МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.12 Информационная безопасность

программы подготовки специалистов среднего звена

09.02.04 Информационные системы (по отраслям)

Форма обучения: *очная*

Владивосток 2020

Рабочая программа учебной дисциплины *ОП.12 Информационная безопасность* разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности *09.02.04 Информационные системы (по отраслям)*, утвержденного приказом Минобрнауки России от *14 мая 2014 г., №524*, примерной образовательной программой.

Разработчик(и): *Д.А.Атабаева, преподаватель*

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от «15» апреля 2020 г.

Председатель ЦМК _____ *А.Д. Гусакова*

подпись

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы: общепрофессиональная дисциплина ОП.12 входит в профессиональный учебный цикл.

1.2 Требования к результатам освоения учебной дисциплины

В результате освоения учебной дисциплины обучающийся должен уметь:

– проводить анализ и оценку уязвимостей компьютерной системы;

– применять меры информационной безопасности процедурного уровня

– осуществлять защиту информации от несанкционированного доступа;

– настраивать безопасность почтового клиента;

– настраивать параметры аутентификации пользователей;

– осуществлять регистрацию и аудит информационной безопасности;

– настраивать системы разграничения доступа;

– применять криптографические методы и средства зашиты информации;

– использовать средства антивирусной защиты;

– использовать стандарты и спецификации информационной безопасности.

В результате освоения учебной дисциплины обучающийся должен знать:

– понятие и составляющие информационной безопасности;

– виды угроз информации и методы защиты от них;

– законы, стандарты и спецификации информационной безопасности;

– меры процедурного уровня информационной безопасности;

– меры программно-технического уровня информационной безопасности;

– методы защита информации от несанкционированного доступа;

– способы разграничения полномочий и доступа к объектам;

– осуществление регистрации и аудита в компьютерной системе;

– проведение оценки рисков компьютерной системы;

– применение средств антивирусной защиты.

В части освоения основного вида профессиональной деятельности и соответствующих компетенций:

ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 2.6	Использовать критерии оценки качества и надежности функционирования информационной системы.

1.3. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	*99*
Обязательная аудиторная учебная нагрузка (всего)	*68*
в том числе:	
теоретические занятия	*34*
практические занятия	*34*
Самостоятельная работа обучающегося (всего)	*25*
Итоговая аттестация в форме диф. зачета	

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Введение в информационную безопасность	Содержание темы: 1. Информационная безопасность. 2. Основные понятия. Модели информационной безопасности. 3. Виды защищаемой информации.	4	1
	Лабораторные работы: Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	4	2
	Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.	5	3
Тема 2. Правовое обеспечение информационной безопасности	Содержание темы: 1. Основные нормативно-правовые акты в области информационной безопасности. 2. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.	6	1
	Лабораторные работы: Использование криптографических средств защиты информации	6	2
	Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.	7	2, 3
Тема 3. Организационное обеспечение информационной безопасности	Содержание темы: 1. Основные стандарты в области обеспечения информационной безопасности. 2. Политика безопасности. 3. Экономическая безопасность предприятия.	6	1
	Лабораторные работы: Реализация работы инфраструктуры открытых ключей	6	2
	Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.	5	2, 3
Тема 4. Технические средства и методы защиты информации	Содержание темы: 1. Инженерная защита объектов. 2. Защита информации от утечки по техническим каналам.	8	1
	Лабораторные работы: Средства стеганографии для защиты информации	8	2
	Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.	7	2, 3

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Содержание темы: 1. Основные виды сетевых и компьютерных угроз. 2. Средства и методы защиты от сетевых компьютерных угроз.	6	1
	Лабораторные работы: Настройка безопасного сетевого соединения	6	2
	Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.	3	2, 3
Тема 6. Криптографические методы защиты информации	Содержание темы: 1. Симметричные и ассиметричные системы шифрования. 2. Цифровые подписи (Электронные подписи). 3. Инфраструктура открытых ключей. 4. Криптографические протоколы.	4	1
	Лабораторные работы: Антивирусные средства защиты информации	4	2
	Самостоятельная работа осуществляется выполнением заданий по текущему контролю и сдачей промежуточного контроля.	2	2, 3

Уровни освоения учебного материала:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории информационных систем. Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя.

Технические средства обучения:

а) программное обеспечение: БД Консультант плюс, OpenSSL, TrueCrypt, ImageSpy, OpenVPN, MS Office, демоверсии VipNet client, SecretNet

б) компьютеры с лицензионным программным обеспечением и мультимедийное оборудование.

3.2. Информационное обеспечение реализации программы (перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы)

3.2.1. Основные источники

1. Технические средства информатизации : учебник / В.П. Зверева, А.В, Назаров. — Москва : КУРС, НИЦ ИНФРА-М, 2017. - 256 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/615331

2. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - Москва : Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-627-0 - Текст : электронный. - URL: https://new.znanium.com/catalog/product/516806

3. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с. — (Профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/775200

4. Основные положения информационной безопасности : учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2017. — 208 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/927190

5. Безопасность и управление доступом в информационных системах : учеб. пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2017. — 368 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/537054

6. Участие в планировании и организации работ по обеспечению защиты информации: учебник / В.П. Зверева, А.В. Назаров. — Москва : КУРС: ИНФРА-М, 2017. — 320 с. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/635130

7. Компьютерные сети : учеб. пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2017. — 464 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/792686

8. Программное обеспечение компьютерных сетей : учеб. пособие / О.В. Исаченко. — Москва : ИНФРА-М, 2017. — 117 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/851518

3.2.2. Дополнительные источники

1. Дискретная математика : учебник / А.И. Гусева, В.С. Киреев, А.Н. Тихомирова. — Москва : КУРС: ИНФРА-М, 2017. — 208 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/910991

2. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. - Москва : КУРС; ИНФРА-М, 2017. — 360 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/952085

3. Технические средства информатизации: учебник / В.П. Зверева, А.В. Назаров. – Москва : КУРС: ИНФРА–М, 2017. – 248 с. – (Среднее профессиональное образование) - Текст : электронный. - URL: https://new.znanium.com/catalog/product/752310

4. Введение в специальность программиста : учебник / В.А. Гвоздева. — 2-е изд., испр. и доп. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 208 с. — (Профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/552523

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1 Контроль и оценка

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Контроль усвоения дисциплины осуществляется в виде текущей, промежуточной аттестации по результатам которых формируется итоговая оценка по дисциплине. Контроль осуществляются с использованием организационных форм и количественных показателей контроля (баллов), закрепленных для данной дисциплины.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
проводить анализ и оценку уязвимостей компьютерной системы	Текущий контроль в форме: выполнения и защиты практического задания, самостоятельной работы
применять меры информационной безопасности процедурного уровня	
осуществлять защиту информации от несанкционированного доступа	
настраивать безопасность почтового клиента	
настраивать параметры аутентификации пользователей	
осуществлять регистрацию и аудит информационной безопасности	
настраивать системы разграничения доступа	
применять криптографические методы и средства зашиты информации	
использовать средства антивирусной защиты	
использовать стандарты и спецификации информационной безопасности	
Знания:	
понятие и составляющие информационной безопасности	Текущий контроль в форме: выполнения и защиты практического задания, самостоятельной работы. Экспертное наблюдение и оценка деятельности обучающегося в процессе освоения образовательной программы на практических занятиях, в ходе компьютерного тестирования, подготовки электронных презентаций, при выполнении индивидуальных домашних заданий Итоговый контроль (диф. зачет) контрольная работа
виды угроз информации и методы защиты от них	
законы, стандарты и спецификации информационной безопасности	
меры процедурного уровня информационной безопасности	
меры программно-технического уровня информационной безопасности	
методы защита информации от несанкционированного доступа	
способы разграничения полномочий и доступа к объектам	
осуществление регистрации и аудита в компьютерной системе	
проведение оценки рисков компьютерной системы	
применение средств антивирусной защиты	

4.2. Контроль и оценка результатов развития общих компетенций и обеспечивающих их умений

Результаты (освоенные общие компетенции)	Основные показатели результатов подготовки	Формы и методы контроля
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	понимание сущности и социальной значимости своей будущей профессии, проявление к ней устойчивого интереса	Наблюдение и оценка деятельности учащихся при проведении учебно-воспитательных мероприятий профессиональной направленности
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	мотивированное обоснование выбора и применения методов и способов выполнения поставленной задачи, объективная оценка своей работы.	Наблюдение и оценка активности учащихся при проведении учебно-воспитательных мероприятий профессиональной направленности.
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	умение принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	Наблюдение и оценка деятельности учащихся при проведении учебно-воспитательных мероприятий профессиональной направленности
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	оперативность поиска и использования необходимой информации для качественного выполнения профессиональных заданий, профессионального и личностного развития	Наблюдение и оценка результатов деятельности обучающегося в процессе освоения образовательной программы на практических и семинарских занятиях, при выполнении внеаудиторных самостоятельных работ, рефератов.
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	демонстрация умения оперативно осуществлять операции, предлагаемые преподавателем, делать анализ и давать оценку полученной информации, в т.ч. и с использованием программного обеспечения	Экспертное наблюдение и оценка деятельности обучающегося в процессе освоения образовательной программы на практических занятиях, в ходе компьютерного тестирования, подготовки электронных презентаций, при выполнении индивидуальных домашних заданий.
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	коммуникабельность при взаимодействии с обучающимися и преподавателями в ходе обучения.	Экспертное наблюдение и оценка коммуникативной деятельности обучающегося в процессе освоения образовательной программы на практических занятиях, при выполнении индивидуальных домашних заданий. Наблюдение и оценка использования учащихся коммуникативных методов и приемов при подготовке и проведении учебно-воспитательных мероприятий различной тематики.
ОК. 7 Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	умение брать ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	Экспертное наблюдение и оценка использования учащимися методов и приемов личной организации при подготовке и проведении учебно-воспитательных мероприятий различной тематики. Экспертное наблюдение и оценка динамики достижений учащихся в учебной и общественной деятельности.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение	способность к организации и планированию самостоятельных занятий при изучении дисциплины. демонстрация потребности в получении дополнительных знаний, возможностей	Экспертное наблюдение и оценка использования учащимися методов и приемов личной организации в процессе освоения образовательной программы на практических занятиях, при выполнении индивидуальных домашних заданий. Экспертное наблюдение и оценка использования

квалификации.	самореализации	учащимися методов и приемов личной организации при подготовке и проведении учебно-воспитательных мероприятий различной тематики. Экспертное наблюдение и оценка динамики достижений учащихся в учебной и общественной деятельности.
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	проявление интереса к инновациям в области профессиональной деятельности	Наблюдение и оценка результатов деятельности обучающегося в процессе освоения образовательной программы на практических и семинарских занятиях, при выполнении внеаудиторных самостоятельных работ, рефератов

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И СЕРВИСА

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине
ОП.12 Информационная безопасность

программы подготовки специалистов среднего звена
09.02.04 Информационные системы (по отраслям)

Форма обучения: *очная*

Владивосток 2020

Контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине *ОП.12 Информационная безопасность* разработаны в соответствии с требованиями ФГОС СПО по специальности *09.02.04 Информационные системы (по отраслям)*, утвержденного приказом Минобрнауки РФ от *14 мая 2014 г., №524*, примерной образовательной программой, рабочей программой учебной дисциплины.

Разработчик: Д.А.Атабаева*, преподаватель*

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от «15» апреля 2020 г

Председатель ЦМК _____ *А.Д. Гусакова*

1 Общие сведения

Контрольно-оценочные средства (далее – КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП.12 «информационная безопасность».

КОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта (с использованием оценочного средства - устный опрос в форме собеседования, выполнение лабораторных заданий)

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК[1]	Код результата обучения[1]	Наименование результата обучения[1]
ОК 1-9 ПК 2.6	З1	Сущность и понятие информационной безопасности, характеристику ее составляющих
	З2	Место информационной безопасности в системе национальной безопасности страны
	З3	Источники угроз информационной безопасности и меры по их предотвращению
	З4	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи
	З5	Современные средства и способы обеспечения информационной безопасности
	У1	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
	У2	Применять основные правила и документы сертификации Российской Федерации
	У3	Классифицировать основные угрозы безопасности информации

[1]- *в соответствии с рабочей программой учебной дисциплины*

3 Соответствие оценочных средств контролируемым результатам обучения

3.1 Средства, применяемые для оценки уровня теоретической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель[2] овладения результатами обучения	Наименование оценочного средства и представление его в КОС[3]	
			Текущий контроль[4]	Промежуточная аттестация[4]
Тема 1.1 СРС по Теме 1.1	З1	понятие и составляющие информационной безопасности; виды угроз информации и методы защиты от них;	Устный опрос (п. 5.1, Тема 1, вопросы 1-17)	Вопросы на экзамен 1-7 (п. 6.1)
	З2	способность классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; перечислить основные цели и задачи РФ в области обеспечения информационной безопасности; перечислить и рассказать федеральные законы в области защиты информации	Устный опрос (п. 5.1, Тема 1, вопросы 17-34)	Вопросы на экзамен 8-15 (п. 6.1)
	У1	проводить анализ и оценку уязвимостей компьютерной	Лабораторная работа №1 (п.	

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель[2] овладения результатами обучения	Наименование оценочного средства и представление его в КОС[3]	
			Текущий контроль[4]	Промежуточная аттестация[4]
		системы; применять меры информационной безопасности процедурного уровня	5.3)	
Тема 1.2 СРС по Теме 1.2	З2	законы, стандарты и спецификации информационной безопасности; меры процедурного уровня информационной безопасности; меры программно-технического уровня информационной безопасности;	Устный опрос (п. 5.1, Тема 2, вопросы 1-23)	Вопросы на экзамен 16-31 (п. 6.1)
	У2	осуществлять защиту информации от несанкционированного доступа; настраивать параметры аутентификации пользователей;	Лабораторная работа №2 (п. 5.3)	
Тема 1.3 СРС по Теме 1.3	З3	методы защита информации от несанкционированного доступа; способы разграничения полномочий и доступа к объектам;	Устный опрос (п. 5.1, Тема 1, вопросы 1-23)	Вопросы на экзамен 32-40 (п. 6.1)
	У3	осуществлять регистрацию и аудит информационной безопасности; настраивать системы разграничения доступа;	Лабораторная работа №3 (п. 5.3)	
Тема 1.4 СРС по Теме 1.4	З4	осуществление регистрации и аудита в компьютерной системе;	Устный опрос (п. 5.1, Тема 4, вопросы 1-23)	Вопросы на экзамен 41-49 (п. 6.1)
	З5	проведение оценки рисков компьютерной системы;	Устный опрос (п. 5.1, Тема 4, вопросы 24-47)	
	У4	применять криптографические методы и средства зашиты информации; использовать стандарты и спецификации информационной безопасности	Лабораторная работа №4 (п. 5.3)	
Тема 1.5 СРС по Теме 1.5	З6	применение средств антивирусной защиты.	Устный опрос (п. 5.1, Тема 5, вопросы 1-25)	Вопросы на экзамен 50-54 (п. 6.1)
	У5	использовать средства антивирусной защиты;	Лабораторная работа №5 (п. 5.3)	

3.2 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Тема 1.1 Практическое занятие № 1	З1	Знать требования к защите информации определенного типа	Лабораторная работа №1 (п. 5.3)	Вопросы на экзамен 1-15 (п. 6.1)
	У1	Классификация защищаемой информации по видам тайны и степеням конфиденциальности; проведение анализа защищенности объекта защиты информации в зависимости от содержания информации и степени ее конфиденциальности		
	П1	Выполнять настройку компонентов подсистем безопасности		
Тема 1.2 Практическое занятие № 2	З2	основные функции, назначение и принципы работы распространенных операционных систем и сред	Лабораторная работа №2 (п. 5.3)	Вопросы на экзамен 16-31 (п. 6.1)
	У2	Описание объекта защиты; проведение анализа защищенности объекта защиты информации по видам угроз, характеру происхождения угроз, классам каналов несанкционированного получения информации, источникам появления угроз;		
Тема 1.3 Практическое занятие № 3	З3	общие принципы построения алгоритмов, основные алгоритмические конструкции	Лабораторная работа №3 (п. 5.3)	Вопросы на экзамен 32-40 (п. 6.1)
	У3	Определение типов потенциальных нарушителей; описание модели потенциального нарушителя; использовать языки программирования.		
Тема 1.4 Практическое занятие № 4	З4	базовые системные программные продукты и пакеты прикладных программ	Лабораторная работа №4 (п. 5.3)	Вопросы на экзамен 41-49 (п. 6.1)
	У4	осваивать и использовать базовые системные программные продукты и пакеты прикладных		

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
		программ		
Тема 1.5 Практическое занятие № 5	З5	Современные средства и способы обеспечения информационной безопасности	Лабораторная работа №5 (п. 5.3)	Вопросы на экзамен 50-54 (п. 6.1)
	У5	Выбрать наиболее подходящую программу для защиты информации от несанкционированного доступа		

4 Описание процедуры оценивания

Уровень образовательных достижений обучающихся по дисциплине оценивается по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом.

Критерии оценивания устного ответа

оценочные средства: устное сообщение.

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием

логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

оценочные средства: письменный отчет по лабораторной работе.

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии выставления оценки студенту на зачете/ экзамене

оценочные средства: устный опрос в форме ответов на вопросы.

Оценка по промежуточной аттестации	Характеристика уровня освоения дисциплины
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на итоговом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на среднем уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в

	изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже базового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

Тема 1. Введение в информационную безопасность

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
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. Право. Источники права.
14. Какие основные законы в области защиты информации в РФ?
15. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
16. Стратегия национальной безопасности. Доктрина информационной безопасности.
17. Что такое конфиденциальная информация?
18. Что такое персональные данные?
19. В каких случаях возможно использовать персональные данные без согласия обладателя?
20. Охарактеризуйте биометрические данные как персональные данные.
21. Что такое профессиональная тайна?
22. Что такое служебная тайна?
23. Что такое коммерческая тайна?
24. Что такое режим коммерческой тайны?
25. Что такое государственная тайна?
26. Опишите правовой режим государственной тайны.
27. ФЗ-149.
28. ФЗ-152.
29. ФЗ-98.
30. ФЗ-390.
31. ФЗ-395-1.
32. ФЗ-126.
33. ФЗ-374 и ФЗ-375.
34. Постановление правительства №1119.

Тема 2. Правовое обеспечение информационной безопасности

1. Какие основные международные стандарты в области информационной безопасности?
2. "Оранжевая книга"
3. ISO/IEC 15408.
4. Как связаны международные стандарты и стандарты РФ?
5. ГОСТ Р ИСО/МЭК 27002-2012.
6. ГОСТ Р ИСО/МЭК 27005-2010.
7. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
8. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
9. Приказ ФСБ №378.
10. Приказ ФСТЭК №21.
11. Приказ ФСТЭК №17.
12. Приказ ФСТЭК №31.
13. Приказ ФСТЭК №28.
14. Приказ ФСТЭК №638.
15. Приказ ФСТЭК №9.
16. Приказ ФСТЭК №119.
17. Приказ Гостехкомиссии №114.
18. Руководящие документы Гостехкомиссии.
19. Меры защиты информации в государственных информационных системах. (Методический документ ФСТЭК).
20. Что такое политика безопасности?
21. Служба безопасности предприятия. Структура. Функции.
22. Типовая инструкция сотрудника по обеспечению информационной безопасности.
23. Экономическая разведка. Промышленный шпионаж.

Тема 3. Организационное обеспечение информационной безопасности

1. Что такое инженерная защита объектов?
2. Каким способом описывается инженерная защита. Описать модель.
3. Какие средства применяются для защиты 1-го периметра?
4. Какие средства применяются для защиты 2-го периметра?
5. Какие средства применяются для защиты 3-го периметра?
6. Пожарные сигнализации.
7. Охранные сигнализации
8. Биометрия. Биометрические характеристики.
9. Что такое технические каналы утечки информации?
10. Перечислите основные виды технических каналов утечки информации?
11. Что такое спецпроверка?
12. Что такое специсследование?
13. Что такое спецобследование?
14. Перечислите методы защиты информации от утечки по зрительному каналу.
15. Перечислите методы защиты информации от утечки по электромагнитному каналу.
16. Перечислите методы защиты информации от утечки по электрическому каналу.
17. Перечислите методы защиты информации от утечки по индукционному каналу
18. Перечислите методы защиты информации от утечки по параметрическому каналу.
19. Перечислите методы защиты информации от утечки по воздушному каналу.
20. Перечислите методы защиты информации от утечки по вибрационному каналу.
21. Перечислите методы защиты информации от утечки по акустоэлектрическому каналу.
22. Перечислите методы защиты информации от утечки по оптикоэлектронному каналу.
23. Перечислите средства и методы защиты информации от утечки информации в телефонных линиях.

Тема 4. Технические средства и методы защиты информации

1. Что такое программно-аппаратные средства защиты информации?
2. Какие механизмы реализуют программно-аппаратные средства защиты информации?
3. Какие компьютерные угрозы безопасности существуют?
4. Что такое сетевая разведка? Какие методы защиты против нее существуют?
5. Что такое инъекция? Какие виды инъекций существуют? Какие методы защиты против них существуют?
6. Что такое отказ в обслуживании? Какие методы защиты против него существуют?
7. Основные виды программных уязвимостей.
8. Бэкдоры.
9. Что такое переполнение буффера? Методы защиты.
10. Что такое дефекты форматных строк? Методы защиты.
11. Что такое целочисленные переполнения? Методы защиты.
12. Ошибки обработки исключений. Методы защиты.
13. Внедрение команд. Методы защиты.
14. Некорректные обработки ошибок. Методы защиты.
15. Гонки. Методы защиты.
16. Выполнение кода с завышенными привилегиями.
17. Атака "Человек по середине".
18. Что такое IP-спуффинг? Какие методы защиты против него существуют?
19. ARP.
20. DHCP.
21. NAT.
22. PAT.
23. IPv4. IPv6.
24. Что такое ARP-спуффинг? Какие методы защиты против него существуют?
25. Чтотакое DNS Cache Poisoning? Какие методы защиты против него существуют?
26. Чтотакое NetBIOS/NBNS spoofing? Какие методы защиты против него существуют?
27. VPN.
28. Социальная инженерия.
29. Фрод. Методы борьбы с фродом.
30. Что такое фишинг? Какие методы защиты против него существуют?
31. Кардинг. Методы защиты от кардинга.
32. Darkweb.
33. DMZ.
34. Анонимайзеры.
35. Прокси-серверы.
36. Резервное копирование.
37. Honey pot.
38. DLP-системы. SIEM-системы.
39. Сканеры безопасности.
40. Системы обнаружения вторжений.
41. Системы предотвращения вторжений.
42. Вредоносные программы. Компьютерные вирусы. Виды вирусов.
43. Эксплоиты.
44. Механизм работы вируса.
45. Антивирусы. Виды антивирусов.
46. Механизмы работы антивируса.
47. Межсетевой экран.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности

1. Что такое шифр? Какие виды шифров существуют?
2. Что такое симметричный шифр? Какие симметричные шифры используются сейчас?
3. Что такое ассиметричный шифр? Какие ассиметричные шифры используются сейчас?
4. Принцип построения симметричных шифров.
5. Принцип построения ассиметричных шифров.
6. Стандартные шифры.
7. Поточные шифры.
8. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
9. Дерево Меркла.
10. Что такое цифровая подпись?
11. Цифровая подпись RSA.
12. Цифровая подпись Эль-Гамаля.
13. Что такое инфраструктура открытых ключей?
14. Жизненный цикл ключа.
15. Аутентификация, идентификация, верификация, авторизация.
16. Простейшие протоколы идентификации.
17. Основной протокол Kerberos.
18. IPSec.
19. Blockchain.
20. Что такое стеганография? Понятие стеганоконтейнера.
21. Какие виды стеганоконтейнеров существуют?
22. Методы создания стеганоконтейнеров на основе текстовой информации.
23. Методы создания стеганоконтейнеров на основе видеоинформации и стоп/кадров.
24. Методы создания стеганоконтейнеров на основе аудиоинформации.
25. Цифровые водяные знаки.

5.2 Перечень тем лабораторных работ

Тема 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности
Тема 2. Использование криптографических средств защиты информации
Тема 3. Реализация работы инфраструктуры открытых ключей
Тема 4. Средства стеганографии для защиты информации
Тема 5. Антивирусные средства защиты информации

6. Примеры оценочных средств для проведения промежуточной аттестации

6.1 Экзаменационные вопросы

1. Что такое информационная безопасность?
2. Какие методы защиты информации выделяют?
3. Перечислите виды защищаемой информации.
4. Право. Источники права.
5. Какие основные законы в области защиты информации в РФ?
6. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
7. Стратегия национальной безопасности. Доктрина информационной безопасности.
8. Опишите правовой режим государственной тайны.
9. ФЗ-149.
10. ФЗ-152.
11. ФЗ-98.

12. ФЗ-390.
13. ФЗ-395-1.
14. ФЗ-126.
15. ФЗ-374 и ФЗ-375.
16. Какие основные международные стандарты в области информационной безопасности?
17. "Оранжевая книга"
18. ISO/IEC 15408.
19. Как связаны международные стандарты и стандарты РФ?
20. ГОСТ Р ИСО/МЭК 27002-2012.
21. ГОСТ Р ИСО/МЭК 27005-2010.
22. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
23. РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
24. Приказ ФСБ №378.
25. Приказ ФСТЭК №21.
26. Приказ ФСТЭК №17.
27. Приказ ФСТЭК №31.
28. Приказ ФСТЭК №28.
29. Приказ ФСТЭК №638.
30. Приказ ФСТЭК №9.
31. Приказ ФСТЭК №119.
32. Приказ Гостехкомиссии №114.
33. Руководящие документы Гостехкомиссии.
34. Меры защиты информации в государственных информационных системах. (Методический документ ФСТЭК).
35. Каким способом описывается инженерная защита. Описать модель.
36. Биометрия. Биометрические характеристики.
37. Что такое технические каналы утечки информации?
38. Что такое спецпроверка?
39. Что такое специсследование?
40. Что такое спецобследование?
41. Что такое программно-аппаратные средства защиты информации?
42. Основные виды программных уязвимостей.
43. Что такое ARP-спуффинг? Какие методы защиты против него существуют?
44. Чтотакое DNS Cache Poisoning? Какие методы защиты против него существуют?
45. Механизм работы вируса.
46. Антивирусы. Виды антивирусов.
47. Что такое шифр? Какие виды шифров существуют?
48. Что такое симметричный шифр? Какие симметричные шифры используются сейчас?
49. Что такое ассиметричный шифр? Какие ассиметричные шифры используются сейчас?
50. Что такое хеш-функция? Какие виды хеш-функций вы знаете?
51. Что такое цифровая подпись?
52. Аутентификация, идентификация, верификация, авторизация.
53. Blockchain.
54. Что такое стеганография? Понятие стеганоконтейнера.