9

организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия		
Этапы формирования компетенции		
Знает	Умеет	Владеет
способы организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью 6.2.1 (1-30)	организация взаимодействие с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия 6.2.2 (1-20), 6.2.3 (1-31)	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 – (1-30) Умеет, если выполнил 6.2.2 – (1-20), 6.2.3 – (1-31) Владеет, если выполнил 6.2.4 –(1-5)		

Компетенция ПК-11

умение защищать права на интеллектуальную собственность
Этапы формирования компетенции

Знает	Умеет	Владеет
права на интеллектуальную собственность 6.2.1 (2,7,10,30)	защищать права на интеллектуальную собственность 6.2.2 (1-18), 6.2.3 (1-6, 11-31)	умение защищать права на интеллектуальную собственность 6.2.4 (1-3)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 – (2,7,10,30) Умеет, если выполнил 6.2.2 – (1-18) 6.2.3 – (1-6) , (11-31) Владеет, если выполнил 6.2.4 – (1-3)		

6.2.Типовые контрольные задания или иные материалы

6.2.1. Типовые вопросы к дифференцированному зачету

1. Особенности современных автоматизированных систем.
2. Требования к системам и средствам защиты информации от несанкционированного доступа.
3. Классификация автоматизированных систем и требования по защите информации.
4. Показатели защищенности средств вычислительной техники.
5. Соответствие классов систем различным уровням конфиденциальности.
6. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности.
7. Политика безопасности.
8. Принципы построения системы защиты информации.
9. Определение уязвимостей автоматизированных систем и выбор средств защиты.
10. Формирование требований к построению систем защиты.
11. Создание автоматизированных систем в защищенном исполнении.
12. Классификация каналов утечки информации.
13. Методы защиты речевой информации.
14. Методы контроля доступа к ресурсам компьютерной системы.
15. Модели безопасности компьютерных систем.
16. Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий.
17. Уязвимости приложений: атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных.
18. Атаки на web-приложения: атаки типа SQL-инъекция и межсайтовый скриптинг.
19. Требования ФСТЭК России к программному обеспечению средств защиты и его классификация по уровню отсутствия недекларированных возможностей.
20. Виртуальные частные сети. Криптографическая защита трафика на всех уровнях модели ISO/OSI.
21. Криптографическая защиты сетевого уровня. Семейство протоколов IPsec и его модификации.

22. Средства криптографической защиты прикладного уровня. Протокол SSL/TLS.

23. Виды межсетевых экранов. Принципы работы межсетевых экранов.

24. Уязвимости основных протоколов сетевого взаимодействия.

25. Место информационной безопасности в системе национальной безопасности.

26. Современная доктрина информационной безопасности Российской Федерации.

27. Государственная, общественная и социальная информационная безопасность.

28. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности.

29. Технические методы и средства защиты информации. Программно-аппаратные средства информационной безопасности.

30. Криптографические методы защиты информации. Комплексное обеспечение информационной безопасности.

6.2.2. Типовые тестовые задания

1. Под информационной безопасностью понимается…

А) 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.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость
В) нет правильного ответа

6. Целостность – это..

А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность – это..

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

8. **Для чего создаются информационные системы**?

А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:

А) статическую
Б) динамичную
В) структурную

10.Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

11.Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

12.Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13.Атака – это…

А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14.Источник угрозы – это..

А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

15.Оно опасности – это…

А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16.Каие события должны произойти за время существования окна опасности?

А) должно стать известно о средствах использования пробелов в защите.

Б) должны быть выпущены соответствующие заплаты.

В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:

А) по спектру И.Б.

Б) по способу осуществления

В) по компонентам И.С.

18.По каким компонентам классифицируется угрозы доступности:

А) отказ пользователей

Б) отказ поддерживающей инфраструктуры

В) ошибка в программе

19.Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

В) все ответы правильные

20.Основными источниками внутренних отказов являются:

А) ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

Б) обрабатывать большой объем программной информации

В) нет правильного ответа

22.Какие существуют грани вредоносного П.О.?

А) вредоносная функция

Б) внешнее представление

В) способ распространения

23.По механизму распространения П.О. различают:

А) вирусы

Б) черви

В) все ответы правильные

24.Вирус – это…

А) код обладающий способностью к распространению путем внедрения в другие программы

Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25.Черви – это…

А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

26.Конфиденциальную информацию можно разделить:

А) предметную
Б) служебную
В) глобальную

27.Природа происхождения угроз:

А) случайные
Б) преднамеренные
В) природные

28.Предпосылки появления угроз:

А) объективные
Б) субъективные
В) преднамеренные

29.К какому виду угроз относится присвоение чужого права?

А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

30.Отказ, ошибки, сбой – это:

А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

31.Отказ - это…

А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

32.Ошибка – это…

А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

33.Сбой – это…

А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

34.Побочное влияние – это…

А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

35.СЗИ (система защиты информации) делится:

А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

36.Что относится к человеческому компоненту СЗИ?

А) системные порты
Б) администрация
В) программное обеспечение

37.Что относится к ресурсам А.С. СЗИ?

А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные

38.По уровню обеспеченной защиты все системы делят:

А) сильной защиты
Б) особой защиты
В) слабой защиты

39.По активности реагирования СЗИ системы делят:

А) пассивные
Б) активные
В) полупассивные

40.Правовое обеспечение безопасности информации – это…

А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

41.Правовое обеспечение безопасности информации делится:

А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные

42.Информацию с ограниченным доступом делят:

А) государственную тайну
Б) конфиденциальную информацию
В) достоверную информацию

43.Что относится к государственной тайне?

А) сведения, защищаемые государством в области военной, экономической

… деятельности
Б) документированная информация
В) нет правильного ответа

44.Вредоносная программа - это…

А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45.Основополагающие документы для обеспечения безопасности внутри организации:

А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

46.К организационно - административному обеспечению информации относится:

А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

47.Что относится к организационным мероприятиям:

А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

48.Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) аппаратные
Б) криптографические
В) физические

49.Программные средства – это…

А) специальные программы и системы защиты информации в информационных системах различного назначения
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…

А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

Ключ к тесту

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.

А	А	А Б	А Б В	А	АБВ	А	А	АБ	АВ
11.	12.	13.	14.	15.	16.	17.	18.	19.	20.
В	А	А	А	А	АБВ	АБВ	АБ	В	АБВ
21.	22.	23.	24.	25.	26.	27.	28.	29.	30.
А	БВ	В	А	А	АБ	АБ	АБ	А	А
31.	32.	33.	34.	35.	36.	37.	38.	39.	40.
А	А	А	А	АБВ	АБ	В	АБВ	АБ	А
41.	42.	43.	44.	45.	46.	47.	48.	49.	50.
В	Б	А	А	АБВ	АБВ	АВ	АБВ	А	А

6.2.3. Темы рефератов

1. Основные понятия информационной безопасности. Цель защиты информации в частном и государственном секторе.
2. Современные требования к системе информационной безопасности организации.
3. Основные этапы создания системы защиты информации в организации.
4. Функциональное построение системы защиты информации.
5. Организационное построение системы защиты информации в организации. Семирубежная модель защиты.
6. Практические проблемы обеспечения информационной безопасности.
7. Место информационной безопасности в системе национальной безопасности Российской Федерации.
8. Структура Государственной системы обеспечения информационной безопасности Российской Федерации.
9. Структура и задачи Федеральной службы по техническому и экспортному контролю, и ее роль в управлении информационной безопасностью в РФ.
10. Иерархия законодательства Российской Федерации в области информационной безопасности.
11. Основные направления обеспечения информационной безопасности на предприятии.
12. Многоуровневая структура системы защиты информации на предприятии.
13. Стратегии организации защиты информации на предприятии.
14. Архитектура системы защиты конфиденциального документооборота на предприятии.
15. Основные направления формирования конфиденциальных документов на предприятии.
16. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений на предприятии.
17. Порядок документирования конфиденциальных сведений.
18. Основные носители конфиденциальных сведений и угрозы конфиденциальному документообороту.
19. Жизненный цикл конфиденциального документа.
20. Структура документированной системы защиты в РФ.

21. Цели и задачи Политики информационной безопасности на предприятии

22. Уровни Политики информационной безопасности на предприятии.

23. Разработка Концепции безопасности информации и Регламента обеспечения безопасности информации на предприятии.

24. Понятие Профиль защиты и его составляющие.

25. Система физической защиты (СФЗ): основные задачи и способы их решения на предприятии.

26. Сценарии последовательности действий нарушителя СФЗ.

27. Организация инженерно-технических средств охраны.

28. Международные стандарты в области информационной безопасности.

29. Цели, задачи и стадии проведения аудита информационной безопасности.

30. Виды аудита информационной безопасности, применяемые на различных стадиях жизненного цикла обследуемого объекта.

31. Состав работ по проведения аудита информационной безопасности.

6.2.4. Типовые задания на контрольную работу

Задание 1. Информационная безопасность операционной системы.

Сравнительная оценка информационной безопасности 2-3 операционных систем. Например, Windows, Linux, FreeBSD, Android или др.

Отчет: В документе Word напечатать для выбранных версий OS скриншоты наблюдений 2-5 процессов, служб, автозагрузок, настроек операционной системы с краткими комментариями и оценками угроз, уязвимостей и мер защиты каждой операционной системы.

Задание 2. Информационная безопасность серверных баз данных

Оценка информационной безопасности серверных баз данных. Написать сценарии работы с сервером баз данных СУБД MySQL или Oracle Database Express Edition 11g, привести примеры конфигурационных файлов и скриншоты настроек прав доступа к данным.

Отчет: В документе Word напечатать скриншоты, примеры сценариев и конфигурационных файлов настроек безопасности баз данных, комментарии к ним с оценками информационной безопасности баз данных.

Задание 3. Информационная безопасность Web-сайта

Оценка информационной безопасности Web-сайта (HTML, CSS, JavaScript, PHP). Написать или использовать готовые 1-2 сценария работы с данными Web-сайта. Использовать в сценарии работу с сессиями, шифрование пароля или данных.

Отчет: В документе Word напечатать скриншоты настроек безопасности Web-сайта и примеры конфигурационных файлов, комментарии к сценариям для Web-сайта с оценками информационной безопасности сайта и сервера.

Задание 4. «Алгоритм Хаффмана».

1) подсчитать встречаемость каждого символа в тексте индивидуального задания;

2) построить дерево Хаффмана;

3) записать текст в формате заархивированного файла (в виде последовательности кодов символов);

4) рассчитать коэффициент сжатия и результаты вычислений представить в виде следующей таблицы (для представления одного символа в исходном тексте выделяется 8 бит):

Символ	А	Б	…	…	…	ИТОГО
Количество символов	4	8	…	…	…	
Исходный размер	4*8=32	8*8=64	…	…	…	
Код замены	010	11100	…	…	…	
Итоговый размер	4*3=12	8*5=40	…	…	…	

5) сделать вывод, в котором необходимо указать во сколько раз уменьшился размер файла.

Варианты индивидуальных заданий

Вариант №1

Сеню - с ног, Саню - в бок, Соню - в лоб. Все в сугроб - хлоп!

Всех скороговорок не перескороговоришь,
не перевыскороговоришь.
Вылит колокол не по-колоколовски,
надо колокол переколоколовать, перевыколоколовать.

Вариант №2

Когда-то галок поп пугая,
В кустах заметил попугая,
И говорит тут попугай:
“Пугать ты галок, поп, пугай.
Но только галок, поп, пугая,
Не смей пугать ты попугая!”

Вариант №3

На мели мы налима лениво ловили,
Меняли налима вы мне на линя.
О любви не меня ли вы мило молили,
И в туманы лимана манили меня?
На речной мели мы на налима набрели.

Вариант №4

На дворе дрова, за двором дрова,
под двором дрова, над двором дрова,
дрова вдоль двора, дрова
вширь двора, не вмещает двор дров!
Наверно, выдворим дрова с вашего двора
обратно на дровяной двор.

Вариант №5

Скороговорун скороговорил скоровыговаривал,
Что всех скороговорок не перескороговоришь
не перескоровыговариваешь, но заскороговошившись, выскороговорил - что все скороговорки перескороговоришь, перескоровыговариваешь.

Задание 5. «Шифрование методом многоалфавитной замены»

Используя метод многоалфавитной замены по таблице Вижинера зашифруйте текст индивидуального варианта, используя ключ, приведенный в таблице 1.

Таблица 1

Вариант	Ключ шифрования	Вариант	Ключ шифрования
1	НЕФТЬ	14	ПТИЦА
2	УГОЛЬ	15	МИРАЖ
3	СПОРТ	16	САРАЙ
4	ЧУГУН	17	СТЕНА
5	СЕВЕР	18	СФЕРА
6	ЗАПАД	19	ВАГОН
7	ХОЛОД	20	БИЛЕТ
8	ЗАМОК	21	ЗАЧЁТ
9	ШАХТА	22	ИГРОК
10	ЛЕНТА	23	ПЛИТА
11	КУКЛА	24	ЛИНИЯ
12	ЭКРАН	25	КРЫША
13	КОШКА		

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература

1. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 c. — 978-5-238-02857-6. — Режим доступа: http://www.iprbookshop.ru/72444.html

2. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс] : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69405.html

3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89453.html (дата обращения: 21.06.2020). — Режим доступа: для авторизир. пользователей

4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

б) дополнительная литература

1.Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 c. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77320.html (дата обращения: 21.06.2020). — Режим доступа: для авторизир. пользователей

2.Гостехкомиссия России. Руководящий документ. «Защита от несанкционированного доступа к информации, термины и определения».

3.Гостехкомиссия России. Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа кинформации».

4.Гостехкомиссия России. Руководящий документ. «Средства вычислительной техники.Защита от несанкционированного доступа к информации. Показатели защищенностиот несанкционированного доступа к информации».

5.Гостехкомиссия России. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

6. Гостехкомиссия России. Руководящий документ. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты секретной информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Security Lab http://www.securitylab.ru/ - проект компании Positive Technologies. Помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.

2. Threatpost https://threatpos - новостной сайт об информационной безопасности от Kaspersky Lab. Авторитетный источник, на который ссылаются ведущие новостные агентства, такие как The New York Times и The Wall Street Journal.

3. Anti-Malware https://www.anti-malware.ru/ - информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме.

4. Geektimes https://geektimes.ru/hub/infosecurity/ - популярный хаб сайта geektimes.ru про информационную безопасность. Десятки тысяч просмотров статей, публикации о новинках индустрии и активное обсуждение в комментариях.

5. CNEWS http://safe.cnews.ru/ - раздел новостного издания о высоких технологиях CNEWS, посвященный информационной безопасности. Публикуются новости и экспертные статьи.

9. Научный журнал «Вопросы кибербезопасности» http://cyberrus.com/ - печатаются статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации.

10. Журнал “Information Security” http://www.itsec.ru/articles2/allpubliks - в журнале публикуются технические обозрения, тесты новых продуктов, а также описания комплексных интегрированных решений, внедренных на российских предприятиях и в государственных органах.

11. Клуб информационной безопасности http://wiki.informationsecurity.club/doku.php/main - клуб информационной безопасности — некоммерческая организация, развивающая ИБ и решающая задачи в этой сфере. На сайте есть «База знаний», где можно найти нормативные документы, программное обеспечение, книги, ссылки на интересные ресурсы.

12. ISO27000.RU http://www.iso27000.ru/ - это площадка для общения специалистов по ИБ. Есть тематический каталог ссылок на ресурсы по информационной безопасности и защите информации.

13. Ассоциация по вопросам защиты информации BISA http://bis-expert.ru/ - сообщество, созданное под эгидой Ассоциации Business Information Security (BISA), выпускает свой журнал, проводит вебинары, а также является организатором мероприятий.

9. Методические указания для обучающихся по освоению дисциплины

При проведений лекций, практических занятий, самостоятельной работе студентов применяются интерактивные формы проведения занятий с целью погружения студентов в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

1. Творческое задание. Выполнение творческих заданий требуют от студента воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода.

2. Групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижении лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

10. Перечень информационных технологий, используемых при

осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- программы, обеспечивающие доступ в сеть Интернет (например, «Google Chrome»);
- программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);
- программы для реализации алгоритмов шифрования/дешифрования данных (например, Microsoft Office Excel, Lazarus).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины требуются специальные материально-технические средства (компьютерный класс). Во время лекционных занятий, которые проводятся в большой аудитории, используется проектор для демонстрации слайдов, схем, таблиц и прочего материала.