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
«27» марта 2020 г.

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки
09.03.02 Информационные системы и технологии

Направленность
Создание, модификация и сопровождение информационных систем, администрирование баз данных

Уровень высшего образования
бакалавриат

Форма обучения
очная

Краснодар
2020

Рабочая программа дисциплины «Информационная безопасность» разработана на основе ФГОС ВО 09.03.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки РФ 19 сентября 2017 г. № 926.

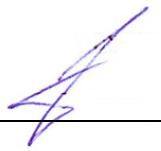
Автор:
канд. техн. наук, доцент  В.Н. Лаптев

Рабочая программа обсуждена и рекомендована к утверждению решением кафедры компьютерных технологий и систем от 16.03.2020 г., протокол № 7.

Заведующий кафедрой
д-р техн. наук, профессор  В.И. Лойко

Рабочая программа одобрена на заседании методической комиссии факультета прикладной информатики, протокол от 27.03.2020 г., протокол № 7.

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

Руководитель
основной профессиональной
образовательной программы
канд. физ.-мат. наук, доцент  С.В. Лаптев

1 Цель и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является

— формирование у обучаемых потребности в постоянном развитии своих знаний и способностей их эффективного использования в области теоретических основ и технологий информационной безопасности (ИБ) и защиты информации (ЗИ);

— освоения умений и навыков практического обеспечения должной информационной безопасности (ИБ) при создании, модификации и сопровождении автоматизированных информационных систем (АИС), правильном администрировании их баз данных (БД) в строгом соответствии со стратегией развития искусственного интеллекта в Российской федерации (РФ) на период до 2030 года.

Такая целевая установка способствует быстрому развитию искусственного интеллекта (ИИ) - комплексу технологических решений, позволяющих имитировать когнитивные (познавательные) функции человека (включая самообучение и поиск управленческих решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс включает в себя информационно-коммуникационную инфраструктуру (ИКС), программное обеспечение (ПО), в котором используется методы машинного обучения, процессы и сервисы по обработке данных и быстрому поиску правильных управленческих решений. При этом ИИ обеспечивает эффективное использование программных средств и технологий систем ИБ и ЗИ в вычислительных системах и сетях (ВСС)

Задачи дисциплины

- Анализ возможностей по управлению вычислительными ресурсами, взаимодействующими с БД;
- Управления вычислительными ресурсами, взаимодействующими с БД.

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

В результате освоения дисциплины формируются следующие компетенции:

ПКС-3. Способность выполнять работы по обеспечению функционирования баз данных и их информационной безопасности.

В результате изучения дисциплины «Информационная безопасность» обучающийся готовится к освоению трудовых функций и выполнению

трудовых действий:

Профессиональный стандарт - 06.011 Администратор баз данных.

Трудовая функция - ТФ 3.2.2 Оптимизация распределения вычислительных ресурсов, взаимодействующих с БД.

Трудовые действия:

1. Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с БД;

2.Управления вычислительными ресурсами, взаимодействующими с БД;

3 Место дисциплины в структуре ОПОП ВО

«Информационная безопасность» является дисциплиной части, формируемой участниками образовательных отношений ОПОП ВО подготовки обучающихся 09.03.02 «Информационные системы и технологии», направленность «Создание, модификация и сопровождение информационных систем, администрирование баз данных».

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	**69** 66	 -
— лекции	22	-
— практические	22	-
— лабораторные	22	-
— внеаудиторная	3	-
— зачет	-	-
— экзамен	3	-
Самостоятельная работа в том числе:	**75**	-
— прочие виды самостоятельной работы	75	-
Итого по дисциплине	**144**	-

5 Содержание дисциплины

По итогам изучаемой дисциплины студенты (обучающиеся) сдают экзамен.

Дисциплина изучается на 4 курсе, в 8 семестре по учебному плану очной формы обучения.

Содержание и структура дисциплины по очной форме обучения

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			
				Лк	Пз	Лз	Ср
1	Национальная стратегия развития ИИ в РФ и ее связь с ИБ 1 Цели и задачи стратегии, ее основные понятия. 2 Принципы и технологии стратегии, их использование в совершенствовании ИБ в РФ. 3 Механизм совершенствования ИБ с учетом реализации стратегии развития ИИ.	ПК-3	8	2	2	2	6
2	Объект и предмет ИБ. 1 Угрозы и концепция ИБ. 2 Цели и задачи дисциплины. 3 Направления обеспечения ИБ		8	2	2	2	6
3	Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. 1. Классификация угроз. 2. Случайные и преднамеренные угрозы.		8	2	2	2	6
4	СЗИ от побочных электромагнитных излучений и наводок (ПЭМИН). 1.Методы защиты от ПЭМИН. 2. Средства выявления и защиты от ПЭМИН. 3. Активные методы защиты от ПЭМИН.		8	2	2	2	6
5	Защита информации (ЗИ) от несанкционированного доступа (НСД). 1. Общие требования к защищенности от НСД 2. Защита от программных и аппаратных закладок. 3. Защита от несанкционированных изменений структур		8	2	2	2	6
6	Компьютерные вирусы (КВ) и механизмы борьбы с ними. 1. Классификация КВ. 2. Принципы и методы защиты от КВ. 3. Профилактика заражений КВ в АИС.		8	2	2	2	6
7	Принципы применения криптографической защиты информации 1. Классификация методов криптографического преобразования информации. 2. Стандарты шифрования. 3. Перспективы использования шифрования в АИС.		8	2	2	2	6
8	Стенографическая защита информации. 1. Основные понятия стенографии. 2. Основные угрозы стенографии и типы нарушителей.		8	2	2	2	6

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			
				Лк	Пз	Лз	Ср
	3. Компьютерная и цифровая стенография.						
9	ЗИ в распределенных компьютерных системах (РКС). 1. Архитектура РКС. 2. Обеспечение ИБ в пользовательской подсистеме и специализированных РКС. 3. ЗИ на уровне подсистем управления РВС.		8	2	2	2	7
10	Особенности ЗИ в распределенных компьютерных систем (РКС). 1. Концепция создания защищенных РКС. 2. Методология проектирования защищенных РКС 3. Этапы создания РКС		8	2	2	2	10
11	Теория компьютерных систем защиты информации (КСЗИ). 1. Математическая постановка задачи разработки КСЗИ 2. Моделирование и реализация КСЗИ. 2. Эксплуатация КСЗМ.			2	2	2	10
				22	22	22	75

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

1. Защита информации: практикум для бакалавров / В.Н. Лаптев, С.В. Лаптев, А.В. Параскевов. – Краснодар: КубГАУ, 2015. – 84 с. – Режим доступа: https://edu.kubsau.ru/file.php/118/01_Zashchita_informacii_Praktikum_dlja_bakalavrov.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*	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения ОПОП ВО
ПКС-3. Способность выполнять работы по обеспечению функционирования баз	

Номер семестра*	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения ОПОП ВО
данных и обеспечению их информационной безопасности	
5	Операционные системы
6	Разработка приложений под мобильные устройства
7	Кроссплатформенные приложения
8	Преддипломная практика
8	Выполнение и защита выпускной квалификационной работы

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

Планируемые результаты освоения компетенции. Индикаторы достижения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный не достигнут)	удовлетворительно (минимальный пороговый)	хорошо (средний)	отлично (высокий)	
ПКС-3. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности					
ИД 3.1 **Знать**: Архитектуру систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсные компоненты взаимодействия БД с системами хранения и обработки данных; **ИД 3.2** **Уметь**: Работать с системами хранения и обработки информации; Локализовать проблему работы с ресурсами, возникшую в системе хранения и	Фрагментарные знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки данных;	Неполные знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки данных; Анализа возможностей	Сформированное, но содержащее отдельные пробелы знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в	Сформированные полные знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки	Реферат Доклад Практические, лабораторные работы Экзамен

Планируемые результаты освоения компетенции. Индикаторы достижения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный не достигнут)	удовлетворительно (минимальный пороговый)	хорошо (средний)	отлично (высокий)	
обработки данных; **ИД 3.3** **Иметь навыки**: Анализа воз-можностей по управлению вычислительными ресурсами, взаимодействующими с БД; Управления вычислительными ресурсами, взаимодействующими с БД;	Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с БД; Управления вычислительными ресурсами, взаимодействующими с БД;	по управлению вычислительными ресурсами, взаимодействующими с БД; Управления вычислительными ресурсами, взаимодействующими с БД;	системе хранения и обработки данных; Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с БД Управления вычислительными ресурсами, взаимодействующими с БД;	данных; Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с БД; Управления вычислительными ресурсами, взаимодействующими с БД;	

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

Оценочное средство по компетенции ПКС-3. Способностью выполнять работы по обеспечению функционирование баз данных и их информационной безопасности.

Для текущего контроля

Практические работы по дисциплине **«Информационная безопасность»**

Содержание тем практических (семинарских) занятий (Пз) по дисциплине представлено в следующих 4 файлах,

ИБ Раздел I Организация комплексной ЗИ.pdf

ИБ Раздел II Организационные меры защиты.pdf

ИБ Раздел III Защита от внутренних угроз.pdf

ИБ Раздел IV Защита персональных данных.pdf

имеющихся во всех учебных классах кафедры компьютерных технологий и систем (КТС).

В I разделе представлены материалы по выполнению практическим занятий Пз1–4:

Пз-1 Правовые и нормативно-методологические основы технической защите информации (ЗИ).

Пз-2 Основы технической защиты информации.

Пз-3 Методы и средства защиты информации.

Пз-4 Подготовка и аттестация объекта информатизации по требованиям информационной безопасности.

Во II разделе представлены материалы по темам Пз 5–6:

Пз-5 Практические правила управления ИБ организации.

Пз-6 Аудит ИБ.

В III разделе представлены материалы по темам Пз 7–9:

Пз-7 Внутренние угрозы.

Пз-8 Управление рисками ИБ.

Пз-9 Система управления ИБ организации.

В IV разделе представлены материалы по темам Пз10–11:

Пз-10 Организационно-правовые основы безопасности персональных данных (ПД).

Пз-11 Рекомендации и основные мероприятия по организации и техническому обеспечению безопасности ПД.

Пз 1. Организация комплексной технической ЗИ

Изучаемые вопросы:

1.Актуальность проблемы обеспечения информационной безопасности (ИБ) и защиты информации (ЗИ).

2. Специальные нормативные документы по технической ЗИ.

Задания:

1. Отечественные правовые и нормативно-методологические основы деятельности по ИБ.

2. Сравнительный анализ международных и национальных стандартов ИБ.

Пз 2 Основы технической ЗИ

Изучаемые вопросы:

Классификация информационного ресурса (ИР).

Разработка перечня сведений конфиденциального характера.

2. Угрозы несанкционированного доступа к информации.

Задания:

1. Общие положения и классификация угроз ИБ.

2. Отечественные правовые и нормативно-методологические основы деятельности по ИБ.

3. Технические каналы утечки информации, классификация и и способы реализации.

Пз 3 Методы и средства ЗИ

Изучаемые вопросы:

1. Требования и рекомендации по ЗИ от утечки и по техническим каналам.

2. Основные требования по ЗИ от несанкционированного доступа (НСД) к информации.

Задание:

1. Общие вопросы использования средств криптографической ЗИ.

Пз 4 Подготовка и аттестация объектов по требованиям ИБ

Изучаемые вопросы:

1. Лицензирование деятельности по технической защите конфиденциальной информации (КИ).

2. Категорирование объекта информатизации.

3. Подготовка автоматизированной системы к аттестации по требованиям ИБ.

4. Аттестация объекта информатизации по требованиям ИБ.

Задания:

1. Подготовка защищаемого помещения к аттестации по требованиям ИБ

1. Сертификация средств ЗИ по требованиям ИБ.

3. Методика оценки защищенности КИ от утечки по техническим каналам.

4. Методика аттестационных испытаний системы защиты от НСД.

Пз 5 Практические правила управления ИБ организации

Изучаемые вопросы:

1. Организационная структура обеспечения ИБ.

2. Защита информационных активов (ИА) от физического воздействия.

3. Проблемы разработки, приобретения и обслуживания информационной системы (ИС).

4. Разработка концепции, политик и стандартов ИБ организации.

Задания:

1. Классификация и управление активами.

2. Защита конфиденциальной информации при управлении передачей данных и операционной деятельности.

3. Управление инцидентами ИБ.

4. Основные вопросы управления непрерывностью бизнеса.

Пз 6 Аудит информационной безопасности

Изучаемые вопросы:

1.Актуальность аудита ИБ организации.

2. Проведение аудита ИБ.

Задания:

1. Основные принципы, виды, способы и критерии аудита ИБ.

3. Подготовка к аудиту ИБ предприятия, состав и роли участников.

Пз 7 Внутренние угрозы

Изучаемый вопрос:

1. Персонал компании и безопасность ее информационных активов.

Задание:

1. Процессный подход как основа защиты ИА от внутренних угроз.

Пз-8. Управление рисками ИБ

Изучаемые вопросы:

1. Общие понятия управления информационными ресурсами (ИР).

2. Отработка рисков и факторов, влияющих на выбор средств их минимизации в ИБ.

Задания:

1. Основные внутренние уязвимости информационных активов

2. Анализ рисков ИБ.

Пз-9. Система управления ИБ организации

Изучаемые вопросы:

1. Определение области и границ действия систем управления (СУ) ИБ.

2. Внедрение и функционирование систем управления ИБ организации.

Задание:

1. Роли, обязанности и полномочия по внедрению, мониторингу, анализу и совершенствованию системы управления (СУ) ИБ.

Пз-10. Организационно-правовые основы обеспечения безопасности персональных данных

Изучаемые вопросы:

1. Особенности правового и нормативно-методического регулирования деятельности по обеспечению безопасности ПД.

2. Корпоративные и частные модели угроз по безопасности ПД.

Задание:

1. Использование нормативных документов ФСБ для обеспечения безопасности ПД.

Пз-11 Рекомендации и мероприятия по организации и техническому обеспечению безопасности персональных данных

Изучаемые вопросы:

1. Общий порядок организации обеспечения безопасности персональных данных (ПД) в информационных системах ПД.

2. Классификация ИС ПД.

3. Требования к материальным носителям биометрических ПД и технологиям их хранения вне ИС ПД.

Задания:

1. Классификация ИС ПД.

2. Методы и способы ЗИ от утечки по техническим каналам

Лабораторные работы по дисциплине

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

Лз-2. Создание цифрового сигнала, обеспечивающего требуемый для выживания ОС «эффект системы».

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

Лз-4. Контроль обеспечения безопасности информации.

Лз-5. Применение программных антивирусных комплексов.

Лз- 6. Программирование симметричных и алгебраических алгоритмов шифрования.

Лз7-8. Построение систем защиты информации на основе криптографических преобразований.

Лз-9. Защита программ от изучения.

Лз-10. Система защиты информации Secret Net.

Лз-11. Система защиты информации Net Ware.

Темы докладов:

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Таксономия нарушений ИБ вычислительной системы
6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы ИБ.
8. Модели ИБ и их применение.
9. Классификация средств и методов ИБ от несанкционированного доступа (НСД).
10. Механизмы ИБ от НСД.
11. Государственные требования к системам ИБ.
12. Концепция ИБ от НСД.
13. Особые требования к криптографическим средствам СЗИ.
14. Показатели защищенности средств вычислительной техники (СВТ)
15. Исследование результатов работы антивирусных программ.
16. Алгоритмы электронной цифровой подписи (ЭЦП).
17. Защита файлов и каталогов.
18. Шифрованные логические диски.
19. Криптосистема архиватора WinZip.
20. Уязвимости криптосистемы архиватора Arj.
21. Основные положения национальной стратегии развития искусственного интеллекта на период до 2030 года.
22. Взламывание защиты КС и программ.
23. Средства простановки ключевых меток и защиты программ от копирования.
24. Защита программ при их отладке.
25. Работа пользователей ПК в защищенной среде.

Темы рефератов

1. Классификация компьютерных систем (КС) и требования к защите информации в них.
2. Использование защищенных компьютерных систем.
3. Методы контроля доступа к ресурсам КС.
4. Способы фиксации факта доступа.
5. Структура и функции подсистемы контроля доступа программ и пользователей.
6. Средства активного аудита компьютерных систем.
7. Идентификация и аутентификация субъектов и объектов КС.
8. Идентифицирующая информация и протоколы идентификации.
9. Основные подходы к защите данных от НСД.
10. Иерархический доступ к файлу.
11. Доступ к данным со стороны процесса.
12. Понятие скрытого доступа.
13. Модели управления доступом.
14. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
15. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
16. Активный контроль состояния безопасности КС.
17. Централизованное управление пользователями и контроль их действий.
18. Средства контроля вычислительных процессов.
19. Свойства вычислительных процессов и управление ими.
20. Восстановление удаленных файлов.
21. Средства гарантированного удаления информации.
22. Средства анализа программ.
23. Антивирусные программные комплексы.
24. Настройка и применение антивирусных программ.
25. Устранение проникновения КВ в компьютерную систему
26. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
27. Алгоритмы криптографических преобразований и их характеристики.
28. ЗИ в персонального компьютера (ПК).
29. Перечень и характеристики сертифицированных программно-аппаратных средств (ПАС) СЗИ для ПК.

Вопросы и задания для проведения промежуточного контроля (экзамена)

Вопросы к экзамену

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности страны.

3. Место информационной безопасности в социально-экономических системах.

4. Основные нормативные руководящие документы, касающиеся государственной тайны.

5. Таксономия нарушений ИБ вычислительной системы

6. Три вида возможных нарушений информационной системы

7. Актуальность проблемы информационной безопасности.

8. Модели безопасности и их применение.

9. Классификация методов ИБ от несанкционированного доступа (НСД).

10. Классификация средств ИБ от НСД.

11. Механизмы ИБ от НСД.

12. Государственные требования к системам ИБ.

13. Концепция ИБ от НСД.

14. Требования к криптографическим средствам систем ЗИ (СЗИ).

15. Показатели защищенности средств вычислительной техники (СВТ) от НСД.

16. Классификация компьютерных систем и требования ИБ к них.

17. Использование защищенных компьютерных систем.

18. Методы контроля доступа к ресурсам КС.

19. Способы фиксации факта доступа.

20. Структура и функции подсистемы контроля доступа программ и пользователей.

21. Средства активного аудита компьютерных систем.

22. Идентификация и аутентификация субъектов и объектов КС.

23. Идентифицирующая информация и протоколы идентификации.

24. Основные подходы к защите данных от НСД.

25. Иерархический доступ к файлу.

26. Доступ к данным со стороны процесса.

27. Понятие скрытого доступа.

28. Модели управления доступом.

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

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

31. Построение аппаратных компонент криптозащиты данных.

32. Сущность разрушающих программных средств.

33. Взаимодействие прикладных программ и программы злоумышленника.

34. Классификация разрушающих программных средств и их воздействий.

35. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.

36. Сущность, проявление, классификация КВ.

37. Необходимые и достаточные условия недопущения разрушающих программных воздействий.

38. Понятие изолированной программной среды.

39. Организационные средства защиты от КВ.

40. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.

41. Проблема обеспечение целостности информации.

42. Защита файлов от изменений.

43. Способы обеспечения целостности информации.

44. Электронная цифровая подпись.

45. Криптографические хэш-функции. Схемы вычисления хэш-функции.

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

47. Алгоритмы криптографических преобразований, их характеристики.

48. Методы и средства ограничения доступа к компонентам компьютеров.

49. Построение средств ЗИ для персонального компьютера (ПК).

50. Перечень и характеристики сертифицированных программно-аппаратных средств систем ЗИ от НСД для ПК.

51. Особенности ЗИ в вычислительных сетях.

52. Механизмы реализации атак на вычислительные сети.

53. Защита сетевого файлового ресурса.

54. Определение перечня защищаемых ресурсов и их критичности.

55. Определение категорий персонала и ПАС, на которые распространяется политика безопасности.

56. Определение угроз ИБ.

57. Формирование требований к построению системы ЗИ.

58. Определение уязвимости КС и выбор средств ЗИ.

59. Создание учетных записей пользователей.

60. Создание учетных записей групп.

61. Организация общего доступа к папкам.

62. Активный контроль состояния безопасности КС.

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

64. Централизованное управление пользователями и контроль их действий.

65. Средства контроля вычислительных процессов.

66. Свойства вычислительных процессов и управление ими.

67. Восстановление удаленных файлов.

68. Восстановление отформатированных (дискет) флешек.

69. Средства гарантированного удаления информации.

70. Средства анализа программ.

71. Дизассемблирование программ и исследование кода.

72. Антивирусные программные комплексы.

73. Настройка и применение антивирусных программ.

74. Устранение проникновения КВ в КС.
75. Исследование результатов воздействия КВ на программы в ОС.
76. Исследование результатов работы антивирусных программ.
77. Алгоритмы электронной цифровой подписи.
78. Защита файлов и каталогов. Шифрованные логические диски.
79. Криптосистема архиватора WinZip.
80. Уязвимости криптосистемы архиватора Arj.
81. Основные положения национальной стратегии развития искусственного интеллекта на период до 2030 года.
82. Средства анализа и копирования защищенных флешек (дискет).
83. Взламывание защиты компьютерных программ.
84. Средства простановки ключевых меток и защиты программ от копирования.
85. Исследование дискет, защищенных от копирования
86. Исследование программ с защитой от копирования.
87. Защита программ при их отладке.
88. Защита информации от НСД с помощью СЗИ "Secret Net".
89. Защита информации от НСД в ЛВС с помощью СЗИ "Net Ware".
90. Работа пользователей в защищенной компьютерной среде.

Задания (тесты для проведения экзамена)
Тесты (примеры)

№1 (Балл 1)

Организационные средства обеспечения защиты информации:

1 ○ специальные пакеты программ или отдельные программы, предназначенные для решения задач защиты информации
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 защиты информации
5 ○ различные механические, электронные и т п устройства, встраиваемые в аппаратуру с целью решения задач защиты информации

№2 (1)

Законодательные средства обеспечения защиты информации:

1 ○ специальные пакеты программ или отдельные программы, предназначенные для решения задач защиты информации
2 ○ сложившиеся в обществе нормы или правила, нарушение которых приравнивается к несоблюдению правил поведения
3 ○ механические, электрические, электронные и тп устройства и системы, которые создают препятствия на пути дестабилизирующих факторов
4 ○ мероприятия, специально предусматриваемые в технологии функционирования автоматизированных систем с целью решения задач защиты информации
5 ◉ нормативно-правовые акты, с помощью которых регламентируются права, обязанности и ответственность лиц, имеющих отношение к функционированию системы

№3 (1)

Морально-этические средства обеспечения защиты информации:

1 ○ специальные пакеты программ или отдельные программы, предназначенные для решения задач защиты информации
2 ◉ сложившиеся в обществе нормы или правила, нарушение которых приравнивается к несоблюдению

правил поведения

3 ○ механические, электрические, электронные и т п устройства и системы, которые создают препятствия на пути дестабилизирующих факторов

4 ○ мероприятия, специально предусматриваемые в технологии функционирования автоматизированных систем с целью решения задач защиты информации

5 ○ нормативно-правовые акты, с помощью которых регламентируются права, обязанности и ответственность лиц, имеющих отношение к функционированию системы

№4 (1)

Функциональные требования к системе защиты информации:

1 ○ минимизация затрат на систему Максимальное использование серийных средств

2 ○ структурированность всех компонентов системы Простота эксплуатации

3 ◉ обеспечение решения требуемой совокупности задач защиты Удовлетворение всем требованиям защиты

4 ○ комплексное использование средств Оптимизация архитектуры

5 ○ минимизация помех пользователям Удобство для персонала системы защиты

№5 (1)

Эргономические требования к системе защиты информации:

1 ○ комплексное использование средств Оптимизация архитектуры

2 ◉ Минимизация помех пользователям Удобство для персонала системы защиты

3 ○ минимизация затрат на систему Максимальное использование серийных средств

4 ○ структурированность всех компонентов системы Простота эксплуатации

5 ○ обеспечение решения требуемой совокупности задач защиты Удовлетворение всем требованиям защиты

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

Контроль освоения дисциплины проводится в соответствии с Пл КубГАУ 2.5.1 «Текущий контроль успеваемости и промежуточная аттестация обучающихся».

Текущий контроль по дисциплине позволяет оценить степень восприятия учебного материала и проводится для оценки результатов изучения разделов/тем дисциплины.

Текущий контроль проводится как контроль тематический (по итогам изучения определенных тем дисциплины) и рубежный (контроль определенного раздела или нескольких разделов, перед тем, как приступить к изучению очередной части учебного материала).

Критерии оценки теста:

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.

Реферат

Реферат — это краткое изложение в письменном виде содержания и результатов индивидуальной учебно-исследовательской деятельности, имеет регламентированную структуру, содержание и оформление. Его задачами являются:

1. Формирование умений самостоятельной работы студентов с источниками литературы, их систематизация;
2. Развитие навыков логического мышления;
3. Углубление теоретических знаний по проблеме исследования.

Текст реферата должен содержать аргументированное изложение определенной темы. Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список используемых источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д.

Критериями оценки реферата 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 доклада

Критериями оценки доклада являются:

а) соответствие содержания заявленной теме;

б) актуальность, новизна и значимость темы;

в) четкая постановка цели и задач исследования;

г) аргументированность и логичность изложения;

д) научная новизна и достоверность полученных результатов;

е) свободное владение материалом;

ж) состав и количество используемых источников и литературы;

з) культура речи, ораторское мастерство;

и) выдержанность регламента.

Оценка «**отлично**» — выполнены все требования к выполнению доклада: 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 регламент; доклад хорошо воспринимается на слух.

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

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

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

Критерии оценки практической работы

Оценка «**отлично**» выставляется в том случае, когда обучающийся правильно и полностью выполнил основное задание и, возможно при необходимости, дополнительное задание практической работы, ответил правильно на теоретические вопросы, на дополнительные вопросы. Показал отличные знания и умения при выполнении практической работы в рамках учебного материала.

Оценка «**хорошо**» выставляется в том случае, когда обучающийся правильно и полностью выполнил задание практической работы, ответил на теоретические вопросы с небольшими неточностями, на большинство дополнительных вопросов также, возможно, допуская незначительные ошибки. Показал достаточно хорошие знания и умения при выполнении практической работы в рамках учебного материала.

Оценка «**удовлетворительно**» выставляется в том случае, когда обучающийся правильно выполнил задание практической работы, ответил на теоретические вопросы с существенными неточностями. Показал минимальные удовлетворительные знания и умения при выполнении практической работы в рамках учебного материала.

Оценка «**неудовлетворительно**» выставляется в том случае, когда обучающийся неправильно выполнил задание практической работы, не ответил на теоретические вопросы. Показал недостаточный уровень знаний и умений при выполнении практической работы в рамках учебного материала.

Критерии оценки лабораторной работы

Оценка «**отлично**» выставляется в том случае, когда обучающийся правильно и полностью выполнил основное задание и, возможно при необходимости, дополнительное задание лабораторной работы, ответил правильно на теоретические вопросы, на дополнительные вопросы. Показал отличные знания и умения при выполнении лабораторной работы в рамках учебного материала.

Оценка «**хорошо**» выставляется в том случае, когда обучающийся правильно и полностью выполнил задание лабораторной работы, ответил на теоретические вопросы с небольшими неточностями, на большинство дополнительных вопросов также, возможно, допуская незначительные ошибки. Показал достаточно хорошие знания и умения при выполнении лабораторной работы в рамках учебного материала.

Оценка «**удовлетворительно**» выставляется в том случае, когда обучающийся правильно выполнил задание лабораторной работы, ответил на теоретические вопросы с существенными неточностями. Показал минимальные удовлетворительные знания и умения при выполнении лабораторной работы в рамках учебного материала.

Оценка «**неудовлетворительно**» выставляется в том случае, когда обучающийся неправильно выполнил задание лабораторной работы, не ответил на теоретические вопросы. Показал недостаточный уровень знаний и умений при выполнении лабораторной работы в рамках учебного материала.

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 учебнойсформулированы 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.

8 Перечень основной и дополнительной учебной литературы

Основная учебная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Галатенко В.А.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 266 с.— Режим доступа: http://www.iprbookshop.ru/97562.html

2. Информационная безопасность: учеб. пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. В. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с. https://edu.kubsau.ru/file.php/118/IB_Uch_posobie_21.05.2020_AAA_570178_v1_.PDF

3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные. — Саратов: Профобразование, 2019.— 702 с.— Режим доступа: http://www.iprbookshop.ru/87995.html

Дополнительная учебная литература

1. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов. — Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Режим доступа: http://www.iprbookshop.ru/33430.html

2. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — Режим доступа: http://www.iprbookshop.ru/33857.html

3. Суворова Г.М. Информационная безопасность [Электронный ресурс]: учебное пособие/ Суворова Г.М.— Электрон. текстовые данные. — Саратов: Вузовское образование, 2019.— 214 с.— Режим доступа: http://www.iprbookshop.ru/86938.html

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/

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: https://edu.kubsau.ru/file.php/118/01_Zashchita_informacii_Praktikum_dlja_bakalavrov.pdf

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных 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 лицензионного программного обеспечения

№	Наименование	Краткое описание
1.	Microsoft Windows	Операционная система
2.	Microsoft Office (включает Word, Excel, PowerPoint)	Пакет офисных приложений
3.	Система тестирования INDIGO	Тестирование

11.2 Перечень профессиональных баз данных и информационных справочных систем

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

11.3 Доступ к сети Интернет и ЭИОС 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 — 157,1 кв.м; учебная аудитория для проведения учебных занятий. 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 №1 ЭК, площадь — 64,9 кв.м; посадочных мест — 30; учебная аудитория для проведения учебных занятий 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 №403 ЭК, посадочных мест — 50; площадь — 83,5 кв.м; учебная аудитория для проведения учебных занятий. сплит-система — 2 шт.; специализированная мебель (учебная доска, учебная мебель); технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

		пособий (ноутбук, проектор, экран); программное обеспечение: Windows, Office. Помещение №303 ЭК, посадочных мест — 30; площадь — 63,1 кв.м; учебная аудитория для проведения учебных занятий. 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 №4 ЭК, площадь — 31,1 кв.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 №310 ЭК, площадь — 3,6 кв.м; помещение для хранения и профилактического обслуживания учебного оборудования. лабораторное оборудование (плейер — 1 шт.;); технические средства обучения (сетевое оборудование — 1 шт.; акустическая система — 1 шт.; микрофон — 2 шт.).	
2	Информационная безопасность	Помещение №206 ЭК, посадочных мест — 20; площадь — 41 кв.м.; помещение для самостоятельной работы обучающихся. технические средства обучения (компьютер персональный — 9 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета;	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

		специализированная мебель (учебная мебель). Программное обеспечение: Windows, Office, специализированное лицензионное и свободно распространяемое программное обеспечение, предусмотренное в рабочей программе. Помещение №211а НОТ, посадочных мест — 30; площадь — 47,1 кв.м; помещение для самостоятельной работы обучающихся. технические средства обучения (принтер — 2 шт.; экран — 1 шт.; проектор — 1 шт.; сетевое оборудование — 1 шт.; ибп — 1 шт.; компьютер персональный — 6 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.	