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 2020 г.

Рабочая программа дисциплины

Информационная безопасность и защита персональных данных сотрудников

Направление подготовки
38.03.03 Управление персоналом

Квалификация выпускника
Бакалавр

Для всех
форм обучения

Симферополь 2020

Содержание

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

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов по дисциплине
ОПК-10	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	***Знать:*** - методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; - Трудовой кодекс РФ и иные нормативные правовые акты, содержащие нормы трудового права, процедуры приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом РФ и особенности оформления сопровождающей документации. ***Уметь:*** - решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; - использовать знание Трудового кодекса РФ и иных нормативных правовых актов, содержащих нормы трудового права, знанием процедур приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом РФ и владением навыками оформления сопровождающей документации. ***Владеть:*** - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; - знанием Трудового кодекса РФ и иных нормативных правовых актов, содержащих нормы трудового права,
ПК-10	знанием Трудового кодекса Российской Федерации и иных нормативных правовых актов, содержащих нормы трудового права, знанием процедур приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом Российской Федерации и владением навыками оформления сопровождающей документации	

		знанием процедур приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом РФ и владением навыками оформления сопровождающей документации.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.ДВ.01.01 «Информационная безопасность и защита персональных данных сотрудников» входит в вариативную часть.

Дисциплина основывается на знании следующих дисциплин: «Информационные технологии в управлении персоналом», «Профессиональные компьютерные программы», «Управление персоналом организации».

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 5 зачетных единицы (ЗЕ), 180 академических часов.

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

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 5 зачётных единицы 180 часов

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	180
Контактная работа	94
Аудиторная работа (всего):	90
Лекции	44
Семинары, практические занятия	46
Самостоятельная работа обучающихся	86
Дифференцированный зачет	4

Для заочной формы обучения

Общая трудоёмкость дисциплины составляет 5 зачётных единицы 180 часов

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	180
Контактная работа	22
Аудиторная работа (всего):	18
Лекции	10
Семинары, практические занятия	8
Самостоятельная работа обучающихся	158
Дифференцированный 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)

№ п/п	Наименование темы	Всего		Количество часов					
		ОФО	ЗФО	Контактная работа (аудиторная работа)				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
1	Информационная безопасность и безопасность информации. Основные задачи обеспечения защиты информации.	12	15	2	1	2		8	14
2	Нормативно-правовые основы информационной безопасности.	10	13,5	2	0,5	2	1	6	12
3	Организационное обеспечение информационной безопасности	12	13,5	2	0,5	4	1	6	12
4	Понятие угрозы. Виды противников или «нарушителей».	14	14	4	1	4	1	6	12
5	Защита информации.	14	14	2	1	4	1	8	12
6	Правовые обеспечения защиты персональных данных	16	13	4	1	4		8	12
7	Организационное обеспечение защиты персональных данных.	16	14	4	1	4	1	8	12
8	Методы криптографии. Средства криптографической защиты информации (СКЗИ).	14	14	4	1	4	1	6	12
9	Использование криптографических средств для решения задач идентификация и аутентификация.	14	14	4	1	4	1	6	12
10	Общее представление о структуре защищенной информационной системы.	12	13	4	1	2		6	12
11	Идентификация и аутентификация.	14	12	4		4		6	12
12	Сервисы управления доступом.	14	12	4		4		6	12
13	Защита данных и сервисов от воздействия вредоносных программ.	14	14	4	1	4	1	6	12
	Всего по дисциплине	176	176	44	10	46	8	86	158
	Дифференцированный зачет	4	4						
	Всего по дисциплине	**180**	**180**	**44**	**10**	**46**	**8**	**86**	**158**

4.2 Содержание дисциплины, структурированное по темам (разделам)

Раздел 1. Введение в безопасность информационных систем

Тема 1. Информационная безопасность и безопасность информации.

Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

Тема 2. Нормативно-правовые основы информационной безопасности.

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности.

Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.

Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.

Тема 3. Организационное обеспечение информационной безопасности.

Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования.

Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе.

Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

Раздел 2. Угрозы безопасности информационных систем и их реализация

Тема 4. Понятие угрозы. Виды противников или «нарушителей».

Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).

Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Тема 5. Защита информации.

Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

Раздел 3. Защита персональных данных.

Тема 6. Правовые обеспечения защиты персональных данных

Правовые основы защиты персональных данных. Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации предприятия по защите персональных данных. Требование к документации юридических лиц по защите персональных данных. Требования к документации по обработке персональных данных работников. Типовые документы, регламентирующие получение, обработку, хранение и передачу персональных данных. Планирование мероприятий по защите персональных данных. Угрозы безопасности персональных данных. Классификация информационных систем персональных данных (ИСПДн).

Тема 7 Организационное обеспечение защиты персональных данных.

Основы организации и обеспечения комплексной защиты персональных данных при их обработке в ИСПДн. Порядок создания и эксплуатации ИСПДн. Методы работы с постоянными сотрудниками. Административно-правовые нарушения в области связи и информации. Ответственность за нарушение требований по защите персональных данных. Система государственного надзора и контроля в области персональных данных. Проверка персонала при приеме на работу.

Раздел 4. Криптографические системы защиты информации

Тема 8. Методы криптографии. Средства криптографической защиты информации (СКЗИ).

Криптографические преобразования. Шифрование и дешифрование информации.

Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами).

Тема 9. Использование криптографических средств для решения задач идентификация и аутентификация.

Контроль за целостностью информации. Хэш-функции, принципы использования. Современные симметричные криптосистемы. Двухключевые криптографические системы хэш-функций для обеспечения целостности данных.

Раздел 5. Программно-технические средства защиты информации

Тема 10. Общее представление о структуре защищенной

информационной системы.

Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.

Тема 11. Идентификация и аутентификация.

Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.

Тема 12. Сервисы управления доступом.

Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.

Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.

Тема 13. Защита данных и сервисов от воздействия вредоносных программ.

Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.

Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

4.3. Темы практических занятий

Раздел 1. Введение в безопасность информационных систем

Тема 1. Информационная безопасность и безопасность информации.

Тема 2. Нормативно-правовые основы информационной безопасности.

Тема 3. Организационное обеспечение информационной безопасности.

Раздел 2. Угрозы безопасности информационных систем и их реализация

Тема 4. Понятие угрозы. Виды противников или «нарушителей».

Тема 5. Защита информации.

Раздел 3. Защита персональных данных.

Тема 6. Правовые обеспечения защиты персональных данных

Практическое занятие №5 Изучение ФЗ № 152-ФЗ «О персональных данных»

Практическое занятие №6 Порядок работы с персональными данными работника.

Практическое занятие №7 Планирование мероприятий по защите персональных данных.

Практическое занятие №8 Изучение методов обезличивания персональных данных.

Тема 7 Организационное обеспечение защиты персональных данных.

Практическое занятие №9 Риск-подход к моделированию угроз ИБ.

Практическое занятие №10 Подготовка объекта к аттестации. Типовые формы документов.

Практическое занятие №11 Модели угроз безопасности персональных данных при их обработке в информационных системах.

Практическое занятие №12 Типовые формы документов, предполагающие или допускающие содержание персональных данных.

Раздел 4. Криптографические системы защиты информации

Тема 8. Методы криптографии. Средства криптографической защиты информации (СКЗИ).

Тема 9. Использование криптографических средств для решения задач идентификация и аутентификация.

Раздел 5. Программно-технические средства защиты информации

Тема 10. Общее представление о структуре защищенной информационной системы.

Тема 11. Идентификация и аутентификация.

Тема 12. Сервисы управления доступом.

Тема 13. Защита данных и сервисов от воздействия вредоносных программ.

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

Раздел	Содержание заданий, выносимых на СРС	Кол-во часов ОФО	Кол-во часов ЗФО	Учебно-методическое обеспечение
1.	Информационная безопасность и безопасность информации. Основные задачи обеспечения защиты информации.	8	14	Учебно- методическое пособие
2.	Нормативно-правовые основы информационной безопасности.	6	12	Учебно- методическое пособие
3.	Организационное обеспечение информационной безопасности	6	12	Учебно- методическое пособие
4.	Понятие угрозы. Виды противников или «нарушителей».	6	12	Учебно- методическое пособие
5.	Защита информации.	8	12	Учебно- методическое пособие
6.	Правовые обеспечения защиты персональных данных	8	12	Учебно- методическое пособие
7.	Организационное обеспечение защиты персональных данных.	8	12	Учебно- методическое пособие
8.	Методы криптографии. Средства криптографической защиты информации (СКЗИ).	6	12	Учебно- методическое пособие
9.	Использование криптографических средств для решения задач идентификация и аутентификация.	6	12	Учебно- методическое пособие
10.	Общее представление о структуре защищенной информационной системы.	6	12	Учебно- методическое пособие
11.	Идентификация и аутентификация.	6	12	Учебно- методическое пособие

Раздел	Содержание заданий, выносимых на СРС	Кол-во часов ОФО	Кол-во часов ЗФО	Учебно-методическое обеспечение
12.	Сервисы управления доступом.	6	12	Учебно- методическое пособие
13.	Защита данных и сервисов от воздействия вредоносных программ.	6	12	Учебно- методическое пособие

5.1.Методические указания по организации самостоятельной работы

1. Самостоятельная (внеаудиторная) работы — важнейшая задача студента.
2. Самостоятельная работа студентов выражается в подготовке студента к практическим работам и семинарским занятиям на основании теоретического материала.
3. В качестве организационных форм занятий по дисциплине учебным планом определены лекционные, практические и семинарские занятия.
4. Практические работы направлены на обучение основам разработки нормативно-методических документов организации на основе требований стандартов. Практикум рассчитан на приобретение студентами углубленных знаний положений стандартов при организации документооборота.
5. Выполнение практических работ производится каждым студентом индивидуально.
6. Текущий контроль успеваемости предполагает оценку выполнения студентом всех видов работ, предусмотренных формами контроля знаний в соответствии с рабочей программой дисциплины.
7. К итоговому контрольному мероприятию допускаются только те студенты, которые отчитались за пропущенные занятия, т. е. выполнили и защитили все практические работы.

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

6.1 Паспорт фонда оценочных средств по дисциплине

Компетенция ОПК-10

способностью 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-комму-никационных техноло-гий и с	- решать стандартные задачи профессио-нальной деятельности на основе информационной и библиографической культуры с применением информационно-комму-никационных техноло-гий и с учетом основных требований	- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-комму-никационных технологий и с

учетом основных требований информаци-онной безопасности. 6.2.1 (1-50)	информа-ционной безопасности. 6.2.2 (1-22) 6.2.3 (1-20)	учетом основных требований информаци-онной безопасности. 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-50) Умеет, если выполнил 6.2.2 (1-22), 6.2.3 (1-20) Владеет, если выполнил 6.2.4 (1-5)		

Компетенция ПК-10

знанием Трудового кодекса Российской Федерации и иных нормативных правовых актов, содержащих нормы трудового права, знанием процедур приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом Российской Федерации и владением навыками оформления сопровождающей документации		
Этапы формирования компетенции		
Знает	Умеет	Владеет
- Трудовой кодекс Российской Федерации и иные нормативные правовые акты, содер-жащие нормы трудового права, процедуры приема, увольнения, перевода на другую работу и перемещения персонала в соответ-ствии с Трудовым кодексом Российской Федерации и особенно-сти оформления сопро-вождающей документа-ции. 6.2.1 (1-50)	использовать знание Трудового кодекса Российской Федерации и иных нормативных правовых актов, содержащих нормы трудового права, знани-ем процедур приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом Российской Федерации и владением навыками оформления сопровожда-ющей документации 6.2.2 (1-22) 6.2.3 (1-20)	- знанием Трудового кодекса Российской Федерации и иных нормативных правовых актов, содержащих нормы трудового права, знанием процедур приема, увольнения, перевода на другую работу и перемещения персонала в соответствии с Трудовым кодексом Российской Федерации и владением навыками оформления сопровождающей документации. 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-50) Умеет, если выполнил 6.2.2 (1-22), 6.2.3 (1-20) Владеет, если выполнил 6.2.4 (1-5)		

6.2 Типовые контрольные задания или иные материалы

6.2.1. Дифференцированный зачёт

а) типовые вопросы:

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
2. Распространение объектно-ориентированного подхода на информационную безопасность.
3. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз. Защита информации от случайных угроз.

4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы в РФ.
5. Законодательный уровень информационной безопасности. Обзор зарубежного законодательства в области ИБ.
6. Назначение и задачи в сфере обеспечения информационной безопасности.
7. Международные стандарты информационного обмена. Стандарт ISO/IEC15408.
8. Российские стандарты защищенности автоматизированных систем.
9. Основные положения теории информационной безопасности. Модели безопасности и их применение.
10. Информационная безопасность в условиях функционирования в России глобальных сетей.
11. Виды противников или "нарушителей".
12. Классификация компьютерных вирусов. Методы и средства борьбы с вирусами. Виды возможных нарушений информационной системы. Виды защиты.
13. Шпионское ПО. Рекламное ПО.
14. Система охраны объектов компьютерных систем.
15. Организация работы с конфиденциальными информационными ресурсами.
16. Защита от злоумышленных действий обслуживающего персонала и пользователей. Защита от несанкционированного копирования программного обеспечения.
17. Средства защиты компьютеров. Программно аппаратные методы и средства ограничения доступа к компонентам компьютера.
18. Типы несанкционированного доступа и условия работы средств защиты.
19. Методы криптографии.
20. Основные понятия шифрования. Стандарты шифрования.
21. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом.
22. Методы и средства хранения ключевой информации. Анализ программных реализаций.
23. Защита от разрушающих программных воздействий.
24. Основные технологии построения защищенных ЭИС.
25. Системные вопросы защиты программ и данных.
26. Защита вычислительной сети. Классификация вторжений.
27. Системы архивирования и дублирования информации.
28. Защита информации в операционных системах. Защита информации в прикладном ПО.
29. Проблема защиты информации в распределенных сетях.
30. Межсетевой экран. Классификация межсетевых экранов. Брандмауеры. Основные понятия.

6.2.2. Темы рефератов.

1. Этапы и общие принципы разработки защищенных информационных систем.

2. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений.
3. Сценарии последовательности действий нарушителя системы защиты информации. Пример построения сценария действий нарушителя с использованием графов.
4. Международные стандарты в области защиты информационных систем.
5. Цели, задачи и стадии проведения аудита информационной безопасности.
6. Оценка ущерба от нарушений информационной безопасности на различных этапах жизненного цикла объекта информатизации.
7. Методы оценки рисков информационной безопасности.
8. Шкалы оценки ущерба при нарушении информационной безопасности на объекте оценки.
9. Управление рисками. Модель безопасности с полным перекрытием.
10. Концепция управление рисками согласно ISO-15408.
11. Lifecycle Security – обобщенная схема построения комплексной защиты компьютерной сети предприятия.
12. Методика управления рисками, предлагаемая Microsoft (MSAT).
13. Обзор современных программных продуктов для оценки рисков.
14. Особенности моделирования сложных организационно-технических систем.
15. Моделирование процесса защиты информации в информационной системе с использованием графовых структур.
16. Пример использования графов для расчета защищенности от физического проникновения.
17. Генерирование множества альтернатив с применением экспертных методов при построении защищенной системы обработки информации.
18. Модель процесса защиты информации в виде трёхдольного графа.
19. Оценка альтернативных проектов организации системы защиты информации с использованием критериального метода.
20. Оценка альтернативных проектов организации системы защиты информации с использованием метода парных сравнений.
21. Информационные технологии, используемые в системах поддержки управленческих решений в области построения защищенных систем обработки информации.
22. Перспективные направления в организации и управлении системой защиты информации на предприятии.

6.2.3. Примерные варианты контрольных работ

Вариант 1.

1. Методы оценки рисков информационной безопасности на предприятии.
2. Генерирование множества альтернатив с применением экспертных методов при разработке СЗИ.
3. Основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.

Вариант 2.

1. Этапы построения защищенных систем обработки информации.

2. “Куб безопасности” в координатах ОСНОВА, НАПРАВЛЕНИЯ, ЭТАПЫ. Обработка трехмерных матриц для оценки эффективности СЗИ.

3. Пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.

Вариант 3.

1. Управление рисками. Модель безопасности с полным перекрытием.

2. Модель элементарной защиты объекта информатизации. Пример расчета прочности защиты.

3. Парное сравнение альтернатив (метод парных сравнений).

Вариант 4.

1. Пример использования сетей Петри для построения сценария действий нарушителя и сигнатур атак.

2. Оценка альтернативных проектов организации СЗИ с использованием критериального метода.

3. Обзор современных программных продуктов для оценки рисков.

Вариант 5.

1. Модель многозвенной защиты объекта информатизации. Пример расчета прочности защиты.

2. Альтернативы и критерии. Требования к набору критериев. Оценка важности критериев.

3. Пример исследования эффективности СЗИ с использованием морфологической матрицы.

6.2.4. Типовые вопросы теста

1) Хранение паролей может осуществляться

А. в виде сверток
Б. в открытом виде
В. в закрытом виде
Г. в зашифрованном виде
Д. все варианты ответа верны

2) К системам оповещения относятся:

А. инфракрасные датчики
Б. электрические датчики
В. электромеханические датчики
Г. электрохимические датчики

3) Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?

А. информационный саботаж
Б. физический саботаж
В. информационные инфекции

4) Что не относится к информационной инфекции:

А. троянский конь
Б. фальсификация данных
В. черви
Г. вирусы
Д. логическая бомба

5) Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

А. защита информации от непреднамеренного воздействия
Б. защита информации от несанкционированного воздействия
В. защита информации от несанкционированного доступа
Г. защита от утечки информации

6) Исследование возможности дешифрования информации без знания ключей:

А. криптология
Б. криптоанализ
В. взлом
Г. несанкционированный доступ

7) Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

А. служебная информация
Б. коммерческая тайна
В. банковская тайна
Г. конфиденциальная информация

8) Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

А. комплексное обеспечение информационной безопасности
Б. безопасность ас
В. угроза информационной безопасности
Г. атака на автоматизированную систему
Д. политика безопасности

9) Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

А. защита информации
Б. компьютерная безопасность
В. защищенность информации
Г. защищенность потребителей информации

10) Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:

А. принцип системности
Б. принцип комплексности
В. принцип непрерывной защиты
Г. принцип разумной достаточности
Д. принцип гибкости системы

11) Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

А. комплексное обеспечение информационной безопасности
Б. безопасность ас
В. угрозы информационной безопасности
Г. атака на автоматизированную систему

Д. политика безопасности

12) К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»

А. информация без ограничения права доступа

Б. информация с ограниченным доступом

В. информация, распространение которой наносит вред интересам общества

Г. объект интеллектуальной собственности

Д. иная общедоступная информация

13) Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.

А. государственная тайна

Б. коммерческая тайна

В. банковская тайна

Г. конфиденциальная информация

14) Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:

А. надежность

Б. точность

В. контролируемость

Г. устойчивость

Д. доступность

15) Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:

А. принцип системности

Б. принцип комплексности

В. принцип непрерывной защиты

Г. принцип разумной достаточности

Д. принцип гибкости системы

16) Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:

А. комплексное обеспечение информационной безопасности

Б. безопасность АС

В. угроза информационной безопасности

Г. атака на автоматизированную систему

Д. политика безопасности

17) К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики, сведения о семейном положении, сведения об имущественном или финансовом состоянии…»

А. информация без ограничения права доступа

Б. информация с ограниченным доступом

В. информация, распространение которой наносит вред интересам общества

Г. объект интеллектуальной собственности
Д. иная общедоступная информация

18) Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:

А. комплексное обеспечение информационной безопасности
Б. безопасность ас
В. угроза безопасности
Г. атака на автоматизированную систему
Д. политика безопасности

19) Соотнесите основные виды угроз для АС:

1. Угроза нарушения конфиденциальности 2. Угроза отказа служб 3. Угроза нарушения целостности	А. Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую Б. Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС В. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней

20) Соотнесите классификацию угроз по ряду признаков:

1. по природе возникновения 2. по непосредственному источнику 3. по степени воздействия на АС 4. по способу доступа к ресурсам АС	А. Пассивные и активные Б. Направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС В. Естественные или искусственные Г. Природная среда, человек, санкционированные программные средства и несанкционированные программные средства

21. 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

22. 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

23. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

24. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

25. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

26. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

27. 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

28.Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

29.Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

30.Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

Ключ к тесту

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.
А,Б,Г	А,Б	А,Б	Б	Г	Б	Г	Г	А	З	З	З	А	Г	Б	Б	Б	А	1-В; 2-Б; 3-А	1-В; 2-Г; 3-В;4-А

21.	22.	23.	24.	25.	26.	27.	28.	29.	30.
А	А	А Б	А Б В	А	АБВ	А	А	АБ	АВ

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

а) основная учебная литература:

1. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс] / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — 978-5-4487-0147-4. — Режим доступа: http://www.iprbookshop.ru/72341.html

2. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: http://www.iprbookshop.ru/15845.— ЭБС «IPRbooks», по паролю

3. Бубнов А. А. Основы информационной безопасности (2-е изд., стер.) учеб. пособие / А. А. Бубнов, В. Н. Пржегорлинский, О. А.Савинкин – М.: Академия, 2016. – 256 с.

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/22424.— ЭБС «IPRbooks», по паролю

б) дополнительная литература

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю

2. Кожуханов Н.М. Правовые основы информационной безопасности [Электронный ресурс] : учебное пособие / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. текстовые данные. — М.: Российская таможенная академия, 2013. — 88 с.— Режим доступа:http://www.iprbookshop.ru/69749.html

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

1. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации Федеральной службы по техническому и экспортному контролю РФ: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty

2. The logic behind CRAMM’s assessment of measures of risk and determination of appropriate countermeasures. URL: http://www.cramm.com/downloads/techpapers.htm

3. RiskWatch users manual. URL: http://www.riskwatch.com

9. Методические указания для обучающихся по освоениюдисциплины

При проведении 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, анализа информационных рисков (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.