Рабочая программа дисциплины (модуля) «Защита информации», включая оценочные материалы

1. Требования к результатам обучения по дисциплине (модулю)

1.1. Перечень компетенций, формируемых дисциплиной (модулем) в процессе освоения образовательной программы

Группа компетенций	Категория компетенций	Коды и содержание компетенций
Универсальные	-	-
Общепрофессиональные	-	-
Профессиональные	-	ПК-2. Способен применять системный подход и математические методы в формализации решения прикладных задач, моделировать прикладные (бизнес) процессы и предметную область автоматизации организации
	-	ПК-3 Способен эксплуатировать и сопровождать информационные системы и сервисы, осуществлять ведение информационных хранилищ для решения прикладных задач профессиональной деятельности

1.2. Компетенции и индикаторы их достижения, формируемых дисциплиной (модулем) в процессе освоения образовательной программы

Код компетенции	Код индикатора компетенции	Содержание индикатора компетенции
ПК-2	ПК-2.2	Осуществляет исследование объекта на предмет его автоматизации, выявляет информационные потребности пользователей и угрозы информационной безопасности
ПК-3	ПК-3.3	Применяет на практике функциональные и технологические стандарты ИС, работы с технологиями сбора, накопления, обработки, передачи и распространения информации

1.3. Результаты обучения по дисциплине (модулю)

Цель изучения дисциплины (модуля) – обзор современных проблем в сфере информационной безопасности в информационных системах, направлений развития программы информационной безопасности России и формирование практических навыков указанной сфере.

В результате изучения дисциплины (модуля) обучающийся должен

знать:

- математические методы и алгоритмы используемые в разработке программного обеспечения для информационной безопасности компьютерных систем; виды контента информационных ресурсов предприятия и Интернет-ресурсов; основы безопасности жизнедеятельности в области профессиональной деятельности; базовые понятия и определения, используемые в сфере информационной безопасности; основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам

уметь:

- применять на практике собственные и классические алгоритмы криптографической защиты данных; ставить и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным); проектировать, внедрять и организации эксплуатацию ИС и ИКТ; моделировать, анализировать и совершенствовать бизнес-процессы разрабатывать конкретные предложения по результатам исследований, готовить справочно-аналитические материалы для принятия управленческих решений;

владеть:

- навыками работы с алгоритмами криптографической защиты данных; методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия; основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; иметь представление о моделях безопасности ИС.

2. Объем, структура и содержание дисциплины (модуля)

2.1. Объем дисциплины (модуля)

Виды учебной работы	*Формы обучения*	*Формы обучения*	*Формы обучения*
	Очная	*Очно-заочная*	*Заочная*
Общая трудоемкость: зачетные единицы/часы	4/144	4/144	4/144
Контактная работа:	64	42	12
Занятия лекционного типа	32	14	6
Занятия семинарского типа	32	28	6
Консультации	0	0	0
Промежуточная аттестация: экзамен	36	27	9
Самостоятельная работа (СР)	44	75	123

2.2. Темы (разделы) дисциплины (модуля) с указанием отведенного на них количества часов по формам образовательной деятельности

Очная форма обучения

№ п/п	Наименование тем (разделов)	Виды учебной работы (в часах)						
		Контактная работа						СР
		Занятия лекционного типа		Занятия семинарского типа				
		Л	Иные	ПЗ	С	ЛР	Иные	
1.	Понятие информационной безопасности	2	0	2	0	0	0	3
2.	Законодательный уровень информационной безопасности	2	0	2	0	0	0	3
3.	Наиболее распространенные угрозы информационной безопасности	4	0	4	0	0	0	4
4.	Распространение объектно-ориентированного подхода на ИБ	2	0	2	0	0	0	3

5.	Административный уровень информационной безопасности	2	0	2	0	0	0	4
6.	Процедурный уровень информационной безопасности	2	0	2	0	0	0	4
7.	Основные программно-технические меры безопасности информации	2	0	2	0	0	0	3
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности	4	0	4	0	0	0	4
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	4	0	4	0	0	0	4
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	2	0	2	0	0	0	3
11.	Криптография: шифрование и обеспечение целостности	2	0	2	0	0	0	3
12.	Протоколирование и аудит, шифрование, контроль целостности	2	0	2	0	0	0	3
13.	Антивирусная защита компьютерных систем	2	0	2	0	0	0	3

Очно-заочная форма обучения

		Виды учебной работы (в часах)

№ п/п	Наименование тем (разделов)	Контактная работа						СР
		Занятия лекционного типа		Занятия семинарского типа				
		Л	Иные	ПЗ	С	ЛР	Иные	
1.	Понятие информационной безопасности	1	0	2	0	0	0	5
2.	Законодательный уровень информационной безопасности	1	0	2	0	0	0	5
3.	Наиболее распространенные угрозы информационной безопасности	1	0	2	0	0	0	5
4.	Распространение объектно-ориентированного подхода на ИБ	1	0	2	0	0	0	5
5.	Административный уровень информационной безопасности	1	0	2	0	0	0	5
6.	Процедурный уровень информационной безопасности	1	0	2	0	0	0	5
7.	Основные программно-технические меры безопасности информации	1	0	2	0	0	0	5
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности	1	0	2	0	0	0	7
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	2	0	2	0	0	0	7
10.	Основные программно-	1	0	2	0	0	0	7

	технические меры безопасности информации: Экранирование, Анализ защищенности							
11.	Криптография: шифрование и обеспечение целостности	1	0	2	0	0	0	7
12.	Протоколирование и аудит, шифрование, контроль целостности	1	0	2	0	0	0	7
13.	Антивирусная защита компьютерных систем	1	0	4	0	0	0	5

Заочная форма обучения

№ п/п	Наименование тем (разделов)	Виды учебной работы (в часах)						
		Контактная работа						СР
		Занятия лекционного типа		Занятия семинарского типа				
		Л	Иные	ПЗ	С	ЛР	Иные	
1.	Понятие информационной безопасности	0,5	0	0	0	0	0	10
2.	Законодательный уровень информационной безопасности	0,5	0	0	0	0	0	9
3.	Наиболее распространенные угрозы информационной безопасности	1	0	0	0	0	0	9
4.	Распространение объектно-ориентированного подхода на ИБ	1	0	0	0	0	0	9
5.	Административный уровень информационной безопасности	1	0	0	0	0	0	9
6.	Процедурный уровень информационной безопасности	1	0	0	0	0	0	9
7.	Основные программно-технические меры безопасности информации	1	0	0	0	0	0	9
8.	Основные программно-	0	0	1	0	0	0	10

	технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности							
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	0	0	1	0	0	0	10
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	0	0	1	0	0	0	10
11.	Криптография: шифрование и обеспечение целостности	0	0	1	0	0	0	10
12.	Протоколирование и аудит, шифрование, контроль целостности	0	0	1	0	0	0	10
13.	Антивирусная защита компьютерных систем	0	0	1	0	0	0	9

Примечания:

Л – лекции, ПЗ – практические занятия, С – семинары, ЛР – лабораторные работы, СР – самостоятельная работа.

2.3. Содержание дисциплины (модуля), структурированное по темам (разделам) и видам работ

Содержание лекционного курса

№ п/п	Наименование тем (разделов)	Содержание лекционного курса
1.	Понятие информационной безопасности	Базовые понятия и определения, используемые в сфере информационной безопасности.
2.	Законодательный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем. Разработка макетов справочно-аналитических материалов для принятия управленческих решений на основе законодательного уровня ИБ.

3.	Наиболее распространенные угрозы информационной безопасности	Разновидности угроз информационной безопасности. Классификация уязвимости систем безопасности. Объективные уязвимости. Случайные уязвимости. Классификация угроз. Пиратское программное обеспечение. Человеческий фактор. Компьютерные вирусы. Инсайдерские утечки. Физические средства защиты. Услуга защиты от DDoS-атак.
4.	Распространение объектно-ориентированного подхода на ИБ	Основные понятия объектно-ориентированного подхода. О необходимости объектно-ориентированного подхода к информационной безопасности.
5.	Административный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на административном уровне ИБ. Обзор справочно-аналитических материалов для принятия управленческих решений на административном уровне.
6.	Процедурный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне.
7.	Основные программно-технические меры безопасности информации	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам. Постановка и решение схемотехнических задач, связанных с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным).
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности	Основные программно-технические меры безопасности информации. Идентификация и аутентификация. Управление доступом. Экранирование. Анализ защищенности. Обеспечение отказоустойчивости. Обеспечение безопасного восстановления. Туннелирование.
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	Основные понятия. Описывается протоколирование и аудит, а также криптографические методы защиты. Место мер безопасности в общей архитектуре безопасности.
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	Основные понятия программно-технического уровня информационной безопасности.
11.	Криптография: шифрование и обеспечение целостности	Цель криптографической защиты. Классы криптографической защиты информации. Симметричная и ассиметричная криптография. Хеш – функции. Собственные и классические алгоритмы криптографической защиты данных.
12.	Протоколирование и аудит, шифрование, контроль целостности	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам в рамках реализации процедур протоколирования и аудита, контроля целостности (в т.ч. с использованием элементов шифрования).
13.	Антивирусная защита компьютерных систем	Принципы организации антивирусной защиты информационных систем.

Содержание занятий семинарского типа

№ п/п	Наименование тем (разделов)	Тип	Содержание занятий семинарского типа
1.	Понятие информационной безопасности	ПЗ	Роль справочно-аналитических материалов в принятии управленческих решений. Представление о моделях безопасности ИС.

2.	Законодательный уровень информационной безопасности	ПЗ	Преступления против безопасности компьютерной информации. Информационная безопасность как объект правового регулирования. Понятие преступлений против информационной безопасности и их система. Виды преступлений против информационной безопасности. Методы и средства обеспечения информационной безопасности компьютерных систем.
3.	Наиболее распространенные угрозы информационной безопасности	ПЗ	Основные виды угроз информационной безопасности. Пиратское программное обеспечение. Человеческий фактор. Компьютерные вирусы. Инсайдерские утечки. Средства защиты. Резервное копирование Физические средства защиты. Услуга защиты от DDoS-атак.
4.	Распространение объектно-ориентированного подхода на ИБ	ПЗ	Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
5.	Административный уровень информационной безопасности	ПЗ	Обеспечение информационной безопасности компьютерных систем на административном уровне
6.	Процедурный уровень информационной безопасности	ПЗ	Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне
7.	Основные программно-технические меры безопасности информации	ПЗ	Классификация средств защиты информации. Средства защиты от несанкционированного доступа (НСД). Средства авторизации. Мандатное управление доступа. Управление доступом на основе ролей. Системы анализа и моделирования информационных потоков (CASE-системы). Системы мониторинга сетей: Системы обнаружения и предотвращения вторжений (IDS/IPS). Антивирусные средства. Организационная защита объектов информатизации.
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности	ПЗ	Принципы реализации и использования алгоритмов идентификации и аутентификации, управления доступом и процедур анализа защищенности.
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	ПЗ	Методы шифрования. Криптографического контроля целостности. Цифровые сертификаты.
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	ПЗ	Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.
11.	Криптография: шифрование и обеспечение целостности	ПЗ	Методы проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия с использованием криптографических систем защиты.
12.	Протоколирование и аудит, шифрование, контроль целостности	ПЗ	Основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам в рамках реализации процедур протоколирования и аудита, контроля целостности (в т.ч. с использованием элементов шифрования).
13.	Антивирусная защита компьютерных систем	ПЗ	Типология вирусов. Достоинства и недостатки эвристических алгоритмов поиска вирусов.

Содержание самостоятельной работы

№ п/п	Наименование тем (разделов)	Содержание самостоятельной работы
1.	Понятие информационной безопасности	Представление о моделях безопасности ИС.
2.	Законодательный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем.
3.	Наиболее распространенные угрозы информационной безопасности	Основные виды угроз информационной безопасности. Средства защиты. Физические средства защиты.
4.	Распространение объектно-ориентированного подхода на ИБ	Основные понятия объектно-ориентированного подхода.
5.	Административный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на административном уровне ИБ.
6.	Процедурный уровень информационной безопасности	Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне.
7.	Основные программно-технические меры безопасности информации	Знакомство с методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия.
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности	Принципы реализации и использования алгоритмов идентификации и аутентификации, управления доступом и процедур анализа защищенности.
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	Цифровые сертификаты.
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	Архитектурная безопасность.
11.	Криптография: шифрование и обеспечение целостности	Основные угрозы безопасности информации и возможные способы их реализации, методы и средства противодействия этим угрозам.
12.	Протоколирование и аудит, шифрование, контроль целостности	Использование элементов шифрования
13.	Антивирусная защита компьютерных систем	Достоинства и недостатки эвристических алгоритмов поиска вирусов.

3. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

По дисциплине (модулю) предусмотрены следующие виды контроля качества освоения:

- текущий контроль успеваемости;
- промежуточная аттестация обучающихся по дисциплине (модулю).

3.1. Оценочные материалы для проведения текущей аттестации по дисциплине (модулю)

№ п/п	Контролируемые темы (разделы)	Наименование оценочного средства
1.	Понятие информационной безопасности	Устный опрос. Дискуссионные

		процедуры
2.	Законодательный уровень информационной безопасности	Устный опрос. Дискуссионные процедуры
3.	Наиболее распространенные угрозы информационной безопасности	Устный опрос. Практическое задание
4.	Распространение объектно-ориентированного подхода на ИБ	Устный опрос. Дискуссионные процедуры
5.	Административный уровень информационной безопасности	Устный опрос. Кейсы
6.	Процедурный уровень информационной безопасности	Устный опрос. Дискуссионные процедуры
7.	Основные программно-технические меры безопасности информации	Устный опрос. Кейс
8.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом Анализ защищенности	Устный опрос. Практическое задание
9.	Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	Устный опрос. Исследовательский проект (реферат)
10.	Основные программно-технические меры безопасности информации: Экранирование, Анализ защищенности	Устный опрос. Практические задания
11.	Криптография: шифрование и обеспечение целостности	Устный опрос. Практическое задание
12.	Протоколирование и аудит, шифрование, контроль целостности	Устный опрос. Практическое задание
13.	Антивирусная защита компьютерных систем	Устный опрос. Практические задания

3.1.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе текущего контроля успеваемости

Устный опрос

Тема 1. Понятие информационной безопасности

Вопросы для устного опроса:

1.Что такое информационная безопасность?

2. Что является основными составляющими информационной безопасности?

3. Какие цели и задачи имеет информационная безопасность?

4. В чем заключается важность и сложность проблемы информационной безопасности?

Вопросы для дискуссий:

1. Информация как объект защиты

2. Основные направления информационной безопасности

3. Информация как коммерческая тайна

Тема 2. Законодательный уровень информационной безопасности

Вопросы для устного опроса:

1. Что такое законодательный уровень информационной безопасности и почему он важен

2. Обзор российского законодательства в области информационной безопасности

3. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

4. Другие законы и нормативные акты РФ

5. Обзор зарубежного законодательства в области информационной безопасности

6. О текущем состоянии российского законодательства в области информационной безопасности

Вопросы для дискуссий:

1. Неправомерный доступ к компьютерной информации.
2. Создание, использование и распространение вредоносных компьютерных программ.
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
4. Неправомерное воздействие на критическую информационную инфраструктуру организации
5. Методы и средства обеспечения информационной безопасности компьютерных систем.
6. Защита персональных данных

Тема 3. Наиболее распространенные угрозы информационной безопасности

Вопросы для устного опроса:

1. Основные определения и критерии классификации угроз ;
2. Наиболее распространенные угрозы доступности ;
2.1 Примеры угроз доступности;
2.2 Программные атаки на доступность;
3. Вредоносное программное обеспечение;
4. Основные угрозы целостности ;
5. Основные угрозы конфиденциальности

Практическое задание:

Практическое задание «Модель угроз информационной безопасности информационно-вычислительной системы»

Цель работы: Определение актуальных угроз информационной безопасности (ИБ) для информационно-вычислительной системы (ИВС), формирование защитных мер.

При выполнении практического задания в качестве ИВС может быть как информационная система организации, так и домашняя локальная вычислительная сеть.

В состав ИВС входит: ПО, технические средства обработки, хранения и передачи информации, информационные активы

При выполнении практического задания формируется отчет в котором содержится следующая информация:

Описание информационной системы:

– состав технических средств;
– перечень прикладного ПО;
– перечень средств защиты информации;
– конфиденциальная информация, хранимая и обрабатываемая в ИВС;
– количество пользователей в системе, наличие административных и пользовательских прав у пользователей;
– настройки безопасности ОС и средств защиты (в том числе настройки службы каталогов, парольная политика).
– использование резервного копирования;
– наличие доступа к сети интернет (провайдер, соглашение о предоставлении услуг, технология доступа).
– наличие персональных данных
– наличие инструкций и организационно-распорядительной документации по обеспечению ИБ

Отчет по практическому заданию содержит:

1. Таблицу с источником угроз и защитных мер для каждой актуальной угрозы ИВС

Пример таблицы:

№ п/п	Категория защитных мер	Состав защитных мер
	Организация информационной безопасности	
1	Внутренняя организация	1. Координация вопросов обеспечения ИБ. 2. Распределение обязанностей по обеспечению ИБ. 3. Получение разрешений на использование средств обработки информации. 4. Заключение соглашений о конфиденциальности. 5. Проведение внешнего аудита ИБ
2	Обеспечение безопасности при доступе сторонних организаций	1. Определение рисков, связанных со сторонними организациями. 2. Соблюдение мер безопасности при работе с клиентами. 3. Соблюдение мер безопасности в соглашениях со сторонними организациями

2. Таблицу с перечнем требуемых защитных мер для ИВС

Пример таблицы:

№ п/п	Актуальные угрозы для ИВС	Категория угрозы	Объекты воздействия угрозы	Источник угрозы	Категория требуемых защитных мер (в соответствии с первой таблицей)	Требуемые защитные меры
1	Несанкционированное физическое проникновение	Взлом	сетевое оборудование, компьютеры	внешний	Безопасность оборудования	Размещение и защита оборудования

Тема 4. Распространение объектно-ориентированного подхода на ИБ

Вопросы для устного опроса:

1. Что означает "распространение объектно-ориентированного подхода на информационную безопасность"
2. В чём проявляется "распространение объектно-ориентированного подхода на информационную безопасность"
3. Какие преимущества и недостатки имеет "распространение объектно-ориентированного подхода на информационную безопасность"

Вопросы для дискуссии:

1. Использование объектно-ориентированного подхода в информационной безопасности
2. Концепции объектно-ориентированного подхода

Тема 5. Административный уровень информационной безопасности

Вопросы для устного опроса:

1. Административный уровень информационной безопасности:
Основные понятия
2. Политика безопасности
3. Программа безопасности
4. Синхронизация программы безопасности с жизненным циклом систем

Кейсы.

Кейс 1.

Описание ситуации В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании программный продукт и передал его конкурентам, которые выпустили программу на рынок под своим товарным знаком.

Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено.

Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте.

Задания.

1. Определите возможные причины инцидента и степень ответственности сотрудника.
2. Определите меры, направленные на предотвращение повторных инцидентов.
3. Подготовьте проекты соответствующих документов.

Кейс 2.

Описание ситуации В одной из компаний сотрудник хранил на мобильном компьютере конфиденциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден.

Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам.

Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе.

Задания.

1. Определите возможные причины инцидента и степень ответственности сотрудника.
2. Определите меры, направленные на предотвращение повторных инцидентов.
3. Подготовьте проекты соответствующих документов.

Тема 6. Процедурный уровень информационной безопасности

Вопросы для устного опроса:

1. В чем заключается и для чего предназначен "процедурный уровень информационной безопасности"?
2. Основные меры процедурного уровня информационной безопасности

Вопросы для дискуссии:

1. Каковы цели и особенности реализации указанного класса мер процедурного уровня ИБ?

а. Управление персоналом
б. Физическая защита
в. Поддержание работоспособности
г. Реагирование на нарушения режима безопасности
д. Планирование восстановительных работ

Тема 7. Основные программно-технические меры безопасности информации

Вопросы для устного опроса:

1. В чем заключается и для чего предназначен "программно-технический уровень информационной безопасности"?
2. Почему средства по обеспечению безопасности в информационных системах называются "сервисами"? Что такое "полный набор сервисов ИБ" и как можно классифицировать

сервисы в нем?

Кейс:

Прототип «Командного процессора» с элементами защиты

Цель работы: реализовать в «командном процессоре» защиту на уровне пользователя с применением метода паролей или его модификаций; реализовать процедуру управления системой защиты на уровне пользователя.

Структура командного процессора (блок «защита на уровне пользователя»).

Субъекты: Суперпользователь/администратор, другие пользователи.

Объекты: база учетных записей пользователей.

Минимальный набор команд:

изменение своего пароля,добавление нового пользователя, удаление пользователя, изменение учетной записи пользователя (изменение логина, дополнительных полей учетной записи (если они есть)), просмотр информации о текущем пользователе, просмотр разрешенной информации о существующих в системе пользователях, несколько нейтральных команд (дата, время, список доступных команд системы и т.п.).

Минимальная функциональность:

пароль не должен быть виден на экране, в системе всегда присутствует хотя бы один суперпользователь, обыкновенный пользователь ограничен в действиях, создаёт новых пользователей (удаляет существующих) только суперпользователь, суперпользователь может изменять пароли всех пользователей, при изменении/добавлении пароля запрашивается его подтверждение, имена пользователей в системе попарно различны (не повторяются), возможность зайти под другим пользователем, не закрывая приложение, работать в системе может только пользователь, успешно прошедший процедуру аутентификации.

Тема 8. Основные программно-технические меры безопасности информации: идентификация и аутентификация, управление доступом. Анализ защищенности

Вопросы для устного опроса:

1. Какие особенности современных информационных систем являются существенными с точки зрения организации информационной безопасности на программно-техническом уровне?
2. Что означает и какое место в обеспечении информационной безопасности занимает архитектурная безопасность?

Практическое задание:

Цель - получение сведений об уровне (состоянии) защищенности инфраструктуры от реализации недопустимых событий, а также выработка маршрутной карты по модернизации информационной инфраструктуры (на примере, который предложит преподаватель).

Необходимо решить следующие задачи:

– описать возможные стратегические риски информационной безопасности;

– описать возможные уязвимости информационной инфраструктуры, которые могут быть использованы внешними и внутренними нарушителями;

– выявление недостатков применяемых средств защиты информации и программных обеспечений, а также оценка возможности их использования нарушителем;

– разработка маршрутной карты по модернизации информационной инфраструктуры

Тема 9. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись

Вопросы для устного опроса:

1. Для чего предназначена и какую роль в ИБ играют протоколирование, аудит, шифрование, контроль защищенности и цифровая подпись?
2. Какие существуют способы реализации протоколирования, аудита, шифрования, контроля защищенности и цифровой подписи и в чем их особенности?
3. Почему пара сервисов обычно рассматривается совместно друг с другом?

а. пара сервисов "протоколирование" и "аудит";

б. пара сервисов "шифрование" и "контроль целостности".

4. Что такое, как реализуется и где используется "электронная цифровая подпись"?

Исслеловательский проект (реферат)

1. Алгоритмы цифровой подписи
2. Протоколирование и аудит
3. Шифрование, контроль целостности

Тема 10. Основные программно-технические меры безопасности информации. Экранирование. Анализ защищенности

Вопросы для устного опроса:

1. Для чего предназначена и какую роль в ИБ играют экранирование и анализ защащенности?
2. Как и с какими угрозами ИБ позволяют бороться сервис X ?

а. Экранирование;

б. Анализ защищенности.

Практическое задание:

Практические задания

1. Разработать интерфейс пользователя «Сервис безопасности экранирование».
2. Разработать интерфейс пользователя «Сервис безопасности анализ защищенности».

Тема 11. Криптография: шифрование и обеспечение целостности

Вопросы для устного опроса:

1. Что такое криптография?
2. Что такое алгоритм шифрования?
3. Как с помощью шифрования защищаются данные?
4. Какой алгоритм шифрования самый стойкий?
5. Что такое ключ шифрования?

Практическое задание:

1. Криптографические алгоритмы

Цель работы: освоение практических приемов криптографического преобразования информации.

Особенности реализации:

Шифрование. В большинстве случаев необходимо указывать, что шифровать и ключ шифрования.

Расшифрование. Необходимо указывать, что расшифровать и соответствующий ключ.

Пример возможного алгоритма «Перестановка по матрице»:

0. Ограничения: S=2 – мин размер матрицы, I=7 – макс размер матрицы, E=’*’-символы для дополнения;
1. Исходный текст – P, длина текста N символов;
2. Если N-1 больше S то переход к п.10;
3. Если N-1 меньше I, то K=I Иначе K=N-1;
4. Используемый ключ: матрица перестановок R (KxK);

5. Выделить очередной блок исходного текста размером K*K;
6. Если блок полностью пустой, то переход к п.11;
7. Если блок не полный, то дополнить символами E;
8. Осуществить перестановку в блоке, согласно матрице R;
9. Переход к п.5;
10. Ошибка: размер сообщения слишком мал;
11. Конец.

Тема 12. Протоколирование и аудит, шифрование, контроль целостности

Вопросы для устного опроса:

1. Протоколирование и аудит
2. Активный аудит
3. Шифрование
4. Контроль целостности

Практическое задание:

Стеганография

Тема: Исследование метода компьютерной стеганографии для защиты информации.

Цель работы: освоить практические приемы стеганографического преобразования информации.

Задача: создать приложение, выполняющее две функции: функцию скрытия исходного текста в контейнере стеганографическим методом и функцию извлечения текста из контейнера.

Тема 13. Антивирусная защита компьютерных систем

Вопросы для устного опроса:

1. Антивирусная защита компьютерных систем
2. Вирусы и средства борьбы с ними
3. Основы информационной безопасности при работе на компьютере
4. Инфраструктуры открытых ключей

Практические задания:

Задание 1. Тестирование флешки на наличие компьютерного вируса.

Вставьте флешку в компьютер.

Запустите имеющуюся у вас антивирусную программу.

Задайте область проверки — режим проверки — лечение зараженных файлов и нажмите кнопку Проверить.

Обратите внимание на индикатор процесса сканирования. Если антивирусная программа обнаружила вирусы и произвела лечение файлов (что видно в отчете о сканировании), запустите процесс сканирования дискеты еще раз и убедитесь, что все вирусы удалены.

Составьте отчет о проделанной работе, описав каждый пункт выполнения задания.

Задание 2. Антивирусная проверка информации на жестком диске.

Запустите имеющуюся у вас антивирусную программу и проверьте наличие вирусов на локальном диске C:.

Задание 3. Проверка флешки с записанным файлом на наличие вируса.

Найдите на диске C: файлы с любым расширением, начинающиеся на букву w (маска для поиска — w*). Скопируйте самый маленький по размеру из найденных файлов на флешку (проведите сортировку по размеру). Проверьте флешку с записанным файлом на наличие вирусов.

Задание 4. Ответьте на вопросы:

1. Что такое компьютерный вирус?

2. На какие типы разделяют компьютерные вирусы в различных видах классификации?
3. Чем отличаются макровирусы от обычных загрузочных вирусов?
4. Каковы основные пути проникновения вирусов в компьютер?
5. По каким признакам можно судить о поражении компьютера вирусом?
6. Какие типы антивирусных программ вам известны?
7. Каковы назначение и основные функции Антивируса Касперского?
8. Как проверить CD-диск или флешку на наличие вируса с помощью программы Антивирус Касперского?
9. В каком файле содержится информация о зараженных и вылеченных объектах?
10. Перечислите профилактические меры для борьбы с заражением вирусами.

3.1.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности в ходе текущего контроля успеваемости

Устный ответ

Оценка знаний предполагает дифференцированный подход к обучающемуся, учет его индивидуальных способностей, степень усвоения и систематизации основных понятий и категорий по дисциплине. Кроме того, оценивается не только глубина знаний поставленных вопросов, но и умение использовать в ответе практический материал. Оценивается культура речи, владение навыками ораторского искусства.

Критерии оценивания: последовательность, полнота, логичность изложения, анализ различных точек зрения, самостоятельное обобщение материала, использование профессиональных терминов, культура речи, навыки ораторского искусства. Изложение материала без фактических ошибок.

Оценка *«отлично»* ставится в случае, когда материал излагается исчерпывающе, последовательно, грамотно и логически стройно, при этом раскрываются не только основные понятия, но и анализируются точки зрения различных авторов. Обучающийся не затрудняется с ответом, соблюдает культуру речи.

Оценка *«хорошо»* ставится, если обучающийся твердо знает материал, грамотно и по существу излагает его, знает практическую базу, но при ответе на вопрос допускает несущественные погрешности.

Оценка *«удовлетворительно»* ставится, если обучающийся освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении материала, затрудняется с ответами, показывает отсутствие должной связи между анализом, аргументацией и выводами.

Оценка *«неудовлетворительно»* ставится, если обучающийся не отвечает на поставленные вопросы.

Кейсы (ситуации и задачи с заданными условиями)

Обучающийся должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи могут решаться устно и/или письменно. При решении задач также важно правильно сформулировать и записать вопросы, начиная с более общих и, кончая частными.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка *«отлично»* ставится в случае, когда обучающийся выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка *«хорошо»* ставится, если обучающийся в целом выполнил все требования, но не совсем четко определяется опора на теоретические положения, изложенные в научной литературе по данному вопросу.

Оценка *«удовлетворительно»* ставится, если обучающийся показал положительные результаты в процессе решения задачи.

Оценка *«неудовлетворительно»* ставится, если обучающийся не выполнил все требования.

Практическое задание

Обучающийся должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи могут решаться устно и/или письменно.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка *«отлично»* ставится в случае, когда обучающийся выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка *«хорошо»* ставится, если обучающийся в целом выполнил все требования, но не совсем четко определяется опора на теоретические положения, изложенные в научной литературе по данному вопросу.

Оценка *«удовлетворительно»* ставится, если обучающийся показал положительные результаты в процессе решения задачи.

Оценка *«неудовлетворительно»* ставится, если обучающийся не выполнил все требования.

Дискуссионные процедуры

Круглый стол, дискуссия, полемика, диспут, дебаты, мини-конференции являются средствами, позволяющими включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Задание дается заранее, определяется круг вопросов для обсуждения, группы участников этого обсуждения.

Дискуссионные процедуры могут быть использованы для того, чтобы студенты:

–лучше поняли усвояемый материал на фоне разнообразных позиций и мнений, не обязательно достигая общего мнения;

– смогли постичь смысл изучаемого материала, который иногда чувствуют интуитивно, но не могут высказать вербально, четко и ясно, или конструировать новый смысл, новую позицию;

– смогли согласовать свою позицию или действия относительно обсуждаемой проблемы.

Критерии оценивания – оцениваются действия всех участников группы. Понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Соответствие реальной действительности решений, выработанных в ходе игры. Владение терминологией, демонстрация владения учебным материалом по теме игры, владение методами аргументации, умение работать в группе (умение слушать, конструктивно вести беседу, убеждать, управлять временем, бесконфликтно общаться), достижение игровых

целей, (соответствие роли – при ролевой игре). Ясность и стиль изложения.

Оценка *«отлично»* ставится в случае, когда все требования выполнены в полном объеме.

Оценка *«хорошо»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия полностью соответствуют заданным целям. Решения, выработанные в ходе игры, полностью соответствуют реальной действительности. Но некоторые объяснения не совсем аргументированы, нарушены нормы общения, нарушены временные рамки, нарушен стиль изложения.

Оценка *«удовлетворительно»* ставится, если обучающиеся в целом демонстрируют понимание проблемы, высказывания и действия в целом соответствуют заданным целям. Однако, решения, выработанные в ходе игры, не совсем соответствуют реальной действительности. Некоторые объяснения не совсем аргументированы, нарушены временные рамки, нарушен стиль изложения.

Оценка *«неудовлетворительно»* ставится, если обучающиеся не понимают проблему, их высказывания не соответствуют заданным целям.

Исследовательский проект (реферат)

Исследовательский проект – проект, структура которого приближена к формату научного исследования и содержит доказательство актуальности избранной темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, историографии, обобщение результатов, выводы.

Результаты выполнения исследовательского проекта оформляется в виде реферата.

Критерии оценивания - поскольку структура исследовательского проекта максимально приближена к формату научного исследования, то при выставлении учитывается доказательство актуальности темы исследования, определение научной проблемы, объекта и предмета исследования, целей и задач, источников, методов исследования, выдвижение гипотезы, обобщение результатов и формулирование выводов, обозначение перспектив дальнейшего исследования.

Оценка *«отлично»* ставится в случае, когда обучающийся демонстрирует полное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«хорошо»* ставится, если обучающийся демонстрирует значительное понимание проблемы, все требования, предъявляемые к заданию выполнены.

Оценка *«удовлетворительно»* ставится, если обучающийся, демонстрирует частичное понимание проблемы, большинство требований, предъявляемых к заданию, выполнены

Оценка *«неудовлетворительно»* ставится, если обучающийся демонстрирует непонимание проблемы, многие требования, предъявляемые к заданию, не выполнены.

3.2. Оценочные материалы для проведения промежуточной аттестации

3.2.1. Критерии оценки результатов обучения по дисциплине (модулю)

Шкала оценивания	Результаты обучения	Показатели оценивания результатов обучения
ОТЛИЧНО	Знает:	- обучающийся глубоко и всесторонне усвоил материал, уверенно, логично, последовательно и грамотно его излагает, опираясь на знания основной и дополнительной литературы, - на основе системных научных знаний делает квалифицированные выводы и обобщения, свободно оперирует категориями и понятиями.
	Умеет:	- обучающийся умеет самостоятельно и правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, используя научные понятия, ссылаясь на нормативную базу.

	Владеет:	- обучающийся владеет рациональными методами (с использованием рациональных методик) решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал навыки - выделения главного, - связкой теоретических положений с требованиями руководящих документов, - изложения мыслей в логической последовательности, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
ХОРОШО	Знает:	- обучающийся твердо усвоил материал, достаточно грамотно его излагает, опираясь на знания основной и дополнительной литературы, - затрудняется в формулировании квалифицированных выводов и обобщений, оперирует категориями и понятиями, но не всегда правильно их верифицирует.
	Умеет:	- обучающийся умеет самостоятельно и в основном правильно решать учебно-профессиональные задачи или задания, уверенно, логично, последовательно и аргументировано излагать свое решение, не в полной мере используя научные понятия и ссылки на нормативную базу.
	Владеет:	- обучающийся в целом владеет рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении смог продемонстрировать достаточность, но не глубинность навыков, - выделения главного, - изложения мыслей в логической последовательности, - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
УДОВЛЕТВО-РИТЕЛЬНО	Знает:	- обучающийся ориентируется в материале, однако затрудняется в его изложении; - показывает недостаточность знаний основной и дополнительной литературы; - слабо аргументирует научные положения; - практически не способен сформулировать выводы и обобщения; - частично владеет системой понятий.
	Умеет:	- обучающийся в основном умеет решить учебно-профессиональную задачу или задание, но допускает ошибки, слабо аргументирует свое решение, недостаточно использует научные понятия и руководящие документы.
	Владеет:	- обучающийся владеет некоторыми рациональными методами решения сложных профессиональных задач, представленных деловыми играми, кейсами и т.д.; При решении продемонстрировал недостаточность навыков - выделения главного, - изложения мыслей в логической последовательности, - связки теоретических положений с требованиями руководящих документов, - самостоятельного анализа факты, событий, явлений, процессов в их взаимосвязи и диалектическом развитии.
НЕУДОВЛЕТВО-РИТЕЛЬНО	Знает:	- обучающийся не усвоил значительной части материала; - не может аргументировать научные положения; - не формулирует квалифицированных выводов и обобщений; - не владеет системой понятий.

	Умеет:	обучающийся не показал умение решать учебно-профессиональную задачу или задание.
	Владеет:	не выполнены требования, предъявляемые к навыкам, оцениваемым «удовлетворительно».

3.2.2. Контрольные задания и/или иные материалы для проведения промежуточной аттестации

Список вопросов для устных ответов (варианты теста)

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности
3. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
4. Понятие сервиса информационной безопасности. Идентификация и аутентификация.
5. Понятие сервиса информационной безопасности. Управление доступом.
6. Понятие сервиса информационной безопасности. протоколирование и аудит.
7. Понятие сервиса информационной безопасности. управление и анализ защищенности.
8. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
9. Понятие сервиса информационной безопасности. экранирование и туннелирование.
10. Понятие сервиса информационной безопасности. криптография: шифрование.
11. Понятие сервиса информационной безопасности. криптография: контроль целостности.
12. Криптология: базовые понятия и терминология.
13. Криптографические примитивы и их свойства.
14. Модели основных криптоаналитических атак.
15. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ.

Вариант теста

1. Конфиденциальная информация это

a) сведения, составляющие государственную тайну

b) сведения о состоянии здоровья высших должностных лиц

c) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ

d) данные о состоянии преступности в стране

2. Какая информация подлежит защите?

a) информация, циркулирующая в системах и сетях связи

b) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

c) только информация, составляющая государственные информационные ресурсы

d) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

3. Наиболее надежным механизмом для защиты содержания сообщений является …?

4. Первым этом разработки системы защиты ИС является … потенциально возможных угроз информации.

5. Удачная криптоатака называется …?

6. Под информационной безопасностью понимается:
a) 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
b) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия
c) нет верного ответа
7. Защита информации:
a) небольшая программа для выполнения определенной задачи
b) комплекс мероприятий, направленных на обеспечение информационной безопасности
c) процесс разработки структуры базы данных в соответствии с требованиями пользователей
8. Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?
9. Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается …?
10. Защита с применением меток безопасности, согласно «Оранжевой книге», используется в системах класса …?

Тексты проблемно-аналитических и (или) практических учебно-профессиональных задач

Написать программу преобразования исходных данных по методу гаммирования.

```
#include<iostream.h>
#include<conio.h>
#include<stdlib.h>
#include<math.h>

constint Max=12;
void main()
{
 bool M[Max]={true, true, false, true, false};
 bool A[Max]={false, true, false, true, true};
randomize();
for( shorti=0;i<Max;i++){M[i]=floor(random(2));}
for( shorti=0;i<Max;i++){A[i]=floor(random(2));}
 //cout<<M[0];
cout<<"";
for( shorti=0;i<Max;i++){cout<<A[i];}
cout<<"\n----------";
for(int k=0;k<100;k++){
cout<<"\n";

float N = 0;
        for( shorti=0;i<Max;i++){N+=M[i]*A[i];}

cout<<"["<<M[0]<<"]<-";
```

```
for( shorti=0;i<Max;i++){cout<<M[i];}

for( shorti=1;i<Max;i++){M[i-1]=M[i];}

M[Max-1]=fmod(N,2);
cout<<"<-["<<M[Max-1]<<"]";
getch();
 }
getch();
}
```

3.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков в ходе промежуточной аттестации

Процедура оценивания знаний (тест)

Предлагаемое количество заданий	20
Последовательность выборки вопросов из каждого раздела	Определена по разделам
Критерии оценки	- правильный ответ на вопрос
«5» если	правильно выполнено 90-100% тестовых заданий
«4» если	правильно выполнено 70-89% тестовых заданий
«3» если	правильно выполнено 50-69% тестовых заданий

Процедура оценивания знаний (устный ответ)

Предел длительности	10 минут
Предлагаемое количество заданий	2 вопроса
Последовательность выборки вопросов из каждого раздела	Случайная
Критерии оценки	- требуемый объем и структура - изложение материала без фактических ошибок - логика изложения - использование соответствующей терминологии - стиль речи и культура речи - подбор примеров их научной литературы и практики
«5» если	требования к ответу выполнены в полном объеме
«4» если	в целом выполнены требования к ответу, однако есть небольшие неточности в изложении некоторых вопросов
«3» если	требования выполнены частично – не выдержан объем, есть фактические ошибки, нарушена логика изложения, недостаточно используется соответствующая терминологии

Процедура оценивания умений и навыков (решение проблемно-аналитических и практических учебно-профессиональных задач)

Предлагаемое количество заданий	1
Последовательность выборки	Случайная
Критерии оценки:	- выделение и понимание проблемы - умение обобщать, сопоставлять различные точки зрения - полнота использования источников - наличие авторской позиции - соответствие ответа поставленному вопросу - использование социального опыта, материалов СМИ, статистических данных - логичность изложения - умение сделать квалифицированные выводы и обобщения с точки зрения решения профессиональных задач - умение привести пример

	- опора на теоретические положения - владение соответствующей терминологией
«5» если	требования к ответу выполнены в полном объеме
«4» если	в целом выполнены требования к ответу, однако есть небольшие неточности в изложении некоторых вопросов. Затрудняется в формулировании квалифицированных выводов и обобщений
«3» если	требования выполнены частично – пытается обосновать свою точку зрения, однако слабо аргументирует научные положения, практически не способен самостоятельно сформулировать выводы и обобщения, не видит связь с профессиональной деятельностью

4. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

4.1. Электронные учебные издания

1. Никифоров, С. Н. Защита информации. Защищенные сети: учебное пособие / С. Н. Никифоров. — Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 80 с. — ISBN 978-5-9227-0762-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/74382.html. — Режим доступа: для авторизир. пользователей
2. Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных: учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 с. — ISBN 978-5-9227-0783-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/80747.html. — Режим доступа: для авторизир. пользователей
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/87995.html. — Режим доступа: для авторизир. пользователей

4.2. Электронные образовательные ресурсы

1. Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) – электронная библиотека по всем отраслям знаний http://www.iprbookshop.ru
2. e-Library.ru: Научная электронная библиотека [Электронный ресурс]. – URL: http://elibrary.ru/.
3. Научная электронная библиотека «КиберЛенинка» [Электронный ресурс]. – URL: http://cyberleninka.ru/.

4.3. Современные профессиональные базы данных и информационные справочные системы

Обучающимся обеспечен доступ (удаленный доступ) к ниже следующим современным профессиональным базам данных и информационным справочным системам:

1. Словари и энциклопедии на Академике [Электронный ресурс]. – URL: http://dic.academic.ru.
2. Система информационно-правового обеспечения «Гарант» [Электронный ресурс]. – http://www.garant.ru/.

4.4. Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. Лицензионное программное обеспечение: операционная система Microsoft Windows, пакет офисных приложений Microsoft Office.
2. Свободно распространяемое программное обеспечение: свободные пакеты офисных приложений Apache Open Office, LibreOffice, Kaspersky Free
3. Программное обеспечение отечественного производства: справочно-правовая система «Гарант» (Электронный периодический справочник «Система ГАРАНТ»), Цифровая библиотека IPRsmart (ЦБ IPRsmart), автоматизированная система управления цифровой библиотекой IPRsmart (АСУ ЦБ IPRsmart).

4.5. Оборудование и технические средства обучения

Для реализации дисциплины (модуля) используются учебные аудитории для проведения учебных занятий, которые оснащены оборудованием и техническими средствами обучения, и помещения для самостоятельной работы обучающихся, которые оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду ЧОУ ВО АУП. Допускается замена оборудования его виртуальными аналогами.

Наименование учебных аудиторий для проведения учебных занятий и помещений для самостоятельной работы*	**Оснащенность учебных аудиторий для проведения учебных занятий и помещений для самостоятельной работы оборудованием и техническими средствами обучения**
Учебные аудитории для проведения учебных занятий	Учебные аудитории оборудованы комплектом специализированной мебели, отвечающей всем установленным нормам и требованиям, и техническими средствами обучения, служащими для представления учебной информации большой аудитории: мультимедийный проектор, экран для проектора, стереоколонки, ноутбук с установленным программным обеспечением и доступом в Интернет, доской, наглядно-учебными пособиями в виде презентаций по дисциплине
Лаборатория информационных систем и технологий	Лаборатория оборудована комплектом специализированной мебели, отвечающей всем установленным нормам и требованиям, техническими средствами обучения, служащими для представления учебной информации большой аудитории: мультимедийный проектор, экран для проектора, широкоформатный телевизор, стереоколонки, ноутбук (для преподавателя) с установленным программным обеспечением и доступом в Интернет, компьютеры с установленным программным обеспечением и доступом в Интернет, принтер, доска, наглядно-учебные пособия в виде презентаций по дисциплине
Помещения для самостоятельной работы обучающихся	Помещения оснащены: комплектом специализированной мебели, отвечающий всем установленным нормам и требованиям, сканером, принтером, копировальным аппаратом, компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно - образовательную среду ЧОУ ВО «АУП», ЭБС «IPR-books»

* Номер конкретной аудитории указан в приказе об аудиторном фонде, расписании учебных занятий и расписании промежуточной аттестации.