Министерство образования и науки Астраханской области
Государственное автономное образовательное учреждение
Астраханской области высшего образования
«Астраханский государственный архитектурно-строительный университет»
(ГАОУ АО ВО «АГАСУ»)

УТВЕРЖДАЮ
Первый проректор
_____ /*И.Ю. Петрова*/
Подпись *И.О.Ф.*
«*30*» ____*05*____ *2019г.*

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины

Безопасность информационных технологий и систем
(указывается наименование в соответствии с учебным планом)

По направлению подготовки

09.03.02 «Информационные системы и технологии»
(указывается наименование направления подготовки в соответствии с ФГОС)

Направленность (профиль)

«Информационные системы и технологии в строительстве и архитектуре»
(указывается наименование профиля в соответствии с ОПОП)

Кафедра Системы автоматизированного проектирования и моделирования

Квалификация выпускника ***бакалавр***

Астрахань - 2019

Разработчик:

к.т.н. доцент — (занимаемая должность, учёная степень и учёное звание)

_____ (подпись)

Ю.И. Евдокименко — И.О.Ф.

Рабочая программа рассмотрена и утверждена на заседании кафедры *«Системы автоматизированного проектирования и моделирования»* протокол №10 от 25.05.2019 г.

Заведующий кафедрой _____ (подпись) / Т.В. Хоменко / И.О.Ф.

Согласовано:

Председатель МКН *«Информационные системы и технологии»* направленность (профиль) *«Информационные системы и технологии в строительстве и архитектуре»* _____ (подпись) / Т.В. Хоменко / И.О.Ф.

Начальник УМУ _____ (подпись) И.В. Аксютина / И. О. Ф

Специалист УМУ _____ (подпись) / Е.А. Судакова / И. О. Ф

Начальник УИТ _____ (подпись) / С.В. Пупырев / И. О. Ф

Заведующая научной библиотекой _____ (подпись) Р.С. Кандакешова / И. О. Ф

Содержание

1. Цель освоения дисциплины

Целью освоения дисциплины «Безопасность информационных технологий и систем» является формирование компетенций обучающегося в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии».

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

В результате освоения дисциплины обучающийся должен овладеть следующими компетенциями:

ПК-11 - Способность проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

В результате освоения дисциплин, формирующих компетенцию ПК-11 обучающийся должен овладеть следующими результатами обучения:

Знать:

- дисциплины управления проектами, инструменты и методы анализа требований, верификации требований в проектах в области ИТ, выдачи и контроля поручений (ПК-11.1).

Уметь:

- анализировать входные данные, разрабатывать плановую документацию, работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами на исправление несоответствий) (ПК-11.2).

Иметь практический опыт:

- анализа входных данных, разработки документов, контроля выданных поручений (ПК-11.3).

3. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.18 «Безопасность информационных технологий и систем» реализуется в рамках Блок 1. «Дисциплины (модули)», часть формируемая участниками образовательных отношений. Дисциплина базируется на результатах обучения, полученных в рамках изучения следующих дисциплин: «Правовое обеспечение профессиональной деятельности», «Администрирование информационных систем».

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

Форма обучения	Очная	Заочная
1	2	3
Трудоемкость в зачетных единицах:	8 семестр – 3 з.е.; всего - 3 з.е.	8 семестр – 3 з.е.; всего - 3 з.е.
Лекции (Л)	8 семестр – 12 часов; всего - 12 часов	8 семестр – 4 часа; всего - 4 часа
Лабораторные занятия (ЛЗ)	8 семестр – 36 часов; всего - 36 часов	8 семестр – 6 часов; всего - 6 часов
Практические занятия (ПЗ)	учебным планом не предусмотрены	учебным планом не предусмотрены
Самостоятельная работа (СР)	8 семестр – 60 часов; всего - 60 часов	8 семестр – 98 часов; всего - 98 часов
Форма текущего контроля:		
Контрольная работа	учебным планом не предусмотрены	учебным планом не предусмотрены
Форма промежуточной аттестации:		
Экзамены	семестр – 8	семестр – 8
Зачет	учебным планом не предусмотрены	учебным планом не предусмотрены
Зачет с оценкой	учебным планом не предусмотрены	учебным планом не предусмотрены
Курсовая работа	учебным планом не предусмотрены	учебным планом не предусмотрены
Курсовой проект	учебным планом не предусмотрены	учебным планом не предусмотрены

5. Содержание дисциплины, структурированное по разделам с указанием отведенного на них количества академических часов и типов учебных занятий

5.1. Разделы дисциплины и трудоемкость по типам учебных занятий и работы обучающихся (в академических часах)

5.1.1. Очная форма обучения

№ п/п	Раздел дисциплины. *(по семестрам)*	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по типам учебных занятий и работы обучающихся				Форма текущего контроля и промежуточной аттестации
				контактная			СР	
				Л	ЛЗ	ПЗ		
1	2	3	4	5	6	7	8	9
1	Раздел 1. Введение в информационную безопасность	6	8	2			4	экзамен
2	Раздел 2. Правовое и организационное обеспечение информационной безопасности	12	8	2	4		6	
3	Раздел 3. Технические средства и методы защиты информации	20	8	2	8		10	
4	Раздел 4. Программно-аппаратные средства и методы обеспечения информационной безопасности	32	8	2	10		20	
5	Раздел 5. Криптографические методы защиты информации. Стеганография.	20	8	2	8		10	
6	Раздел 6. Защита в компьютерных сетях	18	8	2	6		10	
Итого		**108**		**12**	**36**		**60**	

5.1.2. Заочная форма обучения:

№ п/п	Раздел дисциплины *(по семестрам)*	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по типам учебных занятий и работы обучающихся				Форма текущего контроля и промежуточной аттестации
				контактная			СР	
				Л	ЛЗ	ПЗ		
1	2	3	4	5	6	7	8	9
1	Раздел 1. Введение в информационную безопасность	10	8				10	экзамен
2	Раздел 2. Правовое и организационное обеспечение информационной безопасности	14	8	1			13	
3	Раздел 3. Технические средства и методы защиты информации	19	8	1	2		16	
4	Раздел 4. Программно-аппаратные средства и методы обеспечения информационной безопасности	30	8	1	2		27	
5	Раздел 5. Криптографические методы защиты информации. Стеганография.	17	8	1			16	
6	Раздел 6. Защита в компьютерных сетях	18	8		2		16	
	Итого	**108**		**4**	**6**		**98**	

5.2. Содержание дисциплины, структурированное по разделам

5.2.1. Содержание лекционных занятий

№	Наименование раздела дисциплины	Содержание
1	2	3
1	Раздел 1. Введение в информационную безопасность	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации и инструменты анализа данных и требований.
2	Раздел 2. Правовое и организационное обеспечение информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Верификация требований в проектах в области ИТ.
3	Раздел 3. Технические средства и методы защиты информации	Инженерная защита объектов. Защита информации от утечки по техническим каналам. Выдача и контроль поручений по технической защите информации.
4	Раздел 4. Программно-аппаратные средства и методы обеспечения информационной безопасности	Классификация программно-аппаратных средств защиты информации. Вирусы. Классификация вирусов. Антивирусные программы. Профилактика защиты информации от компьютерных вирусов.
5	Раздел 5. Криптографические методы защиты информации. Стеганография.	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Основные понятия стеганографии. Стеганографическая система. Алгоритмы стеганографии.
6	Раздел 6. Защита в компьютерных сетях	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от компьютерных угроз.

5.2.2. Содержание лабораторных занятий

№	Наименование раздела дисциплины	Содержание
1	2	3
1	Раздел 2. Правовое и организационное обеспечение информационной безопасности	Анализ входных данных и назначение прав пользователей при произвольном доступе Windows Назначение прав пользователей при произвольном доступе Linux
2	Раздел 3. Технические средства и методы защиты информации	Знакомство с инженерно-техническими средствами защиты. Разработка плановой документации по использованию технических средств защиты информации.
3	Раздел 4. Программно-аппаратные средства и методы обеспечения информационной безопасности	Управление шаблонами безопасности Windows. Анализ безопасности системы с использованием плановой документации.

4	Раздел 5. Криптографические методы защиты информации. Стеганография.	Архивирование и восстановление информации, исправление несоответствий. Шифрующая файловая система EFS и управление сертификатами. Разработка регламентирующих документов и контроль их выполнения.
5	Раздел 6. Защита в компьютерных сетях	Технология защиты сетевых компьютеров. Составление записей по качеству и работа с ними.

5.2.3. Содержание практических занятий

учебным планом не предусмотрены

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

Очная форма обучения

№	Наименование раздела дисциплины	Содержание	Учебно-методическое обеспечение
1	2	3	4
1	Раздел 1. Введение в информационную безопасность	Изучение теоретического материала по рекомендованной в рабочей программе литературе. Подготовка к экзамену.	[1],[8]
2	Раздел 2. Правовое и организационное обеспечение информационной безопасности	Подготовка к выполнению лабораторных работ. Подготовка к защите лабораторных работ. Подготовка к экзамену. Подготовка к тестированию.	[1],[9]
3	Раздел 3. Технические средства и методы защиты информации	Изучение теоретического и практического материала по рекомендованной в рабочей программе литературе. Подготовка к выполнению лабораторных работ. Подготовка к экзамену.	[1],[2]
4	Раздел 4. Программно-аппаратные средства и методы обеспечения информационной безопасности	Изучение теоретического и практического материала по рекомендованной в рабочей программе литературе. Подготовка к выполнению лабораторных работ. Подготовка к экзамену. Подготовка к тестированию.	[1],[4]
5	Раздел 5. Криптографические методы защиты информации. Стеганография.	Подготовка к выполнению лабораторных работ. Подготовка к экзамену. Подготовка к тестированию.	[1],[6]-[9]
6	Раздел 6. Защита в компьютерных сетях	Изучение теоретического и практического материала по рекомендованной в рабочей программе литературе. Подготовка к выполнению лабораторных работ. Подготовка к экзамену. Проектирование защищенных сетей. Списки доступа. Стандартные и расширенные списки доступа.	[1]-[5],[10]

Заочная форма обучения

№	Наименование раздела дисциплины	Содержание	Учебно-методическое обеспечение

1	2	3	4
1	Раздел 1. Введение в информационную безопасность	Изучение теоретического материала по рекомендованной в рабочей программе литературе. Подготовка к экзамену.	[1],[8]
2	Раздел 2. Правовое и организационное обеспечение информационной безопасности	Изучение теоретического материала по рекомендованной в рабочей программе литературе. Подготовка к экзамену. Подготовка к тестированию.	[1],[9]
3	Раздел 3. Технические средства и методы защиты информации	Изучение теоретического и практического материала по рекомендованной в рабочей программе литературе. Подготовка к выполнению лабораторных работ. Подготовка к экзамену.	[1],[2]
4	Раздел 4. Программно-аппаратные средства и методы обеспечения информационной безопасности	Изучение теоретического и практического материала по рекомендованной в рабочей программе литературе. Подготовка к выполнению лабораторных работ. Подготовка к экзамену. Подготовка к тестированию.	[1],[4]
5	Раздел 5. Криптографические методы защиты информации. Стеганография.	Изучение теоретического материала по рекомендованной в рабочей программе литературе. Подготовка к экзамену.	[1],[6]-[9]
6	Раздел 6. Защита в компьютерных сетях	Изучение теоретического и практического материала по рекомендованной в рабочей программе литературе. Подготовка к выполнению лабораторных работ. Подготовка к экзамену. Проектирование защищенных сетей. Списки доступа. Стандартные и расширенные списки доступа.	[1]-[5],[10]

5.2.5. Темы контрольных работ
учебным планом не предусмотрены

5.2.6. Темы курсовых проектов/ курсовых работ
учебным планом не предусмотрены

6. Методические указания для обучающихся по освоению дисциплины

Организация деятельности студента
Лекция В ходе лекционных занятий необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и

предусмотренной учебной программой.
Лабораторное занятие Работа в соответствии с методическими указания по выполнению лабораторных работ.
Самостоятельная работа Самостоятельная работа студента над усвоением учебного материала по учебной дисциплине может выполняться в помещениях для самостоятельной работы, а также в домашних условиях. Содержание самостоятельной работы студента определяется учебной программой дисциплины, методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа в аудиторное время может включать: – конспектирование (составление тезисов) лекций; – работу с учебной литературой; – участие в тестировании; – выполнение заданий лабораторной работы. Самостоятельная работа во внеаудиторное время может состоять из: – повторение лекционного материала; – изучения учебной и научной литературы; – изучения нормативных правовых актов (в т.ч. в электронных базах данных); – подготовки к тестированию; – подготовка к лабораторным занятиям.
Подготовка к экзамену Подготовка студентов к экзамену включает три стадии: - самостоятельная работа в течение семестра; - непосредственная подготовка в дни, предшествующие экзамену; - подготовка к ответу на вопросы, содержащиеся в билете.

7. Образовательные технологии

Перечень образовательных технологий, используемых при изучении дисциплины.

Традиционные образовательные технологии

Перечень образовательных технологий, используемых при изучении дисциплины «Безопасность информационных технологий и систем» проводятся с использованием традиционных образовательных технологий ориентирующиеся на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения), учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер. Формы учебных занятий с использованием традиционных технологий:

Лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Лабораторные занятия – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

Интерактивные технологии

Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отно-

шения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды.

По дисциплине «Безопасность информационных технологий и систем» лекционные занятия проводятся с использованием следующих интерактивных технологий:

Лекция-визуализация – представляет собой визуальную форму подачи лекционного материала средствами ТСО или аудиовидеотехники (видео-лекция). Чтение такой лекции сводится к развернутому или краткому комментированию просматриваемых визуальных материалов (в виде схем, таблиц, графов, графиков, моделей). Лекция-визуализация помогает студентам преобразовывать лекционный материал в визуальную форму, что способствует формированию у них профессионального мышления за счет систематизации и выделения наиболее значимых, существенных элементов.

По дисциплине «Безопасность информационных технологий и систем» лабораторные занятия проводятся с использованием следующих интерактивных технологий:

Работа в малых группах – это одна из самых популярных стратегий, так как она дает всем обучающимся (в том числе и стеснительным) возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Все это часто бывает невозможно в большом коллективе.

8. Учебно-методическое и информационное обеспечение дисциплины

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

а) основная учебная литература

1. Исаев, Г.Н. Практикум по информационным технологиям: учебное пособие / Г.Н. Исаев. – Москва: «Омега-Л». – 2013. – 188с. – ISBN 978-5-370-02507-5.

2. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. – Самара: ФГБОУ ВПО «Самарский государственный архитектурно-строительный университет». – 2014. – 113с. – ISBN 978-5-9585-0603-3. – [Электронный ресурс] Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331

3. Пакин, А.И. Информационная безопасность информационных систем управления предприятием: учебное пособие по части курса/ А.И. Пакин. – М.: Издательство «Московская государственная академия водного транспорта». – 2009. – 41с. – [Электронный ресурс] Режим доступа: http://www.iprbookshop.ru/46462.html

б) дополнительная учебная литература

4. Панасенко, С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: «БХВ-Петербург». – 2009. – 576с.

5. Галатенко, В.А. Основы информационной безопасности / В.А. Галатенко. – М.: «Интернет-Университет Информационных Технологий (ИНТУИТ)». – 2016. – 266с. – [Электронный ресурс] Режим доступа: http://www.iprbookshop.ru/52209.html

6. Заляжных, В.А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем / В.А. Заляжных, А.В. Гирик. – СПб.: Издательство «Университет ИТМО». – 2014. – 139с. – [Электронный ресурс] Режим доступа: http://www.iprbookshop.ru/65733.html

7. Петренко, В.И. Теоретические основы защиты информации: учебное пособие / В.И. Петренко. – Ставрополь: Издательство «Северо-Кавказский федеральный университет». – 2015. – 222с. – [Электронный ресурс] Режим доступа: http://biblioclub.ru/index.php?page=book&id=458204

в) перечень учебно-методического обеспечения:

8. Евдошенко, О.И. Методические указания к выполнению лабораторных работ по дисциплине «Безопасность информационных технологий и систем» /О.И. Евдошенко. – Астрахань: АГАСУ. – 2019 г. – 16с
http://moodle.aucu.ru

9. Евдошенко, О.И. Методические указания по выполнению самостоятельной работы по дисциплине «Безопасность информационных технологий и систем» /О.И. Евдошенко. – Астрахань: АГАСУ. – 2019 г. – 16с
http://moodle.aucu.ru

г) перечень онлайн-курсов

10. Основы информационной безопасности [Электронный ресурс] Режим доступа: https://www.intuit.ru/studies/courses/10/10/info

11. Стандарты информационной безопасности [Электронный ресурс] Режим доступа: https://www.intuit.ru/studies/courses/30/30/info

12. Безопасность сетей [Электронный ресурс] Режим доступа: https://www.intuit.ru/studies/courses/102/102/info

8.2. Перечень необходимого лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, используемого при осуществлении образовательного процесса по дисциплине

1. 7-Zip
2. Office 365 A1
3. Adobe Acrobat Reader DC
4. Google Chrome
5. VLC media player
6. Apache Open Office
7. Office Pro Plus Russian OLPNL Academic Edition
8. Kaspersky Endpoint Security
9. Internet Explorer
10. Microsoft SQL Server 2016 Express
11. Visual Studio
12. Microsoft Azure Dev Tools for Teaching

8.3. Перечень современных профессиональных баз данных и информационных справочных систем, доступных обучающимся при освоении дисциплины

1. Электронная информационно-образовательная среда Университета: образовательный портал: http://moodle.aucu.ru
2. Электронно-библиотечная система «Университетская библиотека»: https://biblioclub.ru
3. Электронно-библиотечная система «IPRbooks»: www.iprbookshop.ru
4. Научная электронная библиотека (http://www.elibrary.ru/)
5. Консультант + (http://www.consultant-urist.ru/)
6. Федеральный институт промышленной собственности (https://www1.fips.ru/)
7. Патентная база USPTO (https://www.uspto.gov/patents-application-process/search-patents)

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

№ п\п	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Учебная аудитория для проведения учебных занятий 414056, г. Астрахань, ул. Татищева, 18, аудитория №207 414056, г. Астрахань, ул. Татищева, 18, аудитория №209 414056, г. Астрахань, ул. Татищева, 18, аудитория №211	аудитория №207 Комплект учебной мебели Компьютеры – 15 шт. Стационарный мультимедийный комплект Доступ к информационно – телекоммуникационной сети «Интернет»
		аудитория №209 Комплект учебной мебели Компьютеры – 15 шт. Стационарный мультимедийный комплект Доступ к информационно – телекоммуникационной сети «Интернет»
		аудитория №211 Комплект учебной мебели Компьютеры – 15 шт. Стационарный мультимедийный комплект Доступ к информационно – телекоммуникационной сети «Интернет»
2	Помещение для самостоятельной работы 414056, г. Астрахань, ул. Татищева, 18, аудитория №201 414056, г. Астрахань, ул. Татищева, 18б, аудитория №308	аудитория №201 Комплект учебной мебели Компьютеры – 4 шт. Доступ к информационно – телекоммуникационной сети «Интернет»
		аудитория №308 Комплект учебной мебели Компьютеры – 11 шт. Доступ к информационно – телекоммуникационной сети «Интернет»

10. Особенности организации обучения по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья на основании письменного заявления дисциплина «Безопасность информационных технологий и систем» реализуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья (далее – индивидуальных особенностей).

Лист внесения дополнений и изменений
в рабочую программу учебной дисциплины
«Безопасность информационных технологий и систем»
(наименование дисциплины)

на 20_- 20_учебный год

Рабочая программа пересмотрена на заседании кафедры **«***Систем автоматизированного проектирования и моделирования***»**, протокол № ____ от _____20__г.

Зав. кафедрой

_____ _____ /_____/
ученая степень, ученое звание подпись И.О. Фамилия

В рабочую программу вносятся следующие изменения:
1. _____
2._____
3._____
4._____
5._____

Составители изменений и дополнений:
_____ _____ /_____ /
ученая степень, ученое звание подпись И.О. Фамилия

_____ _____ /_____/
ученая степень, ученое звание подпись И.О. Фамилия

Председатель МКН «*Информационные системы и технологии*»
направленность (профиль) *«Информационные системы и технологии в строительстве и архитектуре»* _____ /_____/
(подпись) И.О.Ф.

Министерство образования и науки Астраханской области
Государственное автономное образовательное учреждение
Астраханской области высшего образования
«Астраханский государственный архитектурно-строительный университет»
(ГАОУ АО ВО «АГАСУ»)

УТВЕРЖДАЮ
Первый проректор
Подпись /И.Ю. Петрова/
И.О.Ф.
«30» 05 2019г.

ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Наименование дисциплины

Безопасность информационных технологий и систем
(указывается наименование в соответствии с учебным планом)

По направлению подготовки

09.03.02 «Информационные системы и технологии»
(указывается наименование направления подготовки в соответствии с ФГОС)

Направленность (профиль)

«Информационные системы и технологии в строительстве и архитектуре»
(указывается наименование профиля в соответствии с ОПОП)

Кафедра Системы автоматизированного проектирования и моделирования

Квалификация выпускника ***бакалавр***

Астрахань - 2019

Разработчики:

к. т. н., доцент — (занимаемая должность, учёная степень и учёное звание)

(подпись)

О.И. Евдокименко — И.О.Ф.

Оценочные и методические материалы рассмотрены и утверждены на заседании кафедры *«Системы автоматизированного проектирования и моделирования»* протокол № 10 от 25.05 2019 г.

Заведующий кафедрой _____ (подпись) / Т.В. Хоменко / И.О.Ф.

Согласовано:

Председатель МКН *«Информационные системы и технологии»* направленность (профиль) *«Информационные системы и технологии в строительстве и архитектуре»* _____ (подпись) / Т.В. Хоменко / И.О.Ф.

Начальник УМУ _____ (подпись) / И.В. Аксютина / И. О. Ф.

Специалист УМУ _____ (подпись) / Е.А. Будникова / И. О. Ф.

Содержание

1. Оценочные и методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Оценочные и методические материалы являются неотъемлемой частью рабочей программы дисциплины (далее РПД) и представлены в виде отдельного документа

1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индекс и формулировка компетенции N	Индикаторы достижений компетенций, установленные ОПОП	Номер раздела дисциплины (в соответствии с п.5.1 РПД)						Формы контроля с конкретизацией задания
		1	2	3	4	5	6	
1	2	3						4
ПК-11 - Способность проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения	Знать:							Экзамен, вопросы 1-41 Тест, вопросы 1-12 Защита лабораторной работы 1-8
	дисциплины управления проектами, инструменты и методы анализа требований, верификации требований в проектах в области ИТ, выдачи и контроля поручений	X	X			X	X	
	Уметь:							
	анализировать входные данные, разрабатывать плановую документацию, работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами на исправление несоответствий)	X		X		X	X	
	Иметь практический опыт:							
	анализа входных данных, разработки документов, контроля выданных поручений	X		X	X		X	

1.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.2.1. Перечень оценочных средств текущей формы контроля

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3
Тесты	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект тестовых материалов
Защита лабораторных работ	Средство, позволяющее оценить умение и владение обучающегося излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Рекомендуется для оценки умений и владений студентов	Темы лабораторных работ и требования к их защите

1.2.2. Описание показателей и критериев оценивания компетенций по дисциплине на различных этапах их формирования, описание шкал оценивания

Компетенция, этапы освоения компетенции	Планируемые результаты обучения	Показатели и критерии оценивания результатов обучения			
		Ниже порогового уровня (не зачтено)	Пороговый уровень (Зачтено)	Продвинутый уровень (Зачтено)	Высокий уровень (Зачтено)
1	2	3	4	5	6
ПК-11 - Способность проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения	Знает: дисциплины управления проектами, инструменты и методы анализа требований, верификации требований в проектах в области ИТ, выдачи и контроля поручений	Отсутствие знания современных технологий и методик защиты информации	Фрагментарное знание современных технологий и методик защиты информации	Знание основных технологий и методик защиты информации, инструментов и методов анализа требований.	Сформировавшееся на высоком уровне знания современных технологий и методик защиты информации
	Умеет: анализировать входные данные, разрабатывать плановую документацию, работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами на исправление несоответствий)	Отсутствие умения управлять информационной безопасностью организации	Фрагментарное умение управлять информационной безопасностью организации	Умение анализировать потенциальные угрозы, разрабатывать плановую документацию под руководством опытного специалиста.	Умение анализировать потенциальные угрозы, самостоятельно разрабатывать плановую документацию в соответствии с требованиями по качеству
	Иметь практический опыт**:** анализа входных данных,	Отсутствие владения методами оценки рисков ин-	Фрагментарное владение методами оценки рисков	Владение технологиями анализ угроз, оценкой защищенности инфор-	Профессиональное владение современными технологиями анализ угроз, обеспечение

	разработки документов, контроля выданных поручений	формационной безопасности; отсутствие владения современными технологиями защиты информации	информационной безопасности; фрагментарное владение современными технологиями защиты информации	мационной среды	полноценной защитой, разработка политики безопасности, контроль поручения.

1.2.3. Шкала оценивания

Уровень достижений	Отметка в 5-бальной шкале	Зачтено/ не зачтено
высокий	«5» (отлично)	зачтено
продвинутый	«4» (хорошо)	зачтено
пороговый	«3» (удовлетворительно)	зачтено
ниже порогового	«2» (неудовлетворительно)	не зачтено

2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ:

2.1. Экзамен

а) типовые вопросы к экзамену (приложение 1)

б) критерии оценивания.

При оценке знаний на экзамене учитывается:

1. Уровень сформированности компетенций.
2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.
4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	Отлично	Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Полно раскрываются причинно-следственные связи между явлениями и событиями. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.
2	Хорошо	Ответы на поставленные вопросы излагаются систематизировано и последовательно. Базовые нормативно-правовые акты используются, но в недостаточном объеме. Материал излагается уверенно. Раскрыты причинно-следственные связи между явлениями и событиями. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.
3	Удовлетворительно	Допускаются нарушения в последовательности изложения. Имеются упоминания об отдельных базовых нормативно-правовых актах. Неполно раскрываются причинно-следственные связи между явлениями и событиями. Демонстрируются поверхностные знания вопроса, с трудом решаются конкретные задачи. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.
4	Неудовлетворительно	Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Не раскрываются причинно-следственные связи между явлениями и событиями. Не проводится анализ. Выводы отсутствуют. Ответы на дополнительные вопросы отсутствуют. Имеются заметные нарушения норм литературной речи.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ:

2.2. Тесты

а) типовые вопросы для тестирования (приложение 2)

б) критерии оценивания.

При оценке по результатам тестов учитывается:

1. Уровень сформированности компетенций.
2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.
4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	Отлично	если выполнены следующие условия: - даны правильные ответы не менее чем на 90% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ; - на все вопросы, предполагающие свободный ответ, студент дал правильный и полный ответ.
2	Хорошо	если выполнены следующие условия: - даны правильные ответы не менее чем на 75% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ; - на все вопросы, предполагающие свободный ответ, студент дал правильный ответ, но допустил незначительные ошибки и не показал необходимой полноты.
3	Удовлетворительно	если выполнены следующие условия: - даны правильные ответы не менее чем на 50% вопросов теста, исключая вопросы, на которые студент должен дать свободный ответ; - на все вопросы, предполагающие свободный ответ, студент дал непротиворечивый ответ, или при ответе допустил значительные неточности и не показал полноты.
4	Неудовлетворительно	если студентом не выполнены условия, предполагающие оценку «Удовлетворительно».

2.3. Защита лабораторной работы

а) типовые задания:

ПК-11

Лабораторная работа №1

1) Создание учетной записи.

1. Откройте оснастку Управление компьютером в Панели инструментов

2. Создайте пользователей (см. таблица 1)

Таблица 1

Имя пользователя	Полное имя	Пароль	Примечание
Ваша фамилия	Это моя учетная запись	2222	Запретить смену пароля пользователем.
Ваше имя	Любое	3333	Срок действия пароля не ограничен.

3. Добавьте любого пользователя из созданных Вами в группу «Опытные пользователи»

4. Перечислите, какие пользователи заданы в системе по умолчанию в виде таблицы:

Имя пользователя	Описание

2) Создание локальной группы.

1. Создайте новую группу: имя группы – Ваша фамилия.
2. Добавьте в группу пользователя с именем Вашей фамилии
3. Перечислите, какие группы заданы в системе по умолчанию в виде таблицы:

Имя группы	Описание

3) Назначения системных прав пользователям

1. Открыть окно настройки прав пользователей (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя);
2. Добавить группу с Вашей фамилией в число групп, обладающих правом «Доступ к компьютеру из сети»;
3. Исключить пользователя «Гость» из числа пользователей, обладающих правом «Локальный вход в систему»;
4. Добавить одного из созданных пользователей к списку пользователей, обладающих правом «Локальный вход в систему» и «Изменение системного времени».

4) Временная блокировка учетной записи.

1. Откройте оснастку Управление компьютером.
2. Откройте папку Пользователи и выберите учетную запись с именем Вашей фамилии.
3. В открывшемся окне установите отметку пункта Отключить учетную запись
4. Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.

Создание пользователей с использованием командной строки

1. Просмотрите пользователей, зарегистрированных в системе
2. Добавьте пользователя inforXXX (XXX – первые три буквы Вашей фамилии) с полным именем пользователя и правом на подключение с 10 до 15 часов с понедельника по среду при обязательном вводе пароля. Убедитесь, что учетная запись создана.
3. Измените системную дату и попробуйте зайти под созданной учетной записью. Сделайте выводы.
4. Заблокируйте созданную запись inforXXX.
5. Просмотрите информацию о пользователе inforXXX.

6. Создайте пользователя infor1XXX: задайте времени подключения с 8 до 15 часов в понедельник, с 10 до 12 часов в среду и с 12 до 15 часов со среды по пятницу, добавьте комментарий «Этот пользователь молодец», использование пароля обязательное, пароль – 1111 и действительное имя – Главный.

7. Сделайте недействительную учетную запись спустя три дня после ее создания.

8. Задайте основной каталог пользователя

Создание пользовательских групп с использованием командной строки

1. Просмотрите зарегистрированные в системе группы

2. Добавьте группу IBXXX

3. Добавьте в созданную группу пользователя inforXXX. Проверьте результат

4. Выведи пользователей, входящих в группу Пользователи

5. Добавьте комментарий к группе IBXXX: Информационная безопасность. Просмотрите внесенные изменения.

6. Удалите группу с именем своей фамилии.

Разграничение доступа к объектам

1. Создайте текстовый файл

2. Зайдите в свойства данного файла и перейдите на вкладку «Безопасность».

3. Просмотрите назначенные права и нажмите кнопку «Добавить»

4. Введите пользователя infor1 и нажмите кнопку «Проверить имя»

5. Запретите полный доступ пользователю к данному файлу.

6. Нажмите кнопку «Дополнительно» и далее «Изменить».

7. Разрешите данному пользователю просматривать атрибуты.

8. Проверить выполненные действия.

9. Создайте папку. Разграничьте к ней доступ пользователя – пользователь может только создавать другие папки в текущей папке.

10. Используя командную строку:

10.1. Просмотрите атрибуты созданного текстового файла

10.2. Открыть пользователю infor1 право на чтение

10.3. Открыть полный доступ к файлу для текущего пользователя

10.4. Запретить полный доступ к файлу

10.5. Назначить права на чтение и запись файла.

Лабораторная работа №2

1) Создание локальной группы

1. Зайдите в систему под следующими данными:

login – root

password - 12345

2. Добавьте группу - infor

3. Используя файл group в каталоге /etc, проверьте что новая группа была создана.

2) Создание учетной записи

1. Добавьте нового пользователя с именем вашей фамилией и добавьте ее в созданную группу.

2. Добавьте пароль пользователя – 1111.

3. Убедитесь в том, что пользователь добавлен в группу.

4. Добавьте созданного пользователя в группу root

3) Назначение прав доступа

1. Перейдите в каталог /

2. Просмотрите содержимое данного каталога

3. Опишите права доступа для home, lost+found, sbin

4. Создайте папку в домашнем каталоге

5. Используя пример №2, лишите остальных пользователей всех прав на созданный каталог. Проверьте выполненные действия.

6. Используя пример №3, добавьте для группы и остальных пользователей право на чтение. Проверьте выполненные действия.

7. Используя знаки «+» и «-», добавьте для группы и остальных пользователей право на выполнение и отмените для остальных пользователей право на чтение.

8. Путем копирования присвойте такие же права группе, что и у создателя (владельца).

9. Используя цифровое представление, назначьте следующие права:

Владелец – все права;

Группа – запрещено выполнение;

Остальные пользователи – читать и выполнять.

Лабораторная работа №3

Ознакомьтесь с устройствами инженерно-технической защиты и заполните следующую таблицу:

Название устройства	Краткое описание	Изображение

Сопоставьте устройство с его описанием:

Спектр МК	Предназначен для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, совещаний
СРМ 700 универсальный прибор	Детектор поля предназначен для обнаружения и локализации радио излучающих специальных технических средств (РСТС) негласного получения информации
ST 007	Комплекс располагает векторным анализатором для излучения спектральных, временных и модуляционных характеристик радиосигналов в реальном времени
МОЗАЙКА (ПК+)	Предназначен для проведения мероприятий по обнаружению и локализации специальных технических средств негласного съема информации, а также для контроля качества защиты информации
ST 031 «ПИРАНЬЯ»	Предназначен для прослушивания крос панелей, телефонной линии, модемов, прослушивания линий ЛВС, позволяет прослушивать речевую информацию сквозь стену

Опишите порядок регистрации в системе с использованием системы «Соболь»

Лабораторная работа №4

Загрузить редактор Шаблона безопасности, редактировать шаблон безопасности и сохранить его с новым именем.

1) Загрузка оснастки Шаблоны безопасности.

1. Откройте консоль MMS и добавьте оснастку «Шаблоны безопасности»

2. Для просмотра значений имеющихся шаблонов в окне оснастки откройте узел Шаблоны безопасности. Опишите шаблоны безопасности, входящие в состав ОС по умолчанию в виде таблицы:

Имя шаблона	Назначение

3. Опишите структуру шаблона в виде таблицы:

Раздел шаблона	Состав раздела, краткое описание
Политика учетных записей	
Локальная политика	

2) Редактирование и сохранение шаблона безопасности.

1. Щелкните на одном шаблоне безопасности compatws

2. Отредактируйте значение параметров данного шаблона и сохраните его под своей фамилией:

Политика паролей:

Политика	Параметры компьютера
Максимальный срок действия пароля	30
Минимальный срок действия пароля	10
Требовать неповторяемость паролей	2

Политика блокировки учетных записей:

Политика	Параметры компьютера
Пороговое значение блокировки	2
Блокировка учетной записи на	2
Сброс счетчика блокировки через	1

Для импорта созданного шаблона необходимо:

1) Открыть оснастку «Локальные параметры безопасности»
2) В контекстном меню корня консоли выбрать пункт «Импорт политики»
3) В открывшемся окне выбрать свой шаблон безопасности.

Завершите сеанс и попробуйте зайти под любой активной учетной записью с неправильным вводом пароля до момента блокировки. Сделайте выводы.

Освоить средства определения политики безопасности:

- Открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности);
- Установить заголовок «Добрый день» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»;
- Установить текст «На этом компьютере могут работать только зарегистрированные пользователи!» в качестве значения параметра «Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»;
- Установить значение «7 дней» для параметра «Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее»;
- Сделать активной учетную запись «Гость»;
- Разрешить форматировать и извлекать съемные носители созданным пользователям в лабораторной работе №1.

Создание ограниченной групповой политики

Ограниченная групповая политика (Restricted Group Policy) позволяет Вам определить, кто будет принадлежать к определенной группе безопасности. Когда шаблон (или политика), определяющая ограниченные группы применена к системе, Диспетчер настройки безопасности добавит членов в группу и удалит членов из нее, что гарантирует актуальное членство в группах согласно параметрам, определенным в шаблоне безопасности или политике. В этом упражнении Вы определите ограниченную групповую политику для локальной группы Администраторы в дополнение к ограниченной Групповой политике, которая уже определена для локальной группы Опытные пользователи (Power Users) в Securews.inf.

Для создания ограниченной Групповой политики

1. На панели слева щелкните правой кнопкой мыши элемент Группы с ограниченным доступом (Restricted Groups) и выберите Добавить группу (Add Group).

2. В качестве имени группы введите IBXXX и нажмите OK.

3. Дважды щелкните IBXXX на панели справа.

Теперь вы можете определить, кто будет членом локальной группы, а также определить другие группы, членом которых может быть группа.

4. Щелкните Добавить (Add), а затем щелкните Обзор (Browse). Появится диалоговое окно Выбор: Пользователи или Группы (Select Users or Groups).

5. Выберите пользователя с вашем именем в диалоговом окне Выбор: Пользователи или Группы (Select Users or Groups). Щелкните кнопку Добавить (Add).

6. Щелкните OK и затем еще дважды щелкните OK.

Когда шаблон безопасности Securews будет использован для настройки системы Windows, ограниченная групповая политика установит, что только локальный пользователь Администратор может принадлежать к локальной группе Администраторы. В процессе конфигурирования диспетчер настройки безопасности удалит всех прочих пользователей, принадлежащих к группе Администраторы на момент конфигурирования. Подобным образом, если на момент настройки пользователь Администратор не является участником группы Администраторы, Диспетчер настройки безопасности добавит пользователя Администратор в группу Администраторы.

• Список "Члены этой группы" пуст (If the Members list is empty) – Если в качестве членов определенной ограниченной группы никакие пользователи не определены (верхнее окно пустое), то когда шаблон будет использован для настройки систем, Диспетчер настройки безопасности удалит всех текущих членов этой группы.

• Список "Эта группа является членом в" пуст (If the Member of list is empty) – если в качестве члена ограниченной группы никакая группа не определена (нижнее окно пустое), действия для регулирования членства в других группах выполняться не будут.

Настройка разрешений для файловой системы

Securews также можно использовать для настройки разрешений доступа к каталогам файловой системы.

1. Щелкните правой кнопкой мыши элемент Файловая система (File System) в панели слева и нажмите Добавить файл (Add File).

2. Выберите каталог %systemroot%\repair. Нажмите OK.

Появится редактор Списка контроля доступа (Access Control List, ACL). Это позволит Вам в шаблоне Securews.inf задать разрешения для каталога %systemroot%\repair.

3. Выберите группу Все (Everyone) в верхней панели и откройте общий доступ.

4. Снимите флажок Переносить наследуемые от родительского объекта разрешения на этот объект (Allow inheritable permissions from parent to propagate to this object).

5. Для подкаталогов и файлов каталога repair, все списки ACL Администраторов настроены на наследование разрешений полного контроля от своего родительского объекта. При этом текущие настройки значения не имеют. Вы определили это, когда выбрали режим Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения (Replace existing permission on all subfolders and files with inheritable permissions).

6. Щелкните OK, чтобы разрешить доступ к каталогу только членам группы Администраторы.

Чтобы сохранить Ваш измененный файл Securews.inf:

1. Щелкните правой кнопкой мыши по шаблону Securews.inf, выберите Сохранить как (Save As) и введите Mysecurews. Нажмите Сохранить (Save).

2. Нажмите кнопку Закрыть (Close) в правом верхнем углу окна, чтобы выйти из оснастки Шаблоны безопасности.

3. Нажмите Да (Yes), чтобы сохранить параметры консоли.

Примените отредактированный шаблон в системе.

Использование команды net accounts.

1 Просмотрите информацию о параметрах политики учетных записей

2 Установите минимальную длину пароля, равную 5

3 Разрешить пользователю менять пароль не чаще, чем раз в 10 дней, принудительно изменять пароль раз в 20 дней, а также задать 10-минутное ожидание перед принудительным отключением с отправкой сообщения.

4 Запретите пользователям повторное использование пяти последних паролей.

Лабораторная работа №5

1 Ознакомиться с теоретическими сведениями

2. Запустите консоль MMC и добавьте оснастку «Анализ и настройка безопасности»

3. Создайте базу данных Mysec на основе шаблона Mysecurews

4. Щелкните правой кнопкой мыши на пункте «Анализ и настройка безопасности» и выберите «Анализ компьютера..». Укажите путь к журнала и нажмите кнопку «ОК»

5. Просмотрите политику учетных записей. Сделайте выводы.

6. Просмотрите параметры безопасности. Выберите политику состояния учетной записи «Гость». Включите данную политику.

7 Установите для политики «Напоминать пользователям об истечении срока действия пароля» значение в базе, соответствующее параметру компьютеру.

8. Раскройте пункт «Файловая система» и выберите каталог repair.

9. Откройте диалоговое окно «Свойства» данного каталога. Далее откройте окна «Безопасность базы данных» и «Последний анализ безопасности» кнопками Показать и Изменить безопасность

Видно, что DACL (Discretionary Access Control List – избирательный список контроля доступа) отличаются, поэтому каталог обозначен как несоответствующий (красный X).

10 Откройте свой шаблон безопасности измените некоторые его параметры по своему усмотрению.

11. Щелкните правой кнопкой мыши на пункте «Анализ и настройка безопасности» и выберите «Настройка компьютера». Укажите путь к журнала.

12. Нажмите ОК. Система будет настроена согласно параметрам, которые определены в шаблоне.

13. Закройте оснастку и сохраните ее под именем IB.

14. Используя командную строку, введите команду gpedit.msc. Последователь раскройте: Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Политика учетных записей – Политика паролей.

Данные, отображаемые на экране, соответствуют данным шаблона безопасности.

15. Используя команду secedit:

15.1 Проверьте синтаксис своего шаблона безопасности при его импорте в базу данных или применении к системе.

15.2. Проведите анализ безопасности системы с использованием своего шаблона, путь к файлу журнала – c:\journal.txt

15.3. Настройте безопасность системы на основе Вашего шаблона, область безопасности – реестр, путь к файлу журнала – c:\journal1.txt.

15.4. Обновите параметры безопасности.

Лабораторная работа №6

1 Ознакомиться с теоретическими сведениями

2. Используя мастер Архивации и восстановления, создайте архив папки, которую необходимо предварительно создать на диске C:. Архив расположите в папке Мои документы. Имя архива – Мой архив. Тип архива – разностный.

3 Заполните следующую таблицу:

Тип архивирования	Описание

4 Параметры архивации – проверять данные после архивации. Заполните следующую таблицу:

Параметр архивирования	Описание

5 Выберите возможность – заменить существующие архивы.

6 Запланировать архивирование со следующими параметрами:

Назначить задание	Ежемесячно
Время начала	10:00
Расписание по месяцам:	По последним понедельникам месяца
Месяца	Все кроме, декабря

7 Укажите пароль администратора

8. Повторите вышеперечисленные действия с указанием своих параметров. Единственное – время архивирование: сейчас.

9. Результирующее окно архивации и отчет включите в отчет по работе.

10 Удалите исходную папку. Используя архив, восстановите папку.

Восстановить файлы в	Исходное размещение
Способ восстановления	Заменить существующий файл

11 Результирующее окно восстановления и отчет включите в отчет по работе.

Лабораторная работа №7

Включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

Для включения режима шифрования выполните следующие действия.

1. Укажите файл (например, создайте файл шифр.txt в папке Мои документы), которую требуется зашифровать, и вызовете контекстное меню «Свойства».

2. В появившемся окне свойств на вкладке Общие нажмите кнопку Дополнительно. Появится окно диалога Дополнительные атрибуты.

3. В группе Атрибуты сжатия и шифрования установите флажок Шифровать содержимое для защиты данных и нажмите кнопку «ОК».

4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки, в появившемся окне диалога укажите режим шифрования: только к этому файлу.

Внимание! После выполнения этих действий файл с Вашей информацией будет автоматически зашифровываться. Просмотр его на другой ПЭВМ будет невозможен.

5. Заново откройте свойства документа. Далее «Дополнительные атрибуты». Нажмите кнопку «Подробно». Просмотрите подробности шифрования.

6. Нажмите кнопку «Добавить». Ознакомьтесь с окном «Выбор пользователя». Далее нажмите кнопку «Просмотр сертификата».

Ознакомьтесь со сведениями о сертификате, составе (в отчете опишите все поля сертификата) и пути. Заполните таблицу:

Кому выдан	
Действителен	
Алгоритм подписи	
Открытый ключ	
Алгоритм отпечатка	
Серийный номер	
Отпечаток	
Поставщик	

7. Задайте понятное имя и описание сертификата в окне «Свойства сертификата».

Создайте резервную копию Сертификата средствами Windows.

Примечание. Резервная копия сертификата необходима для расшифровки данных после переустановки операционной системы или для просмотра зашифрованной информации на другой ПЭВМ.

Внимание! Перед переустановкой операционной системы обязательно создайте копии Сертификатов, так как после переустановки Вы не сможете расшифровать информацию.

Для создания резервной копии сертификата выполните следующие действия.

1. Откройте консоль управления mmc.

2. В меню Консоль выберите оснастку «Сертификаты», установите переключатель в положение «Учетной записи компьютера» и нажмите кнопку Далее.

3. На следующем шаге необходимо выбрать - локальным компьютером

4. В левом подокне оснастки Сертификаты откройте папку Доверенные корневые сертификаты, а затем папку Сертификаты. В правом подокне появится список сертификатов.

5. Просмотрите свойства любого на Ваш выбор сертификата. Напишите для каких целей предназначен сертификат, кем и когда выдан.

6.Экспортируйте данный сертификат с использованием мастера, указав:

- Формат файла – файлы в DER кодировке;
- Имя файла – любое.

7. Просмотреть экспортированный сертификат.

8. Импортировать сохраненный сертификат в папку «Личные».

9. Экспортируйте сертификат, созданный при шифровании файла. Из группы «Доверенные лица», выбрав следующие значения:

- Да, экспортировать закрытый ключ;
- В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку Далее.
- В следующих окнах сообщите пароль (например, 11), защищающий данные файла сертификатах, а также путь сохранения файла (запишите путь к папке, в которой Вы сохранили копию Сертификата) сертификатах.

Завершите работу Мастера экспорта сертификата нажатием кнопки ОК в окне диалога, сообщающем об успешном выполнении процедуры экспорта.

В результате сертификат и секретный ключ будут экспортированы в файл с расширением *.pfx, который может быть скопирован на гибкий диск и перенесен на другой компьютер или использован после переустановки операционной системы.

Импортируйте созданный сертификат в папку Доверенные корневые сертификаты.

Поясните, как изменилось состояние сертификата.

Используя командную строку, выведите справку о команде cipher

1.Используя команду cipher и ключи U и N, просмотрите файлы, которые зашифрованы в системе

2.Создайте агент восстановления.

3.После этого необходимо от имени администратора открыть оснастку "Локальные параметры безопасности" (secpol.msc), выделить пункт "Политики открытого ключа - Файловая система EFS" и в меню "Действие" выбрать "Добавить агент восстановления данных". Откроется "Мастер добавления агента восстановления", на второй странице которого необходимо нажать кнопку "Обзор папок" и указать файл *.cer, созданный программой cipher в п. 3.6. Добавьте также этот сертификат в группу Доверенные корневые сертификаты.

4.Создайте новый ключ шифрования. Отразите его в отчете

5.Создайте еще один текстовый файл и зашифруйте его при помощи команды cipher.

6.Поместить его в отдельную созданную папку, которую тоже зашифруйте.

7.Проверьте зашифрована ли папка.

8.Создайте еще одну папку и в ней - еще несколько файлов, начинающихся с одинаковой буквы. Зашифруйте их одной командой.

Лабораторная работа №8

1. Ознакомитесь с основными теоретическими сведениями и ответьте на вопросы:
2. Выполните задание

Задание 1. Создайте новую политику IP-безопасности на локальном компьютере:

1. Откройте оснастку Управление политикой безопасности IP:

2. Активизируйте оснастку Политика безопасности IP на «Локальный компьютер». Справа отобразятся установленные по умолчанию политики.
3. Запустите мастер создания политик безопасности:
   - вызовите контекстное меню оснастки Политика безопасности IP на «Локальный компьютер»
   - выполните команду Создать политику безопасности IP….
4. Ознакомьтесь с информацией мастера и щелкните по кнопке Далее.
5. Установите Имя политики безопасности IP:
   - введите в поле Имя – My_politic.
   - введите в поле Описание – Это политика IP безопасности локального компьютера
6. Настройте политику безопасного соединения. Для этого установите флажок Использовать правило по умолчанию
7. Установите Способ проверки подлинности правила отклика по умолчанию:
   - активизируйте Использовать сертификат данного центра сертификации;
   - Выберите сертификат, созданный в лабораторной работе №6.
8. Закройте мастера создания политики безопасности кнопкой Готово.

Откроется диалоговое окно Свойства: My_politic.

9. Запустите Мастер правил безопасности и настройте правила безопасности:
   - запустите мастер кнопкой Добавить;
   - выберите Это правило не определяет туннель;
   - выберите Локальное сетевое подключения;
   - Выберите сертификат из п.7;
   - в списке фильтров IP выберите Полный IP трафик;
   - добавьте новое действие фильтра:
     - щелкните по кнопке Добавить;
     - ознакомьтесь с описанием запустившегося мастера;
     - введите в поле Имя – My_filter;
     - Поведение действия фильтра - Разрешить;
     - завершите добавление нового действия кнопкой Готово.
   - активизируйте созданное вами действие и измените его параметры:
     - щелкните по кнопке Изменить;
     - выберите Согласовать безопасность;
     - щелкните по кнопке Добавить и выберите Шифрование и обеспечение целостности;
     - установите флажок Принимать небезопасную связь, но отвечать с помощью IPSEC. Закройте свойства my_filter. Выберите созданное действие фильтра и щелкните кнопку Далее;
   - завершите работу мастер кнопкой Готово.
10. Добавьте в политику фильтр для блокировки всех входящих подключений:
    - откройте диалоговое окно Список фильтров IP кнопкой Добавить на вкладке «Список фильтров»;
    - добавьте новый фильтр:
      - сбросьте флажок Использовать мастер;
      - откройте диалоговое окно Свойства: Фильтр кнопкой Добавить;
      - в поле Адрес источника пакетов выберите Любой адрес IP;
      - в поле Адрес назначения пакетов выберите Мой IP адрес;
      - установите флажок: Отраженный для блокировки приходящих пакетов;
      - установите протокол TCP для фильтрации (вкладка Протокол);
      - завершите настройку нового фильтра кнопкой ОК;
    - закройте диалоговое окно Список фильтров IP кнопкой ОК.
    - Выберите из списка созданный фильтр;

- завершите добавление нового правила кнопкой ОК.

11. Закройте диалоговое окно Свойства: My_politic.

12. Активизируйте выбранную политику (контекстное меню созданной политики/Назначить).

б) критерии оценивания

При оценке знаний на защите лабораторной работы учитывается:

1. Уровень сформированности компетенций.
2. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
3. Уровень знания фактического материала в объеме программы.
4. Логика, структура и грамотность изложения вопроса.
5. Умение связать теорию с практикой.
6. Умение делать обобщения, выводы.

№ п/п	Оценка	Критерии оценки
1	Отлично	Студент правильно называет метод исследования, правильно называет прибор, правильно демонстрирует методику исследования /измерения, правильно оценивает результат.
2	Хорошо	Студент правильно называет метод исследования, правильно называет прибор, допускает единичные ошибки в демонстрации методики исследования /измерения и оценке его результатов
3	Удовлетворительно	Студент неправильно называет метод исследования, но при этом дает правильное название прибора. Допускает множественные ошибки в демонстрации методики исследования /измерения и оценке его результатов
4	Неудовлетворительно	Студент неправильно называет метод исследования, дает неправильное название прибора. Не может продемонстрировать методику исследования /измерения, а также оценить результат

3. Перечень и характеристики процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Процедура проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине регламентируется локальным нормативным актом.

Перечень и характеристика процедур текущего контроля и промежуточной аттестации по дисциплине

№	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Виды вставляемых оценок	Форма учета
1.	Экзамен	Раз в семестр, по окончании изучения дисциплины	По пятибалльной шкале	Ведомость, зачетная книжка, портфолио
2.	Тест	По окончании изучения раздела дисциплины	По пятибалльной шкале	Журнал успеваемости преподавателя
3	Защита лабораторных работ	По расписанию	По пятибалльной шкале	Журнал успеваемости преподавателя

Приложение 1

Типовые вопросы к экзамену

ПК-11

1. Что такое информационная безопасность? Роль информационной безопасности при управлении проектами.
2. Перечислите основные угрозы информационной безопасности при управлении проектами.
3. Какие существуют модели информационной безопасности, используемые при верификации требований в проектах?
4. Какие методы защиты информации выделяют при выдаче и контроле поручений?
5. Что такое правовые методы защиты информации? Разработка документов. Контроль выданных поручений.
6. Что такое организационные методы защиты информации? Каково их предназначение при разработке плановой документации?
7. Что такое технические методы защиты информации? Какие инструменты и методы анализ требований могут быть использованы для организации технической защиты.
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.
13. Какие виды компьютерных угроз существуют?
14. Что такое брандмауэр? Исправление несоответствий при работе брандмауэра.
15. Что такое антивирусная программа?
16. Что такое эвристический алгоритм поиска вирусов?
17. Что такое сигнатурный поиск вирусов? Каково предназначение данного вида поиска при реализации предупреждающих действий.
18. Методы противодействия сниффингу?
19. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
20. Что такое механизм контроля и разграничения доступа?
21. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
22. Что такое средства стеганографической защиты информации?
23. Что такое инженерная защита объектов?
24. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
25. Что такое технические каналы утечки информации?
26. Перечислите основные виды технических каналов утечки информации?
27. Перечислите методы защиты информации от утечки по визуальному каналу.
28. Перечислите методы защиты информации от утечки по воздушному каналу.
29. Перечислите методы защиты информации от утечки по вибрационному каналу.
30. Перечислите методы защиты информации от утечки по индукционному каналу.
31. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
32. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
33. Что такое криптография?
34. Какие используются симметричные алгоритмы шифрования?
35. Какие используются ассиметричные алгоритмы шифрования?
36. Что такое криптографическая хеш-функция?

37. Какие используются криптографические хеш-функции?

38. Что такое цифровая подпись? Анализ входных данных для верификации цифровой подписи.

39. Что такое инфраструктура открытых ключей?

40. Какие российские и международные стандарты на формирование цифровой подписи существуют?

41. Какие основные криптографические протоколы используются в сетях?

Приложение 2

Типовые вопросы для тестирования

ПК-11

1. Что из перечисленного является составляющей информационной безопасности в области управления проектами
- нарушение целостности информации
- проверка прав доступа к информации
- доступность информации
- выявление нарушителя

2.Что из перечисленного является составляющей информационной безопасности
- нарушение целостности информации
- проверка прав доступа к информации
- конфиденциальность информации
- выявление нарушителя

3. Сколько уровней формирования режима информационной безопасности при верификации требований в проектах существует
- три
- четыре
- два
- пять

4. Какой из перечисленных уровней не относится к уровням формирования режима ИБ?
- законодательно-правовой
- информационный
- административный
- программно-технический

5. Какой из перечисленных уровней не относится к уровням формирования режима ИБ при разработке документов?
- законодательно-правовой
- конфиденциальный
- административный
- программно-технический

6. Какие из перечисленных уровней относятся к уровням формирования режима ИБ при контроле выданных поручений?
- законодательно-правовой
- конфиденциальный
- административный
- программно-технический

7. ……. - это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействии естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
- компьютерная безопасность
- информационная безопасность

- защита информации
- защита государственной тайны

8. Информационная безопасность - это …… информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействии естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

9. Информационная безопасность - это защищенность информации и поддерживающей ее ……. от случайных или преднамеренных воздействии естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

10. Что не является причиной случайных воздействий на информационную среду в соответствии с записями по качеству
- отказы и сбои аппаратуры
- ошибки персонала
- подбор пароля
- помехи в линиях связи из-за воздействия внешней среды

11. Субъект, в полном объеме реализующий полномочия пользования, распоряжения информацией в соответствии с законодательными актами и разрабатывающий плановую документацию.
- пользователь
- владелец
- собственник
- потребитель

12. Субъект, осуществляющий пользование информацией и реализующий полномочия в пределах прав, установленных законом при выдаче и контроле поручений.
- пользователь
- владелец
- собственник
- потребитель