МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ И.Т. ТРУБИЛИНА»

ФАКУЛЬТЕТ ПРИКЛАДНОЙ ИНФОРМАТИКИ

УТВЕРЖДАЮ
Декан факультета
прикладной информатики
_____
профессор С. А. Курносов
«05» апреля 2022 г.

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
38.03.05 Бизнес-информатика

Направленность
Архитектура предприятия

Уровень высшего образования
Бакалавриат

Форма обучения
очная

Краснодар
2022

Рабочая программа дисциплины «Информационная безопасность» разработана на основе ФГОС ВО 38.03.05 Бизнес-информатика утвержденного приказом Министерства образования и науки РФ 11 августа 2016 г. № 1002.

Автор:
кандидат технических наук, доцент _____ В.Н. Лаптев

Рабочая программа обсуждена и рекомендована к утверждению решением кафедры компьютерных технологий и систем от 04.04.2022, протокол № 8.

Заведующий кафедрой компьютерных технологий и систем, к.т.н., доцент _____ Т.В. Лукьяненко

Рабочая программа одобрена на заседании методической комиссии факультета прикладной информатики, протокол от 25.04.2022 г. №8.

Председатель
методической комиссии
канд. пед. наук, доцент _____ Т.А. Крамаренко

Руководитель
основной профессиональной
образовательной программы
канд. экон. наук, доцент _____ А.Е. Востроknутов

1 Цель и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ), приобретение ими умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в вычислительных систем и сетей (ВСС).

Задачи:

- изучение теоретических основ информационной безопасности; отработки умений и навыков ее эффективного практического использования при информатизации экономической деятельности;

- повышения уровня профессиональной культуры и дисциплины, понимания необходимости грамотного применения ИБ в ИТС.

2 Перечень планируемых результатов по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

В результате освоения дисциплины формируются следующие компетенции:

ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия;

ПК-11 - умение защищать права на интеллектуальную собственность.

Место дисциплины в структуре ОП бакалавриата

«Информационная безопасность» является дисциплиной вариативной части ОПОП ВО подготовки обучающихся по направлению 38.03.05 «Бизнес-информатика», направленность «Архитектура предприятия».

4 Объем дисциплины (144 часа, 4 зачетные единицы)

Виды учебной работы	Объем, часов	
	Очная	Заочная
Контактная работа в том числе:— аудиторная - по видам учебных занятий	47 44	
— лекции	22	
— практические занятия	-	
— лабораторные занятия	22	
— внеаудиторная	3	
— экзамен	3	
Самостоятельная работа в том числе:	97	
— курсовой проект	–	

Виды учебной работы	Объем, часов	
	Очная	Заочная
— прочие виды самостоятельной работы	97	
Итого по дисциплине	144	

5 Содержание дисциплины

По итогам изучаемого курса студенты сдают экзамен. Дисциплина изучается на 4 курсе, в 8 семестре.

Содержание и структура дисциплины: лекции и самостоятельная работа по формам обучения

№ п/п	Наименование темы с указанием основных вопросов	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			
				Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1	Объект и предмет информационной безопасности. 1.1 Угрозы и концепция ИБ. 1.2 Цели и задачи дисциплины. 1.3 Направления обеспечения ИБ	ОПК-1 ПК-9 ПК-11	8	2			10
2	Защита информации (ЗИ) от случайных угроз, традиционного шпионажа и диверсий. 2.1 Классификация угроз 2.2 Случайные угрозы 2.3 Преднамеренные угрозы	ОПК-1 ПК-9 ПК-11	8	2		4	10
3	ЗИ от побочных электромагнитных излучений и наводок (ПЭМИН) 3.1 Методы защиты от ПЭМИН 3.2 Средства выявления и защиты от ПЭМИН 3.3 Активные методы защиты от ПЭМИН	ОПК-1 ПК-9 ПК-11	8	2		2	8
4	4 ЗИ от несанкционированного доступа (НСД) 4.1 Общие требования к защищенности от НСД 4.2 Защита от закладок программных и аппаратных закладок 4.3 Защита от несанкционированного изменения структур	ОПК-1 ПК-9 ПК-11	8	2		2	8
5	Компьютерные вирусы и механизмы борьбы с ними. 5.1 Классификация компьютерных вирусов (КВ) 5.2 Принципы и методы защиты от КВ 5.3 Профилактика заражений КВ АИС	ОПК-1 ПК-9 ПК-11	8	2		2	8
6	Принципы применения криптографической ЗИ. 6.1 Классификация методов криптографического преобразования информации 6.2 Стандарты шифрования 6.3 Перспективы использования шифрования в АИС	ОПК-1 ПК-9 ПК-11	8	2		2	8
7	Программно-аппаратные средства шифрования 7.1 Системы криптографической защиты данных. 7.2 Защита данных от изменений 7.2 Защита файлов от изменений	ОПК-1 ПК-9 ПК-11	8	2		2	9

№ п/п	Наименование темы с указанием основных вопросов	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			
				Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
8	ЗИ в распределенных компьютерных системах (РКС). 8.1 Архитектура РКС 8.2 Обеспечение ИБ в пользовательской подсистеме и специализированных РКС 8.3 ЗИ на уровне подсистем управления РКС	ОПК-1 ПК-9 ПК-11	8	2		2	8
9	Особенности защиты информации в РКС. 9.1 Концепция создания защищенных КС 9.2 Методологи проектирования РКС 9.3 Защита информации в РКС.	ОПК-1 ПК-9 ПК-11	8	2		2	8
10	Теория компьютерных систем защиты информации (КСЗИ). 10.1 Математическая постановка задачи разработки КСЗИ 10.2 Моделирование и реализация жизненного цикла КСЗИ 10.3 Техническая эксплуатация КСЗИ	ОПК-1 ПК-9 ПК-11	8	2		2	10
11	10 Проектирование, запуск, функционирования и развития КСЗИ. 11.1 Проектирование и запуск КСЗИ. 11.2 Особенности функционирования и развития КСЗИ. 11.3 Сертифицированные программно-аппаратные средства.	ОПК-1 ПК-9 ПК-11	8	2		2	10
		Итого		22		22	97

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические указания (для самостоятельной работы)

1. Защита информации: практикум для бакалавров / В.Н. Лаптев, С.В. Лаптев, А.В. Параскевов. – Краснодар: КубГАУ, 2015. – 84 с. Режим доступа: http://www.edu.kubsau.ru/file.php/118/01_Zashchita_informacii_Praktikum_dlja_bakalavrov.pdf

2. Лаптев В.Н. Информационная безопасность. Методические указания по самостоятельной работе обучающихся / В.Н. Лаптев, А.В. Мельников, С.М. Снимщикова. Режим доступа: http://www.edu.kubsau.ru/file.php/_38.05.01_ЕНИ_IB_MU_po_org_SR_Uaptev_Melnicov_Snimshikova_2020_570174_v1_.PDF

7 Фонд оценочных средств для проведения промежуточной аттестации

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП ВО

Номер семестра (номер семестра соответствует этапу формирования компетенции)	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения ОПОП ВО
ОПК-1 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
1	Информатика
12	Программирование
2	Электронная коммуникация
2	Программные и аппаратные средства информатики
2	Информационные технологии поддержки личной работы
2	Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности
3	Объектно-ориентированное программирование
3	Информационные технологии
5	Базы данных
5	Анализ данных
6	Общая теория систем
6	Имитационное моделирование
7	Архитектура предприятия
7	Управление ИТ-сервисами и контентом
8	Электронный бизнес
8	Информационная безопасность
8	Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты
ПК-9 — организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	
2	Электронная коммуникация
5	Управление требованиями к бизнес-приложениям
7	Информационный менеджмент
7	Электронный документооборот
8	Информационная безопасность
8	Преддипломная практика
8	Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты
ПК-11 — умение защищать права на интеллектуальную собственность	
1	Основы правовых знаний
8	Информационная безопасность
8	Преддипломная практика
8	Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые ре-	Уровень освоения	Оценочное

зультаты освоения компетенции	неудовлетворительно	удовлетворительно	Хорошо	Отлично	средство
ОПК-1 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности					
Знать: - основные принципы применения ИКТ в профессиональной деятельности - основные требования по организации защиты информации	Уровень знаний ниже минимальных требований, имели место грубые ошибки	Минимально допустимый уровень знаний, допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Устный опрос Тест, реферат, доклад (доклад с представление презентации), экзамен (вопросы и задания)
Уметь: - применять на практике основные принципы применения ИКТ в профессиональной деятельности - перечислять и давать общую характеристику видов и источников угроз безопасности; - оценивать источники угроз информационной безопасности для различных профессиональных областей; - использовать современные средства защиты информации	При решении стандартных задач не продемонстрированы основные умения, имели место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	
Владеть: - технологиями использования современных ИКТ в рамках профессиональной деятельности - современными технологиями и средствами защиты информации	При решении стандартных задач не продемонстрированы базовые навыки, имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	
ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия					
Знать: - основные принципы взаимодействия с клиентами и партнерами в	Уровень знаний ниже минимальных требований,	Минимально допустимый уровень знаний, допущено много негру-	Уровень знаний в объеме, соответствующем программе под-	Уровень знаний в объеме, соответствующем программе под-	Устный опрос тест, реферат, доклад (доклад с представле-

Планируемые результаты освоения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно	удовлетворительно	Хорошо	Отлично	
процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия.	имели место грубые ошибки	бых ошибок	готовки, допущено несколько негрубых ошибок	готовки, без ошибок	ние презентации), экзамен (вопросы и задания)
Уметь: - управлять требования к ИС по информационной безопасности - обрабатывать запросы заказчика на разных этапах обеспечения информационной безопасности ИС	При решении стандартных задач не продемонстрированы основные умения, имели место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	
Владеть: - методиками коммуникации с клиентами и партнерами в процессе решения задач управления информационной безопасностью - умением обрабатывать запросы клиентов и партнеров в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	При решении стандартных задач не продемонстрированы базовые навыки, имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	
ПК-11 - умение защищать права на интеллектуальную собственность					
Знать: - правовые основы защиты интеллектуальной собственности - теоретические основы ИБ, ее модели, методы и технологии, обеспечивающие ее увязку с эффективной деятельно-	Уровень знаний ниже минимальных требований, имели место грубые ошибки	Минимально допустимый уровень знаний, допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Устный опрос тест, реферат, доклад (доклад с представление презентации), экзамен (вопросы и задания)

Планируемые результаты освоения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно	удовлетворительно	Хорошо	Отлично	
стью предприятий и организаций.					
Уметь: - программировать, комплексно использовать и совершенствовать модели, методы и технологии ИБ в своей профессиональной деятельности - управлять патентами и лицензиями на технологии	При решении стандартных задач не продемонстрированы основные умения, имели место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	
Владеть: - навыками формирования патентных заявок и лицензирования технологий - навыками применения моделей, методов и технологий ЗИ, а также аппаратно-программных и других средств в обеспечении должных условий жизненного цикла ИС, безопасности и целостности их данных и технологий.	При решении стандартных задач не продемонстрированы базовые навыки, имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения ОПОП ВО

7.3.1 Оценочные средства по компетенции ОПК-1 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Устный опрос

Устный вопрос представляет собой форму контроля подготовки обучаемых к выполнению заданий лабораторных занятий, а также их непрерывной самостоятельной работы по освоению знаний, умений и навыков, необходимых для их успешной работы как специалистам по ИБ.

Ниже представлены вопросы устных опросов обучающихся по каждому из 11 лабораторному занятию по дисциплины. Сами лабораторные занятия описаны в Учебном пособии. Информационная безопасность В.И. Лойко, В.Н.Лаптев, Г.А. Аршинов, С.В.Лаптев представленого на образовательном портале КубГАУ, https://edu.kubsau.ru/file.php/_IB_Ucp.posobie_21.05.2020_AAA_570178_v1_.PDP

Для их успешного выполнения по этой компетенции обучаемый должен, как минимум, правильно устно ответить на следующие вопросы и получить оценку.

Лз-1. Решение проблем и задач на базе искусственного интеллекта.

1. Дайте определение искусственному интеллекту (ИИ).
2. Сходств и различие естественного интеллекта (ЕИ) и ИИ.
3. Место и роль взаимодействия ЕИ и ИИ в функционировании и развитии ОС.
4. Сущность открытой системы (ОС). Законы ее функционирования и развития.
5. Сформулировать определения задачи и проблемы.
4. Принципиальное различие терминов задача и проблема.
5. Какие задачи и проблемы необходимо научиться решать в сфере ИБ?

Лз-2. Создание цифрового сигнала, обеспечивающего «эффект системы»

1. Что означает термин «эффект системы»?
2. Зачем для выживания открытой системы (ОС) в различных типовых для нее ситуациях необходимы разные «эффекты системы»!
3. Как выявлять и создавать новые «эффект системы»?

Лз-3. Разграничение доступа к информации в ОС Windows.

1. Для чего нужно разграничение доступа в информации?
2. Почему для разграничения доступа к информации требуется различные типы допуска к ней?

Лз-4. Контроль обеспечения безопасности информации.

1 Сформулировать определение задачи.
2. Дать определение проблемы.
3. В чем состоит принципиальное различие терминов задача и проблема

Лз-5. Применение программных антивирусных комплексов.

1. Для чего нужны антивирусные комплексы?
2. Чем можно объяснить наличие множества антивирусных комплексов?

3. Как в антивирусных комплексах реализуется их функционирования и развития?

4. Каким образом в антивирусных программах идентифицируются разные вирусы?

Лз-6. Программирование симметричных и алгебраических алгоритмов шифрования?

1. Зачем нужно программирование при разработке симметричных и алгебраических алгоритмов шифрования?

2. Особенности симметричных алгоритмов шифрования.

3. Особенности алгебраических алгоритмов шифрования.

Лз7-8. Построение систем ЗИ на основе криптографических преобразований.

1 Сущность криптографических преобразований при ЗИ.

2. Дать определение проблемы.

3. В чем состоит принципиальное различие терминов задача и проблема

Лз-9. Система ЗИ Secret Net.

1. Особенности системы ЗИ Secret Net.

2. Технология ЗИ в Secret Net.

3. Перспективы развития Secret Net.

Лз-10. Система ЗИ Net Ware.

1. Особенности системы ЗИ Net Ware.

2. Технология ЗИ в Net Ware.

3. Перспективы развития Net Ware.

Тесты (примеры)

Тестирование обучаемых по темам, разделам и по всей дисциплине «Информационная безопасность» осуществляется с помощью компьютерной программы INDIGO.

Ниже представлены два примера использования тестов с помощью программы INDIGO.

№1 (Балл 1)

Организационные средства обеспечения информационной безопасности (ИБ):

1 ○ специальные пакеты программ или отдельные программы, предназначенные для решения задач ИБ;

2 ○ сложившиеся в обществе нормы или правила, нарушение которых приравнивается к несоблюдению правил поведения;

3 ◉ мероприятия, специально предусматриваемые в технологии функционирования;

4 ○ автоматизированных систем с целью решения задач ИБ;

5 ○ различные механические, электронные и т.п. устройства, встраиваемые в аппаратуру с целью решения задач ИБ;

Темы рефератов

1. Деловые ресурсы в Интернет и их защита
2. Компьютерные методы статистического анализа и прогнозирования ИБ
3. ЗИ в мультимедийных системах обучения и образовательных ИТ.
4. Развитие представлений об измерении и обработке информации, ее защите.
5. Защита конфиденциальной информации.
6. Базовая информационная технология (БИТ) и ее использование в ИБ.
7. Специфика проведения отраслевого и регионального анализ. Основные положения теории ИБ для ИС и АИС.
8. Разработка модели разграничения доступа к информации. Разграничение доступа к информации.
9. Разграничение доступа к информации в среде Windows XT.
10. Требования к системам и средствам ИБ от НСД.

Темы докладов-презентаций

1. Модификация автоматизированных обучающих систем (АОС) с учетом требований ИБ.
2. Перспективные направления повышения эффективности ИБ на базе ИТ.
3. Информационные технологии в высшей школе и их защита.
4. Перспективные электронные ИС и ИТ, их защита от НСД.
5. Программно-аппаратная защита информации: состояние и перспективы ее развития.
6. Состояние и перспективы развития СЗИ.
7. Модернизация электронных программно-методических комплексов с учетом современных требований к защите авторских прав и информации.
8. Обеспечение ИБ корпоративной ЛВС ФБГОУ ВПО КубГАУ.
9. Перспективные СЗИ для ИПС и БД в экономике.
10. Проблемно-ориентированный информационный консалтинг по ИБ.

7.3.2 Оценочные средства по компетенции ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия

Устный опрос

Лз-1. Решение проблем задач и на базе искусственного интеллекта.

1. Как специалисту по ИБ организовать правильное взаимодействие **с** клиентами и партнерами в процессе решения проблем и задач управления ИБ?

2. Как добиться правильного понимания терминов конфиденциальность, целостность и доступность всеми участниками **ИТ-**инфраструктуры предприятия?

Лз-2. Создание цифрового сигнала, обеспечивающего «эффект системы»

1. Почему цифрой сигнал играет ведущую роль в создании должного «эффекта системы»?

2. Как формируется цифровой сигнал в ОС (у нас АИС)?

3. На каком физическом законе базируется «эффект системы»?

Лз-3. Разграничение доступа к информации в ОС Windows.

1. Как организуется разграничение доступа в информации в ОС Windows?

2. Почему в ОС Windows для разграничения используются 2 способа?

Лз-4. Контроль обеспечения безопасности информации.

1 Для чего нужен контроль для обеспечения ИБ?

2. Каким образом этот контроль обеспечивается?

Лз-5. Применение программных антивирусных комплексов.

1. Для чего нужны адаптированные к специфике деятельности предприятия антивирусные комплексы?

2. Как ими реализуется операции функционирования и развития АИС?

Лз-6. Программирование симметричных и алгебраических алгоритмов шифрования?

1. Почему именно программирование востребовано для реализации алгоритмов шифрования?

2. Сходство и различие симметричных и алгебраических алгоритмов шифрования.

Лз7-8. Построение систем ЗИ на основе криптографических преобразований.

1. Почему криптография – самый надежный способ шифрования информации?

2. Чем криптографическая ЗИ отличается от стеганографической ЗИ?

Лз9-10. Система ЗИ Secret Net и .

1. Отличительные особенности систем ЗИ Secret Net и Net Ware.

2. Технология и из взаимодействия.

Тесты (примеры)

Тестирование обучаемых по темам, разделам и по всей дисциплине «Информационная безопасность» осуществляется с помощью компьютерной программы INDIGO. Ниже представлены пример фрагментарного использования программы INDIGO по компетенции ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ- инфраструктуры предприятия

№1 (Балл 1)

Организационные средства обеспечения информационной безопасности (ИБ):

1 ○ специальные пакеты программ или отдельные программы, предназначенные для решения задач ИБ;

2 ○ сложившиеся в обществе нормы или правила, нарушение которых приравнивается к несоблюдению правил поведения;

3 ◉ мероприятия, специально предусматриваемые в технологии функционирования;

4 ○ автоматизированных систем с целью решения задач ИБ;

5 ○ различные механические, электронные и т.п. устройства, встраиваемые в аппаратуру с целью решения задач ИБ;

Темы рефератов

1. Контроль за состоянием ИБ.
2. Исследование проблем очистки магнитных носителей
3. Современная ИБ от разрушающих программных воздействий
4. Исследование антивирусных программных средств
5. СЗИ на основе криптографических преобразований
6. Исследование уязвимостей криптографического ПО
7. Базовые принципы обеспечения целостности информации
8. Аппаратные средства опознавания пользователей
9. Принципы функционирования СЗИ от НСД в ПЭВМ
10. Исследование уязвимостей криптографического ПО

Темы докладов-презентаций

1. Автоматизированные обучающие системы и ИБ в них.
2. Современные методы и средства ИБ.
3. Современные криптографические методы ИБ.
4. Аппаратно-программные средства обеспечения ИБ в компьютерных системах.
5. Методы ИБ в компьютерных системах и сетях.
6. Базовая информационная технология с учетом требований ИБ.
7. Модели разграничения доступа к информации.
8. Развитие представлений об измерении и обработке информации, ее защите.
9. Способы защиты конфиденциальной информации
10. Схема разграничение доступа к информации в среде Windows XT

7.3.3 Оценочные средства по компетенции ПК-11 - умение защищать права на интеллектуальную собственность

Устный опрос

Лз-1. Решение проблем задач и на базе искусственного интеллекта.

1. Как специалисту по ИБ организовать правильное взаимодействие **с** клиентами и партнерами в процессе решения проблем и задач управления ИБ?

2. Как добиться правильного понимания терминов конфиденциальность, целостность и доступность всеми участниками **ИТ-**инфраструктуры предприятия?

Лз-2. Создание цифрового сигнала, обеспечивающего «эффект системы»

1. Почему цифрой сигнал играет ведущую роль в создании должного «эффекта системы»?

2. Как формируется цифровой сигнал в ОС (у нас АИС)?

3. На каком физическом законе базируется «эффект системы»?

Лз-3. Разграничение доступа к информации в ОС Windows.

1. Для чего необходимо защитить свои права на интеллектуальную собственность?

2. Почему этому необходимо научиться?

Лз-4. Контроль обеспечения безопасности информации.

1. Как отрабатывать умение защищать права на свою интеллектуальную собственность?

2. Каким образом необходимо обеспечивается безопасности конфиденциальной информации?

Лз-5. Применение программных антивирусных комплексов.

1. Применение программных антивирусных комплексов как действенное средство ЗИ.

2. Как практически выбирать эффективный антивирусный комплекс?

Лз-6. Программирование симметричных и алгебраических алгоритмов шифрования?

1. Суть разработки и отладки алгоритмов шифрования.

2. Сущность технологии совместной отладки алгоритма шифорования и программы его реализующей.

Лз7-8. Построение систем ЗИ на основе криптографических преобразований.

1. Перспективы развития криптографии.

2. Перспективы развития стеганографической ЗИ

Лз9-10. Система ЗИ Secret Net и .

1. Как выбирать сетевое средство ЗИ?

2. Какой критерий ЗИ необходимо при этом использовать?

Тесты (примеры)

Тестирование обучаемых по отдельным темам, разделам и по всей дисциплине «Информационная безопасность» осуществляется с помощью компьютерной программы INDIGO **.**

Ниже представлены два примера использования тестов с помощью программы INDIGO **.**

№37 (1)

Внешняя защита, осуществляемая техническими средствами:

1 ☑ охрана территории и помещений;
2 ☐ подавление электромагнитного излучения;
3 ☑ наблюдение;
4 ☐ идентификация;
5 ☑ разграничение доступа;
6 ☐ блокировка;

Темы рефератов

1. Деловые ресурсы в Интернет и их защита
2. Компьютерные методы статистического анализа и прогнозирования ИБ
3. ЗИ в мультимедийных системах обучения и образовательных ИТ.
4. Развитие представлений об измерении и обработке информации, ее защите.
5. Защита конфиденциальной информации
6. Базовая информационная технология (БИТ) и ее использование в ИБ
7. Специфика проведения отраслевого и регионального анализ. Основные положения теории ИБ для ИС и АИС
8. Разработка модели разграничения доступа к информации. Разграничение доступа к информации
9. Разграничение доступа к информации в среде Windows XT
10. Требования к системам и средствам ИБ от НСД

Темы докладов-презентаций

1. Иерархия требований к системам и средствам ИБ от НСД
2. Модель типовых криптографических преобразований
3. Схемы уязвимостей криптографической защиты и реализующих ее программ.
4. Связь принципов функционирования СЗИ от НСД в ПК, вычислительных системах и сетях
5. Модификация автоматизированных обучающих систем (АОС) с учетом требований ИБ.
6. Перспективные направления повышения эффективности ИБ на базе ИТ.
7. Информационные технологии в высшей школе и их защита.
8. Перспективные электронные ИС и ИТ, их защита НСД.
9. Программно-аппаратная защита информации: состояние и перспективы ее развития.
10. Состояние и перспективы развития СЗИ.

Вопросы и задания для проведения промежуточного контроля (экзамена)

Вопросы к экзамену

ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности.
3. Место информационной безопасности экономических систем в национальной безопасности страны.
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
5. Таксономия нарушений информационной безопасности вычислительной системы.
6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы защиты информации.
8. Модели безопасности и их применение.
9. Классификация методов защиты информации от НСД.
10. Классификация средств защиты информации от НСД.

ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия;

1. Механизмы защиты информации от НСД.
2. Государственные требования к построению СЗИ.
3. Концепция защиты информации от НСД.
4. Особые требования к криптографическим средствам СЗИ от НСД.
5. Показатели защищенности СВТ от НСД.
6. Классификация КС и требования по защите информации.
7. Использование защищенных компьютерных систем.
8. Методы контроля доступа к ресурсам компьютерной системы.
9. Способы фиксации факта доступа.
10. Структура и функции подсистемы контроля доступа пользователей.
11. Средства активного аудита компьютерных систем.
12. Идентификация и аутентификация субъектов и объектов КС.
13. Идентифицирующая информация и протоколы идентификации.
14. Основные подходы к защите данных от НСД.
15. Иерархический доступ к файлу.
16. Доступ к данным со стороны процесса.
17. Понятие скрытого доступа.
18. Модели управления доступом.

19. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.

20. Защита алгоритма шифрования и программно-аппаратные средства шифрования.

21. Построение аппаратных компонент криптозащиты данных.

ПК-11 - умение защищать права на интеллектуальную собственность.

22. Сущность разрушающих программных средств.

23. Взаимодействие прикладных программ и программы злоумышленника.

24. Классификация разрушающих программных средств и их воздействий.

25. Компьютерные вирусы как особый класс РПВ.

26. Сущность, проявление, классификация компьютерных вирусов.

27. Необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

28. Организационные средства защиты от компьютерных вирусов.

29. Роль морально-этических факторов в устранении угрозы РПВ.

30. Проблема обеспечение целостности информации.

31. Защита файлов от изменений. Способы обеспечения целостности информации.

32. Электронная цифровая подпись. Криптографические хэш-функции. Схемы вычисления хэш-функции.

33. Методы криптографии и задачи, решаемые криптографическими средствами в КС.

34. Алгоритмы криптографических преобразований, их характеристики.

35. Методы и средства ограничения доступа к компонентам ЭВМ.

36. Построение средств защиты информации для ПЭВМ.

37. Перечень и краткая характеристика сертифицированных программно-аппаратных систем защиты информации (СЗИ) от НСД для ПЭВМ.

38. Особенности защиты информации в вычислительных сетях.

39. Механизмы реализации атак на вычислительные сети.

40. Защита сетевого файлового ресурса.

41. Определение перечня защищаемых ресурсов и их критичности.

42. Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.

43. Определение угроз безопасности информации.

44. Формирование требований к построению СЗИ.

45. Определение уязвимости КС и выбор средств защиты информации.

46. Создание учетных записей пользователей.

47. Создание учетных записей групп.

48. Организация общего доступа к папкам.

49. Активный контроль состояния безопасности компьютерной системы.

50. Средства ведения и анализа системных журналов ОС Windows NT.

51. Централизованное управление пользователями и контроль их действий.

52. Средства контроля вычислительных процессов.

53. Свойства процессов и управление ими.

54. Восстановление удаленных файлов.

55. Восстановление отформатированных дискет.

56. Средства гарантированного удаления информации.

57. Средства анализа программ.

58. Дизассемблирование программ и исследование кода.

59. Антивирусные программные комплексы. Настройка и применение.

60. Устранение проникновения вирусов в компьютерную систему.

61. Исследование результатов воздействия компьютерных вирусов на программы в среде ОС

62. Исследование результатов работы антивирусных программ.

63. Алгоритмы ЭЦП. Реализация ЭЦП В СКЗИ «Верба-OW».

64. Построение СЗИ "Кобра".

65. Защита файлов и каталогов. Шифрованные логические диски.

66. Администрирование СЗИ "Кобра".

67. Исследование временной стойкости криптосистемы архиватора WinZip.

68. Исследование уязвимостей криптосистемы архиватора Arj.

69. Построение аппаратных средств СЗИ "Аккорд" и управление пользователями в ней.

70. Средства анализа и копирования защищенных дискет и взламывания защиты программ.

71. Средства простановки ключевых меток и защиты программ от копирования.

72. Исследование дискет, защищенных от копирования

73. Исследование программ с защитой от копирования.

74. Защита программ от отладки.

75. Защита программ от трассировки.

76. Построение и принцип работы программ СЗИ "Снег-1.0", работа ее администратора.

77. Работа администратора при использовании СЗИ "Secret Net".

78. Работа пользователей ПК в защищенной среде.

79. Работа администратора ЛВС по управлению пользователями.

80. Работа администратора ЛВС по управлению доступом пользователей и процессов к ресурсам системы.

Практические задания для экзамена

В рамках практического задания для оценки освоения компетенций ОПК-1, ПК-9, ПК-11 обучающемуся предлагается выполнить следующее задание

1). Найдите правило, разрешающее отсылку ICMP-пакетов echo reguest. Проверьте его работу для какого-нибудь узла из локальной или внешней сети, используя его ip-адрес (например, командой ping 192.168.0.10 можно проверить доступность компьютера с указным адресом). Если ответ пришел, можно переходить ко второй части задания. Если ответа нет, попробуйте найти такой узел, который пришлет ответ.

2). Выбрав кнопку New Rule создайте правило, запрещающее отсылку icmp-пакетов на данный узел. Проверьте его работу.

3) Получите перечень компьютеров и контроллеров домена. Для указанных преподавателем 1-2 компьютеров выясните установленную операционную систему и используемые ими ip-адреса. Занесите данные в отчет.

4). Получите перечень предоставляемых в общий доступ каталогов на вашем компьютере. Опишите хранимые там данные и охарактеризуйте степень их важности.

5. Для указанных ресурсов и выбранных пользователей опишите действующие разрешения на доступ. При этом надо учитывать, что:

- эффективное (действующее) разрешение складывается из разрешений для пользователя лично и разрешений всех групп, в которые пользователь входит;
- запрещение имеет больший приоритет, чем разрешение;
- при комбинации разрешений для общего ресурса с разрешениями NTFS, приоритетными будут разрешения, максимально ограничивающие доступ.

6. Перечислите и охарактеризуйте стандартные правила, определяющие параметры сессии сканирования. На базе одного из них создайте собственное правило.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и опыта деятельности, характеризующих этапы формирования компетенций

Контроль освоения дисциплины «Информационная безопасность» и оценка знаний обучающихся на зачете производится в соответствии с ПлКубГАУ 2.5.1– «Текущий контроль и успеваемости и промежуточной аттестации студентов».

Критерии оценки знаний обучаемых при проведении устного опроса.

Оценка «отлично» выставляется за полный ответ на поставленный вопрос с включением в содержание ответа лекции, материалов учебников, дополнительной литературы без наводящих вопросов.

Оценка «хорошо» выставляется за полный ответ на поставленный вопрос в объеме лекции с включением в содержание ответа материалов учебников с четкими положительными ответами на наводящие вопросы преподавателя.

Оценка «удовлетворительно» выставляется за ответ, в котором озвучено более половины требуемого материала, с положительным ответом на большую часть наводящих вопросов.

Оценка «неудовлетворительно» выставляется за ответ, в котором озвучено менее половины требуемого материала или не озвучено главное в со-

держании вопроса с отрицательными ответами на наводящие вопросы или студент отказался от ответа без предварительного объяснения уважительных причин.

Критериями оценки доклада, реферата (презентации) являются: новизна текста, обоснованность выбора источников литературы, степень раскрытия сущности вопроса, соблюдения требований к оформлению.

Оценка «**отлично**» — выполнены все требования к написанию реферата: обозначена проблема и обоснована её актуальность; сделан анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция; сформулированы выводы, тема раскрыта полностью, выдержан объём; соблюдены требования к внешнему оформлению.

Оценка «**хорошо**» — основные требования к реферату выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении.

Оценка «**удовлетворительно**» — имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата; отсутствуют выводы.

Оценка «**неудовлетворительно**» — тема реферата не раскрыта, обнаруживается существенное непонимание проблемы или реферат не представлен вовсе.

Критерии оценки знаний студентов при проведении тестирования.

Оценка «отлично» выставляется при условии правильного ответа студента не менее чем 85 % тестовых заданий;

Оценка «хорошо» выставляется при условии правильного ответа студента не менее чем 70 % тестовых заданий;

Оценка «удовлетворительно» выставляется при условии правильного ответа студента не менее 51 %; .

Оценка «неудовлетворительно» выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Критерии оценки на экзамене

Оценка «отлично» выставляется обучающемуся, который обладает всесторонними, систематизированными и глубокими знаниями материала учебной программы, умеет свободно выполнять задания, предусмотренные учебной программой, усвоил основную и ознакомился с дополнительной литературой, рекомендованной учебной программой. Как правило, оценка «отлично» выставляется обучающемуся усвоившему взаимосвязь основных положений и понятий дисциплины в их значении для приобретаемой специальности, проявившему творческие способности в понимании, изложении и использовании учебного материала, правильно обосновывающему принятые

решения, владеющему разносторонними навыками и приемами выполнения практических работ.

Оценка «хорошо» выставляется обучающемуся, обнаружившему полное знание материала учебной программы, успешно выполняющему предусмотренные учебной программой задания, усвоившему материал основной литературы, рекомендованной учебной программой. Как правило, оценка «хорошо» выставляется обучающемуся, показавшему систематизированный характер знаний по дисциплине, способному к самостоятельному пополнению знаний в ходе дальнейшей учебной и профессиональной деятельности, правильно применяющему теоретические положения при решении практических вопросов и задач, владеющему необходимыми навыками и приемами выполнения практических работ.

Оценка «удовлетворительно» выставляется обучающемуся, который показал знание основного материала учебной программы в объеме, достаточном и необходимым для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных учеб-ной программой, знаком с основной литературой, рекомендованной учебной программой. Как правило, оценка «удовлетворительно» выставляется обучающемуся, допустившему погрешности в ответах на экзамене или выполнении экзаменационных заданий, но обладающему необходимыми знаниями под руководством преподавателя для устранения этих погрешностей, нарушающему последовательность в изложении учебного материала и испытывающему затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, не знающему основной части материала учебной программы, допускающему принципиальные ошибки в выполнении предусмотренных учебной программой заданий, неуверенно с большими затруднениями выполняющему практические работы. Как правило, оценка «неудовлетворительно» выставляется обучающемуся, который не может продолжить обучение или приступить к деятельности по специальности по окончании университета без дополнительных занятий по соответствующей дисциплине.

8 Перечень основной и дополнительной литературы

Основная учебная литература:

1. Лойко В.И. Информационная безопасность: учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. В. Лаптев. – Краснодар: КубГАУ, 2020. – 330 с. ISBN 978-5-907346-50-5. Режим доступа: https://edu.kubsau.ru/file.php/_IB_Ucp.posobie_21.05.2020_AAA_570178_v1_.PDP

2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — Электрон. текстовые данные. — М. : Евразийский открытый ин-

ститут, 2012. — 311 c. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677

3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97562.html

Дополнительная учебная литература:

1. Основы управления информационной безопасности. [Электронный ресурс]: Учебное пособие / А.П. Курило [и др.] - М.: Горячая линия – Телеком,2012. – 244 с. Режим доступа: http://www.iprbookshop.ru/43960.— ЭБС «IPRbooks».

2. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Москва : Московский городской педагогический университет, 2011. — 260 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/26486.html

3. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1021744

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень ЭБС

№	Наименование	Тематика	Ссылка
1.	IPRbook	Универсальная	http://www.iprbookshop.ru/
2.	Образовательный портал КубГАУ	Универсальная	https://edu.kubsau.ru/
3.	Znanium	Универсальная	https://znanium.com

10 Методические указания для обучающихся по освоению дисциплины

1. Защита информации: практикум для бакалавров / В.Н. Лаптев, С.В. Лаптев, А.В. Параскевов. – Краснодар: КубГАУ, 2015. – 84 с. Режим доступа: http://www.edu.kubsau.ru/file.php/118/01_Zashchita_informacii_Praktikum_dlja_bakalavrov.pdf

2. Лаптев В.Н. Информационная безопасность. Методические указания по самостоятельной работе обучающихся / В.Н. Лаптев, А.В. Мельников, С.М. Снимщикова. Режим доступа: http://www.edu.kubsau.ru/file.php/_38.05.01_ЕНИ_IB_MU_po_org_SR_Uaptev_Melnicov_Snimshikova_2020_570174_v1_.PDF

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационно-справочных систем

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют: обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети "Интернет"; фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы; организовать процесс образования путем визуализации изучаемой информации посредством использования презентационных технологий; контролировать результаты обучения на основе компьютерного тестирования.

11.1 Перечень программного обеспечения

№	Наименование	Краткое описание
1	Windows	Операционная система
2	Office	Пакет офисных приложений
3	INDIGO	Тестирование

11.2 Перечень современных профессиональных баз данных, информационных справочных и поисковых систем

№	Наименование	Тематика	Электронный адрес
1.	Научная электронная библиотека «eLIBRARY.RU»	Универсальная	https://elibrary.ru

11.3 Доступ к сети Интернет

Доступ к сети Интернет, доступ в электронную информационно-образовательную среду университета

12 Материально-техническое обеспечение для обучения по дисциплине

Планируемые помещения для проведения всех видов учебной деятельности:

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1	Информационная безопасность	Помещение №310 ЭК, посадочных мест — 167; площадь — 157,1кв.м; учебная аудитория для проведения занятий лекционного типа. Сплит-система — 1 шт.; лабораторное оборудование (плейер — 1 шт.;); специализированная мебель(учебная доска, учебная мебель); технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий (ноутбук, проектор, экран); программное обеспечение: Windows, Office. Помещение №310 ЭК, площадь — 3,6кв.м; помещение для хранения и профилактического обслуживания учебного оборудования. Лабораторное оборудование (плейер — 1 шт.;); технические средства обучения (сетевое оборудование — 1 шт.; акустическая система — 1	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

		шт.; микрофон — 2 шт.). Помещение №403 ЭК, посадочных мест — 50; площадь — 83,5кв.м; учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Сплит-система — 2 шт.; специализированная мебель (учебная доска, учебная мебель); технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий (ноутбук, проектор, экран); программное обеспечение: Windows, Office. Помещение №1 ЭК, площадь — 64,9кв.м; посадочных мест — 30; учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. кондиционер — 1 шт.; технические средства обучения (компьютер персональный — 15 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель (учебная доска, учебная мебель) программное обеспечение:	

		Windows, Office, INDIGO. Помещение №3 ЭК, посадочных мест — 30; площадь — 62,1кв.м; учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. сплит-система — 1 шт.; кондиционер — 1 шт.; технические средства обучения (сетевое оборудование — 1 шт.; компьютер персональный — 16 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель (учебная доска, учебная мебель) программное обеспечение: Windows, Office, INDIGO. Помещение №8 ЭК, площадь — 57,8кв.м; посадочных мест — 30; учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Кондиционер — 1 шт.; технические средства обучения (компьютер персональный — 14 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду уни-	

		верситета; специализированная мебель (учебная доска, учебная мебель) программное обеспечение: Windows, Office, INDIGO. Помещение №5 ЭК, посадочных мест — 20; площадь — 40,6кв.м; учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. кондиционер — 1 шт.; технические средства обучения (сетевое оборудование — 1 шт.; компьютер персональный — 9 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель (учебная доска, учебная мебель) программное обеспечение: Windows, Office, INDIGO. Помещение №407 ЭК, посадочных мест — 30; площадь — 59,3кв.м; учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Сплит-система — 2 шт.; доступ к сети «Интернет»; доступ в электронную информационно-	

		образовательную среду университета; специализированная мебель (учебная доска, учебная мебель); технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий (ноутбук, проектор, экран); программное обеспечение: Windows, Office Помещение №4 ЭК, площадь — 31,1кв.м; помещение для хранения и профилактического обслуживания учебного оборудования. кондиционер — 2 шт.; лабораторное оборудование (шкаф лабораторный — 1 шт.; набор лабораторный — 1 шт.;); технические средства обучения (принтер — 1 шт.; проектор — 1 шт.; микрофон — 1 шт.; ибп — 4 шт.; сервер — 1 шт.; носитель информации — 1 шт.; компьютер персональный — 15 шт.). Помещение №4 ЭК, площадь — 9,1кв.м; помещение для хранения и профилактического обслуживания учебного оборудования. сплит-система — 2 шт.; штатив — 1 шт.; лабораторное оборудование (шкаф лабораторный — 2 шт.; стенд лабораторный — 4 шт.;); технические средства обучения (экран — 1 шт.; сетевое оборудование — 5	

		шт.; сервер — 6 шт.; компьютер персональный — 2 шт.).	
2	Информационная безопасность	Помещение №206 ЭК, посадочных мест — 20; площадь — 41кв.м; помещение для самостоятельной работы. Технические средства обучения (компьютер персональный — 9 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель (учебная мебель). Программное обеспечение: Windows, Office, специализированное лицензионное и свободно распространяемое программное обеспечение, предусмотренное в рабочей программе	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13