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
«24» апреля 2023

Рабочая программа дисциплины
Информационная безопасность

Направление подготовки
09.03.03 Прикладная информатика

Направленность
Менеджмент проектов в области информационных технологий, создание и поддержка информационных систем

Уровень высшего образования
Бакалавриат

Форма обучения
Очная, заочная

Краснодар
2023

Рабочая программа дисциплины «Информационная безопасность» разработана на основе ФГОС ВО 09.03.03 Прикладная информатика утвержденного приказом Министерства образования и науки РФ 19 сентября 2017 г. № 922.

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

Рабочая программа обсуждена и рекомендована к утверждению решением кафедры компьютерных технологий и систем от 17.04.2023 г., протокол № 10.

Заведующий кафедрой
канд. техн. наук, доцент  Т.В. Лукьяненко

Рабочая программа одобрена на заседании методической комиссии факультета прикладной информатики, протокол от 24.04.2023 № 8.

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

Руководитель
основной профессиональной
образовательной программы
канд. экон. наук, доцент  Д.А. Замотайлова

1 Цель и задачи освоения дисциплины

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

Задачи:

— изучения 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 обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

В результате изучения дисциплины «Информационная безопасность» обучающийся получает знания, умения и навыки для успешного освоения следующих трудовых функций и выполнения трудовых действий:

Профессиональный стандарт *06.016 «Руководитель проектов в области информационных технологий»*.

Обобщенная трудовая функция – *«Управление проектами в области ИТ на основе полученных планов проектов в условиях, когда проект не выходит за пределы утвержденных параметров»*.

Трудовая функция: *Идентификация конфигурации ИС в соответствии с полученным планом A/01.6.*

Трудовые действия:

- Определение базовых элементов конфигурации ИС;
- Присвоение версии базовым элементам конфигурации ИС;
- Установление базовых версий конфигурации ИС.

Трудовая функция: *Аудит конфигураций ИС в соответствии с полученным планом A/03.6.*

Трудовые действия:

- Формальный физический аудит конфигурации ИС;
- Формальный функциональный аудит конфигурации ИС.

Трудовая функция: *Реализация мер по неразглашению информации, полученной от заказчика A/26.6.*

Трудовые действия:

- Организация подписания договоров о неразглашении информации, полученной от заказчика, внутри организации;
- Осуществление мероприятий по обеспечению соблюдения

договоров о неразглашении.

Профессиональный стандарт *06.015 Специалист по информационным системам.*

Обобщенная трудовая функция – *«Выполнение работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы».*

Трудовая функция: *Определение первоначальных требований заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ B/01.5.*

Трудовые действия:

- Выявление первоначальных требований заказчика к типовой ИС;
- Информирование заказчика о возможностях типовой ИС;
- Определение возможности достижения соответствия типовой ИС первоначальным требованиям заказчика;
- Составление протокола переговоров с заказчиком.

Трудовая функция: *Выявление требований к типовой ИС B/07.5.*

Трудовые действия:

- Сбор данных о запросах и потребностях заказчика применительно к типовой ИС;
- Анкетирование представителей заказчика;
- Интервьюирование представителей заказчика;
- Документирование собранных данных в соответствии с регламентами организации.

Обобщенная трудовая функция – *«Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы».*

Трудовая функция: *Определение первоначальных требований заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ C/01.6.*

Трудовые действия:

- Выявление первоначальных требований заказчика к ИС;
- Информирование заказчика о возможностях типовой ИС и вариантах ее модификации;
- Определение возможности достижения соответствия ИС первоначальным требованиям заказчика;
- Составление протокола переговоров с заказчиком.

Трудовая функция: *Выявление требований к ИС C/11.6.*

Трудовые действия:

- Сбор данных о запросах и потребностях заказчика применительно к ИС;
- Анкетирование представителей заказчика;
- Интервьюирование представителей заказчика;
- Документирование собранных данных в соответствии с регламентами организации.

Трудовая функция: *Анализ требований С/12.6.*

Трудовые действия:

- Анализ функциональных и нефункциональных требований к ИС;
- Спецификация (документирование) требований к ИС;
- Проверка (верификация) требований к ИС.

Трудовая функция: *Согласование и утверждение требований к ИС С/13.6.*

Трудовые действия:

- Согласование требований к ИС с заинтересованными сторонами;
- Запрос дополнительной информации по требованиям к ИС;
- Утверждение требований к ИС у руководства.

Трудовая функция: *Управление доступом к данным С/31.6.*

Трудовые действия:

- Определение необходимого уровня прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС;
- Назначение прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС;
- Отмена прав доступа к репозиторию данных о выполнении работ по созданию (модификации) и сопровождению ИС.

В результате освоения дисциплины формируются следующие компетенции:

– способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

– способность проектировать ИС по видам обеспечения (ПК-3);

– способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-10).

3 Место дисциплины в структуре ОПОП ВО

«Информационная безопасность» является дисциплиной обязательной части ОПОП подготовки обучающихся по направлению 09.03.03 «Прикладная информатика», направленность «Менеджмент проектов в области информационных технологий, создание и поддержка информационных систем».

4 Объем дисциплины (108 часов, 3 зачетные единицы)

Виды учебной работы	Объем, часов	
	Очная	Заочная
Контактная работа в том числе: — аудиторная по видам учебных занятий	63 62	11 10
— лекции	30	4
— практические	32	6
— внеаудиторная	1	1
— зачет с оценкой	1	1
— экзамен	–	–
— защита курсовых работ (проектов)	–	–
Самостоятельная работа в том числе:	45	97
— курсовая работа (проект)	–	–
— прочие виды самостоятельной работы	+	+
Итого по дисциплине	108	108
в том числе в форме практической подготовки	0	0

5 Содержание дисциплины

По итогам изучаемой дисциплины студенты (обучающиеся) сдают зачет с оценкой.

Дисциплина изучается: на очной форме обучения на 2 курсе, в 4 семестре, на заочной форме – на 3 курсе, в з/с.

Содержание и структура дисциплины по очной форме обучения

№ п/п	Наименование темы с указанием основных вопросов	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Практические занятия	Самостоятельная работа
1	Объект и предмет защиты. Угрозы и концепция ИБ. Цели и задачи дисциплины. Направления обеспечения ИБ	ОПК-3, ПК-3, ПК-10	4	4	4	4
2	Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. СЗИ от электромагнитных излучений и закладок, несанкционированного изменения структур		4	4	4	6
3	ЗИ от несанкционированного изменения структур и доступа (НСД)		4	4	4	6
4	Компьютерные вирусы и механизмы борьбы с ними. Принципы и методы защиты от РПВ		4	4	4	5
5	Принципы применения криптографической защиты информации. Программно-аппаратные средства шифрования		4	4	4	6
6	Системы криптографической защиты данных на основе плат "КРИПТОН". Защита файлов от изменений		4	4	4	6
7	Защита информации в распределенных компьютерных системах (РКС). Особенности защиты информации в РКС. Теория компьютерных систем защиты информации (КСЗИ)		4	4	4	6
8	Теория компьютерных систем защиты информации (КСЗИ)		4	2	4	6

№ п/п	Наименование темы с указанием основных вопросов	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Практические занятия	Самостоятельная работа
	Курсовая	–	–	х	х	х
Итого				30	32	45

Содержание и структура дисциплины по заочной форме обучения

№ п/п	Наименование темы с указанием основных вопросов	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Практические занятия	Самостоятельная работа
1	Объект и предмет защиты. Угрозы и концепция ИБ. Цели и задачи дисциплины. Направления обеспечения ИБ	ОПК-3, ПК-3, ПК-10	3, з/с	1		12
2	Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. СЗИ от электромагнитных излучений и закладок, несанкционированного изменения структур		3, з/с	1		12
3	ЗИ от несанкционированного изменения структур и доступа (НСД)		3, з/с	1	1	12
4	Компьютерные вирусы и механизмы борьбы с ними. Принципы и методы защиты от РПВ		3, з/с	1	1	12
5	Принципы применения криптографической защиты информации. Программно-аппаратные средства шифрования		3, з/с		1	12
6	Системы криптографической защиты данных на основе плат "КРИПТОН". Защита файлов от изменений		3, з/с		1	12

№ п/п	Наименование темы с указанием основных вопросов	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Практические занятия	Самостоятельная работа
7	Защита информации в распределенных компьютерных системах (РКС). Особенности защиты информации в РКС. Теория компьютерных систем защиты информации (КСЗИ)		3, з/с		1	12
8	Теория компьютерных систем защиты информации (КСЗИ)		3, з/с		1	13
	Курсовая	–	–	х	х	х
Итого				4	6	97

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

6.1 Методические указания (собственные разработки)

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

6.2 Литература для самостоятельной работы

Основная литература:

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

2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677

3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. — Брянск : Брянский государственный технический университет, 2012. — 268 с. — ISBN 978-89838-487-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/6991.html

Дополнительная литература:

1. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2010.— 328 c.— Режим доступа: http://www.iprbookshop.ru/10746

2. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В.Г. Спицын. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 c. — 978-5-4332-0020-3. — Режим доступа: http://www.iprbookshop.ru/13936.html

3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89453.html

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
ОПК-3 способен 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
1	Деловая коммуникация
1, 2	Алгоритмизация и программирование
2	Вычислительные системы, сети и телекоммуникации
2	Экономика фирмы (предприятия)
2	Учебная практика: ознакомительная практика
2, 3	Информационные системы и технологии
3	Базы данных
4	Информационная безопасность
4	Производственная практика: технологическая (проектно-технологическая) практика
8	Выполнение и защита выпускной квалификационной работы
ПК-3 способность проектировать ИС по видам обеспечения	

Номер семестра*	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения ОПОП ВО
3	Базы данных
4	Теория систем и системный анализ
4	Информационная безопасность
4	Архитектура информационных систем
4, 5	Проектирование информационных систем
5	Имитационное моделирование
5, 6	Методы хранения и анализа данных
6	Производственная практика: эксплуатационная
6	Современные методы, технологии и информационные системы поддержки принятия решений
6, 7	Проектный практикум
6, 7	Стандартизация и управление IT-проектами
8	Интеллектуальные информационные системы
8	Производственная практика: преддипломная
8	Выполнение и защита выпускной квалификационной работы
ПК-10 способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	
4	Информационная безопасность
4	IT-стратегия организаций
4, 5	Проектирование информационных систем
6	Производственная практика: эксплуатационная
6, 7	Стандартизация и управление IT-проектами
8	IT-инфраструктура предприятий (организаций)
8	Производственная практика: преддипломная
8	Выполнение и защита выпускной квалификационной работы

* номер семестра соответствует этапу формирования компетенции

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)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности					
ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки	Отсутствуют все необходимые знания, умения и навыки, необходимые для решения стандартных задач профессиональной деятельности на основе информационной безопасности и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности.	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Владеет навыками подготовки обзоров, аннотаций, составления	Доклады, тесты, кейс-задание, зачет с оценкой (вопросы и задания)

Планируемые результаты освоения компетенции Индикаторы достижения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.				рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	
ПК-3. Способность проектировать ИС по видам обеспечения					
ПК-3.1 Знает существующие методы построения моделей социально-экономических и организационно-технических систем, их архитектуры, а также теорию и средства проектирования структур данных и информационных процессов для проектирования ИС. ПК-3.2. Умеет анализировать данные, полученные по результатам моделирования, проектировать ИС и проводить верификацию её архитектуры. ПК-3.3. Владеет навыками применения современных инструментальных средств, при разработке моделей и проектировании информационных	Отсутствуют все необходимые знания, умения и навыки, необходимые для проектирования информационных систем по видам обеспечения.	Знает существующие методы построения моделей социально-экономических и организационно-технических систем, их архитектуры, а также теорию и средства проектирования структур данных и информационных процессов для проектирования ИС.	Знает существующие методы построения моделей социально-экономических и организационно-технических систем, их архитектуры, а также теорию и средства проектирования структур данных и информационных процессов для проектирования ИС. Умеет анализировать данные, полученные по результатам моделирования, проектировать ИС и проводить верификацию её архитектуры.	Знает существующие методы построения моделей социально-экономических и организационно-технических систем, их архитектуры, а также теорию и средства проектирования структур данных и информационных процессов для проектирования ИС. Умеет анализировать данные, полученные по результатам моделирования, проектировать ИС и проводить верификацию её архитектуры. Владеет навыками применения современных инструментальных средств, при разработке моделей и проектировании информационных	Доклады, тесты, кейс-задание, зачет с оценкой (вопросы и задания)

Планируемые результаты освоения компетенции Индикаторы достижения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
процессов для разработки ИС.				процессов для разработки ИС.	
ПК-10. Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью					
ПК-10.1. Знает методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС. ПК-10.2. Умеет применять методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС. ПК-10.3. Владеет навыками организации ИТ-инфраструктуры и управления информационной безопасностью, в т.ч., обеспечения и контроля соответствия технических, программных и коммуникационных средств для функционирования ИС, разграничение прав доступа к ИС.	Отсутствуют все необходимые знания, умения и навыки, необходимые для участия в организации ИТ-инфраструктуры и управления информационной безопасностью.	Знает методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС.	Знает методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС. Умеет применять методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС.	Знает методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС. Умеет применять методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС. Владеет навыками организации ИТ-инфраструктуры и управления информационной безопасностью, в т.ч., обеспечения и контроля соответствия технических, программных и коммуникационных средств для функционирования ИС, разграничение прав доступа к ИС.	Доклады, тесты, кейс-задание, зачет с оценкой (вопросы и задания)

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

Кейс-задания

Пример кейс-задания

Под **информационной безопасностью** понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в т.ч. владельцам и пользователям информации и поддерживающей инфраструктуре. Обоснуйте или опровергните это понимания ИБ.

Обеспечение ИБ является сложной задачей, для решения которой, требуется, комплексный подход. Выделяют следующие 4 уровни защиты информации (ЗИ): законодательный, аминистративный, процедурный и программно-технический.

Опишите состав этих уровней и укажите, какой уровень является основой для построения системы защиты информации (СЗИ), т.к. он дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников.

Тесты

Примеры тестов

№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 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;

№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;

№6 (1)

Экономические 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;

№7 (1)

Технические 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;

№8 (1)

Организационные 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;

№9 (1)

Техническое обеспечение средств защиты информации:

1 ○ совокупность методов, моделей и алгоритмов, необходимых для оценок уровня защищенности информации и решения других задач защиты;

2 ○ совокупность систем классификации и кодирования данных о защите информации, массивы данных средств защиты информации, а также входные и выходные документы средств защиты информации;

3 ○ совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов средств ЗИ между собой, с компонентами автоматизированной системы и с внешней средой;

4 ○ совокупность программ, необходимых для решения задач управления механизмами защиты.

5 ○ совокупность средств, необходимых для поддержки решения всех задач защиты информации в процессе функционирования средств ЗИ;

№10 (1)

Математическое обеспечение средств защиты информации:

1 ○ совокупность методов, моделей и алгоритмов, необходимых для оценок уровня защищенности информации и решения других задач защиты;

2 ○ совокупность систем классификации и кодирования данных о защите информации, массивы данных средств защиты информации, а также входные и выходные документы средств защиты информации;

3 ○ совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов средств защиты информации между собой, с компонентами автоматизированной системы и с внешней средой;

4 ○ совокупность программ, необходимых для решения задач управления механизмами защиты;

5 ○ совокупность средств, необходимых для поддержки решения всех задач защиты информации в процессе функционирования средств защиты информации;

Доклады

Примеры тем докладов

1. Место и роль информации в функционировании и развитии открытых систем.
2. Международные стандарты описания функционирования и развития информационных технологий (ИТ) и открытых систем (ОИ).
3. Место и роль законодательного уровня в построении систем защиты информации, разработке концепция информационной безопасности страны.
4. Место информационной безопасности (ИБ) в экономических системах.
5. Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации.
6. Таксономия нарушений ИБ в вычислительных системах.
7. Три вида возможных нарушений ИБ в информационных системах.
8. Актуальность проблемы ИБ.
9. Суть моделей информационной безопасности и особенности их применения.
10. Основные понятия ИБ: информация, информационные технологии, информационные системы и их взаимосвязи.

11. Сущность персональных данных и необходимость обеспечения их безопасности.

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

13. Механизмы ИБ от несанкционированного доступа (НСД) к данным.

14. Государственные требования к системам ИБ.

15. Особые требования к криптографическим средствам защиты информации (ЗИ).

16. Показатели защищенности средств вычислительной техники (СВТ)

Вопросы к зачету с оценкой

ОПК-3 способен 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.
11. Механизмы защиты информации от НСД.
12. Государственные требования к построению СЗИ.
13. Концепция защиты информации от НСД.
14. Особые требования к криптографическим средствам СЗИ от НСД.
15. Показатели защищенности СВТ от НСД.

«ПК-3. Способность проектировать ИС по видам обеспечения»

1. Классификация КС и требования по защите информации.
2. Использование защищенных компьютерных систем.
3. Методы контроля доступа к ресурсам компьютерной системы.
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.

«ПК-10. Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью»

1. Сущность, проявление, классификация компьютерных вирусов.
2. Необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.
3. Организационные средства защиты от компьютерных вирусов.
4. Роль морально-этических факторов в устранении угрозы РПВ.
5. Проблема обеспечение целостности информации.
6. Защита файлов от изменений. Способы обеспечения целостности информации.
7. Электронная цифровая подпись. Криптографические хэш-функции. Схемы вычисления хэш-функции.
8. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
9. Алгоритмы криптографических преобразований и их характеристики.
10. Методы и средства ограничения доступа к компонентам ЭВМ.
11. Построение средств защиты информации для ПЭВМ.
12. Перечень и краткая характеристика сертифицированных программно-аппаратных систем защиты информации (СЗИ) от НСД для ПЭВМ.
13. Особенности защиты информации в вычислительных сетях.
14. Механизмы реализации атак на вычислительные сети.
15. Защита сетевого файлового ресурса.
16. Построение аппаратных компонент криптозащиты данных.
17. Сущность разрушающих программных средств.
18. Взаимодействие прикладных программ и программы-злоумышленника.
19. Классификация разрушающих программных средств и их воздействий.
20. Компьютерные вирусы как особый класс РПВ.

Практическое задание на зачет с оценкой.

По предоставленной преподавателем исходной информации по предприятию, дайте определение угрозам информационной безопасности и укажите, какое место и какую роль в нарушении ИБ играют атака и злоумышленник.

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

Критериями оценки доклада являются: качество текста, обоснованность выбора источников литературы, степень раскрытия сущности вопроса, соблюдения требований к оформлению и представлению результатов.

Оценка «**отлично**» — выполнены все требования к написанию реферата, представлению 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 объём; соблюдены требования к внешнему оформлению.

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

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

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

Оценочный лист доклада

ФИО обучающегося _____

Группа_____ преподаватель _____

Дата_____

Наименование показателя	Недостатки и замечания	Оценка
Качество		
1. Соответствие содержания заданию		
2. Грамотность изложения и качество оформления		
3. Самостоятельность выполнения,		
1. Глубина проработки материала,		
2. Использование рекомендованной и справочной литературы		
6. Обоснованность и доказательность выводов		
Общая оценка качества выполнения		

Защита реферата (Представление доклада)		
1. Свободное владение профессиональной терминологией		
2. Способность формулирования цели и основных результатов при публичном представлении результатов		
3. Качество изложения материала (презентации)		
Общая оценка за защиту реферата		
Ответы на дополнительные вопросы		
Вопрос 1.		
Вопрос 2.		
Вопрос 3.		
Общая оценка за ответы на вопросы		
Итоговая оценка		

Критерии оценки знаний при проведении тестирования

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

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

Оценка «**удовлетворительно**» выставляется при условии правильного ответа студента не менее чем на 51 %;

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

Критерии оценки знаний обучающихся при выполнении кейс-заданий:

– полнота проработки ситуации;

– полнота выполнения задания;

– новизна и неординарность представленного материала и решений;

– перспективность и универсальность решений;

– умение аргументировано обосновать выбранный вариант решения.

Кейс-задание не предусматривает выставления оценки.

Критерии оценки на зачете с оценкой

Оценка «**отлично**» выставляется обучаемому, 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 учебной 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.

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

8 Перечень основной и дополнительной учебной литературы

Основная литература:

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

2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова

Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677

3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. — Брянск : Брянский государственный технический университет, 2012. — 268 с. — ISBN 978-89838-487-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/6991.html

Дополнительная литература:

1. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2010.— 328 с.— Режим доступа: http://www.iprbookshop.ru/10746

2. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В.Г. Спицын. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 с. — 978-5-4332-0020-3. — Режим доступа: http://www.iprbookshop.ru/13936.html

3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89453.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

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 презентаций, учебных фильмов; контролировать результаты обучения на основе компьютерного тестирования.

Программное обеспечение:

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

Перечень современных профессиональных баз данных, информационных справочных и поисковых систем

№	Наименование	Тематика	Электронный адрес
1.	Гарант	Правовая	https://www.garant.ru/
2.	Консультант	Правовая	https://www.consultant.ru/
3.	Научная электронная библиотека «eLIBRARY.RU»	Универсальная	https://elibrary.ru

Доступ к сети Интернет и ЭИОС университета

12 Материально-техническое обеспечение для обучения по дисциплине

Планируемые помещения для проведения всех видов учебной деятельности

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
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 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.);	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

	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.).	
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; 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
Информационная безопасность	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.;	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

	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	