МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «КАБАРДИНО-БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. Х.М. БЕРБЕКОВА» (КБГУ)

ИНСТИТУТ ИНФОРМАТИКИ, ЭЛЕКТРОНИКИ И РОБОТОТЕХНИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель образовательной программы _____ А.С.Ксенофонтов

«____» _____ 2019 г.

УТВЕРЖДАЮ

Директор института ИЭиР
_____ Н.В. Черкесова

«____» _____2019г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Направление подготовки (специальность)
10.03.01 – информационная безопасность

Профиль
Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Нальчик 2019

Рабочая программа дисциплины (модуля) «Основы информационной безопасности» / сост. Ксенофонтов А.С. – Нальчик: КБГУ, 2019. – 35 с.

Рабочая программа предназначена для студентов очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность профиль «Информационно-аналитические системы финансового мониторинга» 2 семестра, 1 курса.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1515.

С О Д Е Р Ж А Н И Е

1.	Цели и задачи освоения дисциплины	4
2.	Место дисциплины (модуля) в структуре ОПОП ВО	4
3.	Требования к результатам освоения дисциплины (модуля)	4
4.	Содержание и структура дисциплины (модуля)	6
5.	Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации	9
6.	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности	28
7.	Учебно-методическое обеспечение дисциплины (модуля)	31
7.1.	*Нормативно-законодательные акты*	*31*
7.2.	*Основная литература*	*31*
7.2.	*Дополнительная литература*	*32*
7.3.	*Периодические издания (газета, вестник, бюллетень, журнал)*	*31*
7.4.	*Интернет-ресурсы*	*31*
7.5.	*Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы*	*32*
8.	Материально-техническое обеспечение дисциплины (модуля)	39

1. Цель и задачи освоения дисциплины (модуля)

Целями освоения дисциплины «Основы информационной безопасности» являются:

- развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений;
- расширение кругозора в вопросах информационной безопасности.

Основные **задачи** дисциплины дать знания по вопросам:

- обеспечения информационной безопасности государства;
- изучить основные положения Доктрины информационной безопасности РФ;
- дать знания основ организационно-правового обеспечения защиты информации;
- методологии создания систем защиты информации;
- процессов защищенного сбора, передачи и накопления информации;
- методов и средств ведения информационных войн;
- оценки защищенности и обеспечения информационной безопасности компьютерных систем;
- дать знания основ комплексной системы защиты информации;
- сформировать основы для дальнейшего самостоятельного изучения вопросов обеспечения компьютерной и информационной безопасности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы информационной безопасности» относится к базовой части Блока 1 «Дисциплины (модули)» основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность, профиль «Информационно-аналитические системы финансового мониторинга».

Изучение дисциплины «Основы информационной безопасности» базируется на сумме знаний, полученных студентами в ходе освоения следующих дисциплин: «Базовая компьютерная подготовка обеспечения информационной безопасности», «Информационные технологии», «Физика», «Математика».

Для освоения данной дисциплины, студенты должны владеть следующими знаниями: уметь использовать нормативно-справочные документы, иметь навыки хранения, обработки, передачи и защиты информации; уметь работать с информацией из различных источников; знать виды информационной безопасности и методы защиты информации в них.

Дисциплина позволит расширить теоретическую подготовку бакалавра, получить практические навыки по обеспечению информационной безопасности объекта защиты.

Освоение основных положений данной дисциплины необходимо для получения знаний необходимых при изучении следующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Теория информационной безопасности и методология защиты информации», «Безопасность систем баз данных», «Инженерно-техническая защита информации», прохождения преддипломной практики и написания выпускной квалификационной работы (бакалаврской работы).

3. Требования к результатам освоения дисциплины (модуля)

В совокупности с другими дисциплинами профиля «Информационно-аналитические системы финансового мониторинга» дисциплина «Основы информационной безопасности» направлена

на формирование следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата):

общекультурные компетенции (ОК)

ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности;

обще-профессиональные компетенции (ОПК):

ОПК-5 - способностью использовать нормативные правовые акты в профессиональной деятельности;

ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате изучения дисциплины «Основы информационной безопасности» студент должен:

знать:

- цели, задачи, принципы и основные направления обеспечения информационной безопасности государства;
- основные термины по проблематике информационной безопасности; методологию создания систем защиты информации;
- перспективные направления развития средств и методов защиты информации;
- роль и место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства;
- содержание информационной войны, методы и средства ее ведения;
- современные подходы к построению систем защиты информации;
- компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну;

уметь:

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований;

владеть:

- навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

4. *Содержание и структура дисциплины* **Код контролируемой компетенции (или ее части)**

В таблице 1 приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы (ЛР), коллоквиум (К), рубежный контроль (РК), тестирование (Т).

Таблица 1.

Содержание дисциплины (модуля)»Основы информационной безопасности»

№ п/п	Наименование раздела	Содержание раздела	Код контролируемой компетен-	Форма текущего контроля

			ции (или ее части)	
1	2	3		4[1]
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.	ОК-4, ОПК-5, ОПК-7	ДЗ; ЛР; Т; К; Р, КП; РК
2.	Информационная война, методы и средства ее ведения	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Содержание информационного противоборства на межгосударственном уровне. Содержание информационного противоборства на военном уровне.	ОК-4, ОПК-5	ДЗ; ЛР; Т; К; Р, КП; РК
3.	Критерии защищенности компьютерных систем	Методы и средства обеспечения информационной безопасности компьютерных систем. Методы оценки защищенности компьютерных систем от НСД.	ОПК-5, ОПК-7	ДЗ; ЛР; Т; К; Р, КП; РК
4.	Защита информации, обрабатываемой в автоматизированных системах, от технических разведок	Классификация и возможности технических разведок Компьютерная разведка. Технические каналы утечки информации при эксплуатации АС. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок.	ОПК-7	ДЗ; ЛР; Т; К; Р, КП; РК
5.	Защита АС и СВТ от внешнего электромагнитного воздействия	Генераторы электромагнитных импульсов. Эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ. Методы защиты АС и СВТ от внешнего электромагнитного воздействия.	ОПК-7	ДЗ; ЛР; Т; К; Р, КП; РК
6.	Использование защищенных компьютерных систем.	Основные технологии построения защищенных систем. Методы криптографии.	ОПК-7	ДЗ; ЛР; Т; К; Р, КП; РК

На изучение курса отводится 144 часа (4 з.е.), из них: контактная работа 51 ч., в том числе лекционных – 17 часов; лабораторных – 34 часа; самостоятельная работа студента 66 часов; завершается экзаменом (27 часов).

[1] В графе 4 приводятся планируемые формы текущего контроля: защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), домашнего задания (ДЗ) написание реферата (Р), эссе (Э), коллоквиум (К), рубежный контроль (РК), тестирование (Т) и т.д.

Структура дисциплины (модуля) «Основы информационной безопасности»

Таблица 2.

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)

Вид работы	Трудоемкость, часов / зачетных единиц	
	2 семестр	всего
Общая трудоемкость (в зачетных единицах)	**144**	**144**
Контактная работа (в часах):	**51**	**51**
Лекции (Л)	*17*	*17*
Практические занятия (ПЗ)	*Не предусмотрены*	*Не предусмотрены*
Семинарские занятия (СЗ)	*Не предусмотрены*	*Не предусмотрены*
Лабораторные работы (ЛР)	*34*	*34*
Самостоятельная работа (в часах):	**66**	**66**
Расчетно-графическое задание	*Не предусмотрены*	*Не предусмотрены*
Реферат (Р)	3	3
Эссе (Э)	*Не предусмотрены*	*Не предусмотрены*
Контрольная работа (КР)	*Не предусмотрены*	*Не предусмотрены*
Самостоятельное изучение разделов	43	43
Курсовой проект (КП), курсовая работа (КР)	20	20
Подготовка и прохождение промежуточной аттестации	27	27
Вид промежуточной аттестации	**Экзамен**	**Экзамен**

Таблица 3.

Лекционные занятия

№ п/п	Тема
1.	**Информационная безопасность.** Понятие информационной безопасности. Основные понятия и определения источники возникновения информационных угроз. Состав и методы организационно-правовой защиты информации. Принципы организации разноуровнего доступа в АИС. Основные составляющие информационной безопасности. категории: обеспечение доступности, целостности и конфиденциальности. Основные принципы обеспечения информационной безопасности предприятия. Важность и сложность проблемы информационной безопасности.
2.	**Законодательный уровень обеспечения ИБ.** Меры законодательного уровня ИБ. Правовые акты общего назначения. Закон «Об информации, информатизации и защите информации». Оценочные стандарты в области информационной безопасности. Положения «Оранжевой книги». Классы защищенности компьютерных систем по «Оранжевой книге». Структура требований «Оранжевой книги». Механизмы безопасности «Оранжевой книги». Классы безопасности «Оранжевой книги». Руководящие документы Гостехкомиссии РФ. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Виды требований информационной

	безопасности. Угрозы информационной безопасности. Профиль защиты.
3.	**Принципы обеспечения информационной безопасности.** Проблемы информационной безопасности. Угрозы информационной безопасности. Примеры реализации угрозы нарушения конфиденциальности. Вредоносное программное обеспечение. Модели и принципы защиты информации от несанкционированного доступа. Методы антивирусной защиты информации. **Идентификация и аутентификация пользователей** Системы аутентификации. Парольные схемы аутентификации. Основные компоненты парольной схемы. Использование одноразовых паролей. Схемы аутентификации с третьей доверенной стороной. Аутентификация Kerberos. Аудит в информационных системах. Функции и назначение аудита. Протоколирование и аудит. Активный аудит. **Управление доступом** Основные типы политики управления доступом. Модель произвольного доступа (дискреционная модель). Модель принудительного доступа (мандатная модель). Контроль прав доступа.
4.	**Угрозы информационной безопасности** Анализ угроз информационной безопасности. Причины возникновения угроз. Классификация угроз. Модель осуществления угроз. Основные направления реализации информационных угроз. **Атаки на информационную систему.** Понятие атаки на информационную систему. Классификация атак. Системность, Комплексность. Непрерывность защиты. Разумная достаточность. Гибкость управления и применения. Открытость алгоритмов и механизмом защиты. Простота применения защитных мер и средств. Системность средств защиты информации. Комплексность систем защиты. Средства защиты информационных систем.
5.	**Кодирование информации** Кодирование – обработка информации. Три способа кодирования текста. Кодирование символьной информации в ЭВМ. Кодирование числовой информации в ЭВМ. Представление графической информации в ЭВМ. Представление звука в ЭВМ. **Криптографические методы защиты информации** Требования к системам криптографической защиты. Шифрование - метод защиты информации . Простейшие методы шифрования текста. Системы криптографической защиты информации. Криптографические средства защиты данных. Использование средств криптографической защиты для предотвращения угроз ИБ. Требования к системам криптографической защиты. Классификация алгоритмов шифрования. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Требования к алгоритмам шифрования.
6.	**Информационная безопасность в деятельности организаций** Классификация угроз информационной безопасности. Угроза нарушения конфиденциальности. Понятие политики безопасности. Административный уровень защиты информации. Синхронизация программы безопасности с жизненным циклом системы. Управление доступом. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня. Физическая защита. Поддержка работоспособности ИС. Поддержка работоспособности. Планирование восстановительных работ. **Электронная цифровая подпись** Понятие цифровой подписи. Законодательный уровень применения цифровой подписи. Закон №1-ФЗ «Об электронной цифровой подписи». Законодательный уровень применения цифровой подписи. Основные понятия закона об ЭЦП. Сертификат ключа электронной цифровой подписи. Условия использования электронной цифровой подписи. Механизм формирования электронной цифровой подписи. Условия использования электронной

	цифровой подписи.
7.	**Аппаратные средства защиты информации** Наиболее распространенные аппаратные средства. Классификация аппаратных средств. Закладное устройство. Виды закладных устройств. Обнаружение радиозакладных устройств. Поиск закладных устройств. Многоканальный комплекс «Спектр – Professional». Компьютерный комплекс «Омега». Автоматизированный комплекс радиомониторинга и поиска закладных устройств. обнаружения и измерения излучений от устройств ЭВТ «АКОР-2ПК». Средства обнаружения утечки информации. Средства акустического и вибро-акустического зашумления. Схема утечки информации с помощью микрофона. Схема лазерного канала утечки информации. Схема перехвата путем подключения аппаратуры к ВЧ. ВЧ – навязывание. Аппаратные средства восстановления данных. Восстановление данных при различных ситуациях. **Технические каналы утечки информации** Классификация технических каналов утечки информации. Технические каналы утечки информации, обрабатываемой ТСПИ. Технические каналы утечки информации при передаче ее по каналам связи. Технические каналы утечки информации при передаче ее по каналам связи. Технические каналы утечки речевой информации. Технические каналы утечки видовой информации. Классификация технических каналов утечки информации по физической природе носителя. Классификация акустических каналов утечки информации. Средства акустической разведки.

Таблица 4. Практические занятия (семинарские занятия) – учебным планом не предусмотрены

Таблица 5.

Лабораторные работы по дисциплине (модулю)

№ п/п	Тема
1.	Конфиденциальная информация
2.	Нормативные акты, определяющие основы информационной безопасности в России
3.	Защита информации с помощью пароля
4.	Основы криптографической защиты информации Защита информации шифром перестановки
5.	Защита информации шифром сложной замены
6.	Шифрование с открытым или асимметричным ключом
7.	Кодирование информации методом Шеннона-Фено
8.	Вычисление и проверка подлинности электронной подписи
9.	Работа алгоритма корректирующего кода Хэмминга
10.	Работа с антивирусными программами
11.	Защита от несанкционированного доступа и сетевых хакерских атак
12.	Определение уровней акустических сигналов защищаемого помещения
13.	Расчет информационных рисков объекта информатизации
14.	Технические каналы утечки видовой информации
15.	Анализ технической защищенности объекта информатизации

Таблица 6.

Самостоятельное изучение разделов дисциплины (модуля)

№ п/п	Вопросы, выносимые на самостоятельное изучение
1.	Понятие национальной безопасности.
2.	Роль информационной безопасности в обеспечении национальной безопасности государства.
3.	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение.
4.	Внешние источники угроз.
5.	Внутренние источники угроз.
6.	Направления обеспечения информационной безопасности государства.
7.	Проблемы региональной информационной безопасности.
8.	Содержание информационного противоборства на межгосударственном уровне
9.	Информационное оружие, его классификация и возможности.
10.	Методы и средства обеспечения информационной безопасности компьютерных систем
11.	Программно-аппаратные средства обеспечения информационной безопасности.
12.	Методы оценки защищенности компьютерных систем от НСД.
13.	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
14.	Классификация и возможности технических разведок
15.	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок.
16.	Методы защиты АС и СВТ от внешнего электромагнитного воздействия.

5. Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

В ходе изучения дисциплины предусматриваются ***текущий, рубежный контроль и промежуточная аттестация.***

5.1. Оценочные материалы для текущего контроля. *Цель текущего контроля* – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины «Основы информационной безопасности» и включает: ответы на теоретические вопросы на практическом занятии, решение практических задач и выполнение заданий на лабораторном занятии, самостоятельное выполнение индивидуальных домашних заданий (например, решение задач) с отчетом (защитой) в установленный срок, написание рефератов, дискуссии.

Оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы начисляются в зависимости от сложности задания.

Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине «Информационные технологии в экологии». Развёрнутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

3 балла	**2 балла**	**1 балл**	**0 баллов**

ставится, если обучающийся: 1) полно излагает изученный материал, даёт правильное определенное экономических понятий; 2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; 3) излагает материал последовательно и правильно с точки зрения норм литературного языка.	ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого.	ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но: 1) излагает материал неполно и допускает неточности в определении понятий; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.	ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.

Баллы «1», «2», «3» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных на протяжении занятия. начисляются в зависимости от сложности задания.

5.1.1. Вопросы по темам дисциплины «Основы информационной безопасности»

Тема 1. Информационная безопасность.

- Понятие информационной безопасности. Основные понятия и определения источники возникновения информационных угроз.
- Состав и методы организационно-правовой защиты информации. Принципы организации разноуровнего доступа в АИС.
- Основные составляющие информационной безопасности. категории: обеспечение доступности, целостности и конфиденциальности.
- Основные принципы обеспечения информационной безопасности предприятия. Важность и сложность проблемы информационной безопасности.

Тема 2. Законодательный уровень обеспечения ИБ.

- Меры законодательного уровня ИБ. Правовые акты общего назначения.
- Закон «Об информации, информатизации и защите информации».
- Оценочные стандарты в области информационной безопасности.
- Положения «Оранжевой книги». Классы защищенности компьютерных систем по «Оранжевой книге». Структура требований «Оранжевой книги».
- Механизмы безопасности «Оранжевой книги». Классы безопасности «Оранжевой книги».
- Руководящие документы Гостехкомиссии РФ. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
- Виды требований информационной безопасности. Угрозы информационной безопасности. Профиль защиты.

Тема 3. Принципы обеспечения информационной безопасности.

- Угрозы информационной безопасности. Примеры реализации угрозы нарушения конфиденциальности.
- Вредоносное программное обеспечение. Модели и принципы защиты информации от несанкционированного доступа.
- Идентификация и аутентификация пользователей
- Парольные схемы аутентификации.
- Управление доступом

Тема 4. Угрозы информационной безопасности

- Анализ угроз информационной безопасности. Причины возникновения угроз. Классификация угроз. Модель осуществления угроз. Основные направления реализации информационных угроз.
- Атаки на информационную систему.
- Открытость алгоритмов и механизмом защиты. Простота применения защитных мер и средств.
- Средства защиты информационных систем.

Тема 5. Криптографические методы защиты информации

- Кодирование информации
- Требования к системам криптографической защиты.
- Простейшие методы шифрования текста.
- Системы криптографической защиты информации.
- Требования к системам криптографической защиты.
- Классификация алгоритмов шифрования. Симметричные и асимметричные алгоритмы шифрования.

Тема 6. Информационная безопасность в деятельности организаций

- Угроза нарушения конфиденциальности.
- Понятие политики безопасности. Административный уровень защиты информации.
- Управление доступом.
- Физическая защита.
- Поддержка работоспособности ИС.
- Электронная цифровая подпись
- Законодательный уровень применения цифровой подписи. Закон №1-ФЗ «Об электронной цифровой подписи».
- Сертификат ключа электронной цифровой подписи.
- Механизм формирования электронной цифровой подписи.

Тема 7. Аппаратные средства защиты информации

- Классификация аппаратных средств.
- Закладное устройство. Виды закладных устройств. Обнаружение радиозакладных устройств.
- Средства обнаружения утечки информации.
- Аппаратные средства восстановления данных.
- Технические каналы утечки информации
- Технические каналы утечки информации при передаче ее по каналам связи.
- Технические каналы утечки речевой информации.
- Технические каналы утечки видовой информации.
- Средства акустической разведки.

Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине «Основы информационной безопасности». Развёрнутый ответ студента должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

5 баллов, ставится, если обучающийся:

1) полно излагает изученный материал, даёт правильное определенное экономических понятий;
2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные;
3) излагает материал последовательно и правильно с точки зрения норм литературного языка.

4 балла, ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого.

3 балла, ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но:

1) излагает материал неполно и допускает неточности в определении понятий;
2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;
3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.

0 баллов, ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.

Баллы «5», «4», «3» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных студентом на протяжении занятия

5.1.2. Оценочные материалы для выпонения лабораторных работ

Задания для лабораторных работ

Выполнение лабораторных работ дисциплины «Основы информационной безопасности» заключается в достижении результатов: заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации.

Лабораторная работа №1. Методология проведения аудита информационной безопасности объекта;

-Основные принципы аудита информационной безопасности

-Понятие «аудит информационной безопасности объекта»

-Этапы проведения аудита информационной безопасность

Лабораторная работа №2. Сбор исходных данных для аудита информационной безопасности АИТКС;

-Критерии аудита информационной безопасности

-Что является исходными данными для аудита информационной безопасности АИТКС

-Как происходит сбор исходных данных для аудита информационной безопасности?

Лабораторная работа №3. Выявление уязвимостей информационной системы;

-Понятие «уязвимость»
-Виды уязвимостей информационной системы
-Методика анализа защищенности ИС
-Как происходит выявление уязвимостей информационной системы?
Лабораторная работа №4. Определение рисков от реализации угроз АИТКС;
-Понятие «риск»
-Методы оценки рисков информационной безопасности
-Какие существуют этапы проведения анализа рисков?
Лабораторная работа №5. Идентификация защитных механизмов для АИТКС;
-Что такое идентификация.
-Что такое защитный механизм.
-Приведите примеры защитных механизмов.
-Назовите основные защитные механизмы, используемые в системах защиты информации.
-Как происходит идентификация защитных механизмов.
Лабораторная работа №6. Идентификация нарушителей в АИТКС.
-Что такое идентификация.
-Кто такие нарушители.
-Приведите примеры нарушителей.
-Как можно идентифицировать нарушителей?
-Перечислите виды нарушителей.

Примеры вариантов заданий для лабораторных работ:

Лабораторная работа №1. Основы шифрования данных

Цель работы: изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

Порядок выполнения работы

1. Ознакомьтесь с теоретическими основами шифрования данных в настоящих указаниях, а также в конспектах лекций.
2. Получите вариант задания у преподавателя.
3. Напишите программу согласно варианту задания.
4. Отладьте разработанную программу и покажите результаты работы программы преподавателю.
5. Составьте отчет по лабораторной работе

Содержание отчета

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- вариант задания;
- листинг разработанной программы с комментариями;
- результаты работы программы.

Критерии оценки выполнения лабораторных работ

Результаты выполнения каждой лабораторной работы оцениваются в баллах. Максимальная сумма, набираемая студентом за выполнение каждой лабораторной работы, составляет 5 баллов.

Критерии оценки для выполнения лабораторной работы:

- 4-5 балла выставляется обучающемуся, если соблюдаются критерии: представлен полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения и надлежащим образом оформленный (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся верно и полно ответил на все контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно и в определенный преподавателем срок;

- 3-3,9 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), полностью выполнено задание на лабораторную работу, обучающийся преимущественно верно и полно ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы, лабораторная работа выполнена самостоятельно, возможно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки;

- 2-2,9 балла выставляется обучающемуся, если соблюдаются критерии: представлен недостаточно полный письменный отчет по лабораторной работе, содержащий описание не всех этапов ее выполнения, имеющий, возможно, погрешности в оформлении (в печатном или электронном виде - в соответствие с требованием преподавателя), в основном выполнено задание на лабораторную работу, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с отражением лишь общего направления изложения материала, с наличием достаточно количества несущественных или одной-двух существенных ошибок, лабораторная работа выполнена самостоятельно, с нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература;

- 0,9-1,9 балла выставляется обучающемуся, если соблюдаются критерии: письменный отчет по лабораторной работе (в печатном или электронном виде - в соответствие с требованием преподавателя) не представлен или представлен неполный, отчет содержит описание не всех этапов выполнения работы, имеет погрешности в оформлении, задание на лабораторную работу выполнено не полностью, обучающийся ответил на контрольные вопросы преподавателя по теоретической и практической части лабораторной работы с большим количеством существенных ошибок, продемонстрировал неспособность осветить проблематику лабораторной работы, лабораторная работа выполнена несамостоятельно, с существенным нарушением определенного преподавателем срока предоставления отчета, отчет содержит грамматические и стилистические ошибки, при его составлении использована устаревшая учебная литература, обучающийся при выполнении работы продемонстрировал отсутствие необходимых умений и практических навыков.

При оценке за лабораторную работу менее 0,9 балла, данная работа считается невыполненной и не зачитывается. При невыполнении лабораторной работы хотя бы по одной из изучаемых тем, обучающийся не получает положительную оценку при промежуточном контроле по дисциплине (зачет).

5.1.3. Оценочные материалы для выполнения рефератов

Примерные темы рефератов по дисциплине «Основы информационной безопасности» (контролируемые компетенции ОК-4, ОПК-5, ОПК-7)

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.
16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
18. Способы наблюдения с использованием технических средств.
19. Каналы утечки информации. Технические каналы утечки
20. Классификация технических каналов утечки по физической природе носителя.
21. Классификация технических каналов утечки по информативности.
22. Классификация технических каналов утечки по времени функционирования.
23. Классификация технических каналов утечки по структуре.
24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
25. Перехват электромагнитных излучений.
26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
27. Понятия скрытия информации, виды скрытий. Информационный портрет.
28. Противодействие наблюдению. Способы маскировки.
29. Способы и средства противодействия подслушиванию.
30. Нейтрализация закладных устройств.
31. Состав инженерной защиты и технической охраны объектов.
32. Инженерные конструкции и сооружения для защиты информации. Их классификация.
33. Средства идентификации личности.
34. Классификация датчиков охранной сигнализации.
35. Классификация извещателей.
36. Телевизионные системы наблюдения.
37. Основные средства системы видеоконтроля.
38. Защита личности как носителя информации.
39. Системный подход к защите информации.
40. Параметры системы защиты информации.
41. этапы проектирования системы защиты информации.

Методические рекомендации по написанию реферата

Реферат – продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Изложенное понимание реферата как целостного авторского текста определяет критерии его оценки: новизна текста; обоснованность выбора источника; степень раскрытия сущности вопроса; соблюдения требований к оформлению.

Требования к реферату: Общий объём реферата 20 листов (шрифт 14 Times New Roman, 1,5 интервал). Поля: верхнее, нижнее, правое, левое – 20мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль

Обязательно наличие: содержания (структура работы с указанием разделов и их начальных номеров страниц), введения (актуальность темы, цель, задачи), основных разделов реферата, за-

ключения (в кратком, резюмированном виде основные положения работы), списка литературы с указанием конкретных источников, включая ссылки на Интернет-ресурсы.

В тексте ссылка на источник делается путем указания (в квадратных скобках) порядкового номера цитируемой литературы и через запятую – цитируемых страниц. ***Уровень оригинальности текста – 60%***

Критерии оценки реферата:

«отлично» (5 баллов) ставится, если выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. Обучающийся проявил инициативу, творческий подход, способность к выполнению сложных заданий, организационные способности. Отмечается способность к публичной коммуникации. Документация представлена в срок. Полностью оформлена в соответствии с требованиями

«хорошо» (4балла) – выполнены основные требования к реферату и его защите 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; на дополнительные вопросы при защите даны неполные ответы. Обучающийся достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи. Документация представлена достаточно полно и в срок, но с некоторыми недоработками

«удовлетворительно» (3 балла) – имеются существенные отступления от требований к реферированию. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Обучающийся выполнил большую часть возложенной на него работы. Допущены существенные отступления. Документация сдана со значительным опозданием (более недели). Отсутствуют отдельные фрагменты.

«неудовлетворительно» (0 баллов) – тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Обучающийся не выполнил свои задачи или выполнил лишь отдельные несущественные поручения. Документация не сдана.

5.2. Оценочные материалы для самостоятельной работы обучающегося

Рабочая программа предусматривает проведение лекционных, лабораторных занятий, а также самостоятельную работу обучающихся. В ФГБОУ ВО «Кабардино-Балкарский государственный университет» действует балльно-рейтинговая система оценки учебных достижений обучающихся по образовательным программам, реализуемым на основании федеральных государственных образовательных стандартов. Балльно-рейтинговая система оценки знаний является одной из составляющих системы управления качеством образовательной деятельности в университете.

Перечень типовых заданий для самостоятельной работы сформирован в соответствии с тематикой лекционных и лабораторных занятий по дисциплине «Основы информационной безопасности».

1. Понятие национальной безопасности.
2. Роль информационной безопасности в обеспечении национальной безопасности государства.
3. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение.
4. Внешние источники угроз.
5. Внутренние источники угроз.

6. Направления обеспечения информационной безопасности государства.
7. Проблемы региональной информационной безопасности.
8. Содержание информационного противоборства на межгосударственном уровне
9. Информационное оружие, его классификация и возможности.
10. Методы и средства обеспечения информационной безопасности компьютерных систем
11. Программно-аппаратные средства обеспечения информационной безопасности.
12. Методы оценки защищенности компьютерных систем от НСД.
13. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
14. Классификация и возможности технических разведок
15. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок.
16. Методы защиты АС и СВТ от внешнего электромагнитного воздействия

Критерии формирования оценок по заданиям для самостоятельной работы студента (типовые задачи):

«отлично» (5 баллов) - обучающийся показал глубокие знания материала по поставленным вопросам, грамотно, логично его излагает, структурировал и де-тализировал информацию, избегая простого повторения информации из текста, информация пред-ставлена в переработанном виде. Свободно использует необходимые формулы при решении задач;

«хорошо» (4 балла) - обучающийся твердо знает материал, грамотно его излагает, не допускает существенных неточностей в процессе решения задач;

«удовлетворительно» (3 балла) - обучающийся имеет знания основного материала по поставленным вопросам, но не усвоил его деталей, допускает отдельные неточности при решении задач;

«неудовлетворительно» (0 баллов) – обучающийся допускает грубые ошибки в ответе на поставленные вопросы и при решении задач

5.3. *Оценочные материалы для рубежного контроля* (контролируемые компетенции ОК-4, ОПК-5, ОПК-7)

Рубежный контроль осуществляется по более или менее самостоятельным разделам – учебным модулям курса и проводится по окончании изучения материала модуля в заранее установленное время. Рубежный контроль проводится с целью определения качества усвоения материала учебного модуля в целом. В течение семестра проводится ***три таких контрольных мероприятия по графику***.

В качестве форм рубежного контроля можно использовать тестирование (письменное или компьютерное), проведение коллоквиума или контрольных работ. Выполняемые работы должны храниться на кафедре течении учебного года и по требованию предоставляться в Управление контроля качества. На рубежные контрольные мероприятия рекомендуется выносить весь программный материал (все разделы) по дисциплине.

5.3.1. Оценочные материалы для контрольной работы:

Первая контрольная точка

Типовые вопросы, выносимые на коллоквиум 1-ой контрольной точки (контролируемая компетенция . ОК-4, ОПК-7)

1. Обеспечение информационной безопасности: содержание и структура понятия.

2. Информация, защищаемая информация, объект информатизации, информационные ресурсы, информационная технология.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Защита информации. Основные термины и определения.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Модели угроз и нарушителей информационной безопасности.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Принципы защиты информации от НСД.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Система инженерно-технической защиты информации.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Организационная основа системы обеспечения информационной безопасности РФ.
18. Основные функции системы обеспечения информационной безопасности.

Вторая контрольная точка

Типовые вопросы, выносимые на коллоквиум 2-ой контрольной точки (контролируемая компетенция . ОПК-5, ОПК-7)

1. Определение и виды опасностей
2. Определение и виды угроз
3. Цели системы безопасности
4. Основные задачи системы безопасности предприятия
5. Средства обеспечения безопасности предприятия
6. Определение информационной безопасности
7. Компоненты (источники, объекты, действия) учитываемые при построении модели информационной безопасности предприятия.
8. Наиболее важные компоненты (источники, объекты, действия) модели информационной безопасности предприятия
9. Что является объектом угроз информационной безопасности
10. Что выступает в качестве источников угроз ИБ
11. Разглашение
12. Утечка
13. Несанкционированный доступ
14. Классификация угроз по признакам:
15. Основные принципы, которые следует учитывать при построении систем безопасности
16. Виды конфиденциальной информации
17. Что относится к мерам по обеспечению надежности персонала

18. Виды угроз информационным ресурсам – по возрастанию степени их опасности
19. Задача обеспечения информационной безопасности
20. Реагирование на нарушения информационной безопасности.
21. Принципы управления службой ЗИ
22. Основные цели деятельности службы ЗИ

Третья контрольная точка

Типовые вопросы, выносимые на коллоквиум 3-ой контрольной точки (контролируемая компетенция . ОПК-5, ОПК-7)

1. Определите три цели безопасности.
2. Укажите различие между пассивными и активными атаками на секретную информацию.
3. Перечислите и определите пять служб безопасности.
4. Определите восемь механизмов безопасности.
5. Укажите различие между шифрованием и стеганографией.
6. Покажите различие между Z и Z_n. Какое из этих множеств может содержать отрицательные целые числа? Как мы можем отобразить целое число в Z в целое число в Z_n?
7. Что такое оператор по модулю и какие у него имеются приложения? Перечислите все свойства для операций по модулю.
8. Поясните отличия между моноалфавитным и многоалфавитным шифрами.
9. Перечислите три моноалфавитных шифра.
10. Определите линейное сравнение. Какой алгоритм может использоваться, чтобы решить уравнение $ax \equiv b(\mathrm{mod}\, n)$? Как мы можем решить набор линейных уравнений?
11. Определите шифр с симметричным ключом.
12. Поясните отличия между шифром подстановки и шифром перестановки.
13. Перечислите четыре вида атак криптоанализа.
14. Укажите различия между современным и традиционным шифрами с симметричным ключом.
15. Укажите различие между рассеиванием и перемешиванием
16. Укажите различие между синхронным и несинхронным шифрами потока.
17. Каков размер блока в DES? Каков размер ключа шифра в DES? Каков размер ключей раунда в DES?
18. Сколько перестановок используется в алгоритме шифра DES?
19. Сколько преобразований имеется в каждой версии AES? Сколько ключей необходимо для каждой версии?
20. Сравните DES и AES. Какой из них ориентирован на работу с битом, а какой — на работу с байтом?
21. Объясните идею криптографической системы RSA: Что является односторонней функцией в этой системе? Что является лазейкой в этой системе? Определите открытые и секретные ключи в этой системе. Опишите безопасность этой системы.

Критерии формирования оценок по контрольным точкам (контрольные работы; коллоквиум)

(5 баллов) - ставится за работу, выполненную полностью без ошибок и недочетов; обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, решено 100% задач;

(4 балла) – ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета, не более трех недочетов. Обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, допуская незначительные неточности при решении задач, решено 70% задач;

(3 балла) – ставится за работу, если бакалавр правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой. Обучающийся затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, решено 55% задач

(менее 3 баллов) – ставится за работу, если число ошибок и недочетов превысило норму для оценки 3 или правильно выполнено менее 2/3 всей работы. Обучающийся дает неверную оценку ситуации, решено менее 50 % задач.

5.3.2. Типовые тестовые задания по дисциплине «Основы информационной безопасности»

Тест – система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений студента.

Примерные задания тестового контроля (контролируемая компетенция . ОК-4, ОПК-5, ОПК-7)

Полный перечень тестовых заданий представлен в ЭОИС

Выберите правильные варианты ответа:

I:
S: … информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
-: Угроза
+: Защита
-: Сохранение
I:
S: … защиты – сама информация, носитель информации или информационный процесс, в отношении которых необходимо осуществлять защиту в соответствии с поставленной целью защиты информации.
-: Цель
+: Объект
-: Предмет
I:
S: … защиты информации – являться предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной потери (утечки) информации или несанкционированного и непреднамеренного воздействия на информацию.
+: Цель
-: Объект
-: Предмет
I:
S: … защиты информации – степень соответствия результатов защиты информации по отношению к поставленной цели.
+: Эффективность
-: Надежность
-: Прозрачность
I:
S: Защита информации от … – деятельность по предотвращению распространения защищаемой информации (её разглашения), несанкционированного доступа к защищаемой информации и получения защищаемой информации злоумышленниками.
-: Копирования

-: Разглашения
+: Утечки
I:
S: К … средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности.
-: Техническим
+: Аппаратным
-: Теоретическим
I:
S: Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств … системы.
+: компьютерной
-: технической
-: установки
I:
S: К основным аппаратным средствам защиты информации относятся
-: устройства для прослушивания музыки
-: устройства для распечатки информации
+: устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.)
I:
S: Под … средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.
-: аппаратными
+: программными
-: техническими
I:
S: К основным программным средствам защиты информации относится:
-: программы копирования информации
+: программы идентификации и аутентификации пользователей КС
-: программы для редактирования информации
I:
S: К основным программным средствам защиты информации относится:
-: программы копирования информации
+: программы разграничения доступа пользователей к ресурсам КС
-: программы для редактирования информации
I:
S: Информация, составляющая государственную тайну не может иметь гриф:
а) "для служебного пользования";
б) "особой важности".
I:
S: Утечка информации – это:
а) несанкционированный процесс переноса информации от источника к злоумышленнику;
б) процесс раскрытия секретной информации.
I:
S: Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование - ... угроза:
а) активная;
б) пассивная.

I:

S: Примеры вспомогательных программных средств защиты информации:

-: программы для копирования информации

+: программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

-: программы для просмотра информации

I:

S: Обеспечение информационной безопасности – … задача, потому что сама информационная среда есть сложный и многоплановый механизм, где могут присутствовать такие компоненты, как персонал, электронное оборудование, программное обеспечение.

-: Простая

+: Комплексная

-: Сложная

I:

S: … - наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей

+: Криптография

-: Имитозащита

-: Обеспечение конфиденциальности

I:

S: … - решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней

-: Криптография

-: Обеспечение аутентификации

+: Обеспечение конфиденциальности

I:

S: … - гарантирование невозможности несанкционированного изменения информации

-: Имитозащита

-: Обеспечение аутентификации

+: Обеспечение конфиденциальности

I:

S: … - разработка методов подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия

-: Имитозащита

+: Обеспечение аутентификации

-: Обеспечение конфиденциальности

I:

S: … - это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения

-: Алгоритм

+: Ключ

-: Сертификат

I:

S: Методы вскрытия шифров разрабатывает наука, носящая название …

-: Криптография

+: Криптоанализ

-: Криптология

I:

S: … это совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей: $\{Fk : X \rightarrow S, K \in K\}$.

-: Алгоритм
+: Шифр
-: Сертификат
I:
S: … называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.
+: Криптостойкость
-: Имитозащита
-: Гамирование
I:
S: Управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от грифа секретности информации и уровня доступа пользователя:
а) мандатное, или нормативное, управление доступом (Mandatory Access Control);
б) дискреционное, или произвольное управление доступом (Discretionery Access Control).
I:
S: Совокупность аппаратных, программных и специальных компонент ВС, реализующих функции защиты и обеспечения безопасности - это:
а) ядро безопасности (Trusted Computing Base (TCB));
б) политика безопасности (Security Policy).
I:
S: Идентификация (Identification) - это:
а) процесс распознания сущностей путем присвоения им уникальных меток (идентификаторов);
б) проверка подлинности идентификаторов сущностей с помощью различных (преимущественно криптографических) методов.
I:
S: Акустические, виброакустические, параметрические, акустоэлектрические и оптико-электронный технический канал утечки информации - это:
а) технический канал утечки речевой информации;
б) технический канал утечки видовой информации.
I:
S: Документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации - это:
а) конфиденциальная информация;
б) служебная информация.
I:
S: Наиболее эффективное средство для защиты от сетевых атак:
а) использование сетевых экранов или "firewall";
б) использование только сертифицированных программ-броузеров при доступе к сети Интернет.

Критерии формирования оценок по тестовым заданиям:

(5 баллов) – получают обучающиеся с правильным количеством ответов на тестовые вопросы. Выполнено 100 % предложенных тестовых вопросов;

(4 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 80 –99 % от общего объема заданных тестовых вопросов;

(3 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 60 –79% от общего объема заданных тестовых вопросов;

(менее 3 баллов) – получают обучающиеся правильным количеством ответов на тестовые вопросы – менее 40-59 % от общего объема заданных тестовых вопросов.

5.4. Курсовой проект (работа)

(контролируемая компетенция . ОК-4, ОПК-5, ОПК-7)

Примерные варианты заданий на курсовое проектирование.

Примерные темы курсовых работ.

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации.

2. Основные понятия и общеметодологические принципы теории ин-формационной безопасности.

3. Интересы общества в информационной сфере.

4. Интересы государства в информационной сфере.

5. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

6. Угрозы конституционным правам и свободам человека и гражда-нина в области духовной жизни и информационной деятельности, индивиду-альному, групповому и общественному сознанию, духовному возрождению России.

7. Угрозы информационному обеспечению государственной политики Российской Федерации.

8. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

9. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

10. Внешние источники угроз. Внутренние источники угроз.

11. Направления обеспечения информационной безопасности государства.

12. Содержание информационного противоборства на межгосударственном уровне

13. Информационная безопасность и информационное противоборство.

14. Субъекты информационного противоборства.

15. Цели информационного противоборства. Составные части и методы информационного противоборства.

16. Информационное оружие, его классификация и возможности.

17. Компьютерная система как объект информационного воздействия.

18. Компьютерная система как объект информационной безопасности.

19. Общая характеристика методов и средств защиты информации.

20. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.

21. Программно-аппаратные средства обеспечения информационной безопасности.

22. Методы оценки защищенности компьютерных систем от НСД.

23. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

24. Общие критерии

25. Классификация и возможности технических разведок.

26. Компьютерная разведка, ее объекты и содержание.

27. Технические каналы утечки информации при эксплуатации АС.

28. Роль информационной безопасности в обеспечении национальной безопасности государства.

29. Интересы личности в информационной сфере.

30. Интересы общества в информационной сфере.

31. Интересы государства в информационной сфере.

32. Основные составляющие национальных интересов Российской Фе-дерации в информационной сфере.

33. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуаль-ному, групповому и общественному сознанию, духовному возрождению России.

34. Угрозы информационному обеспечению государственной политики Российской Федерации.

35. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

36. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

37. Внешние источники угроз.

38. Внутренние источники угроз.

39. Направления обеспечения информационной безопасности государства.

40. Проблемы региональной информационной безопасности.

41. Информационная безопасность и информационное противоборство.

42. Субъекты информационного противоборства.

43. Цели информационного противоборства.

44. Составные части и методы информационного противоборства.

45. Информационное оружие, его классификация и возможности.

5.5. *Оценочные материалы для промежуточной аттестации.*

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Промежуточная аттестация предназначена для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины. Осуществляется в конце семестра и представляет собой итоговую оценку знаний по дисциплине «Основы информационной безопасности» в виде проведения экзамена.

Промежуточная аттестация может проводиться в устной, письменной форме, и в форме тестирования. На промежуточную аттестацию отводится до 30 баллов.

Рубежный и промежуточный контроль освоения студентом дисциплины осуществляется в рамках балльно-рейтинговой системы. Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ приведено в таблице 7.

Таблица 7

Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе

№ рейтинговой точки	Коллоквиум	Лаб.практикум	Посещаемость	Тестирование	Итого
1	7	8	3	5	23
2	7	8	3	5	23
3	7	8	4	5	24

Таблица 8

Критерии оценки

Вид мероприятия	Критерии оценки	Баллы
Коллоквиум (устный опрос по теме)	- ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами;	0-21 балл

	- системность знаний по тематике	
Лабораторное занятие	- понимание цели и задач работы - выполнение заданий и обработка результатов - отчет и защита лабораторной работы	0-24 балла
Компьютерное тестирование по разделам дисциплины	Результаты тестирования (Количество баллов = 5*φ, φ - доля правильно отвеченных тестов по теме).	0-15 баллов
Посещение занятий	При более 3 пропусках без уважительной причины занятий аннулируются баллы	0-10 баллов
Экзамен	ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике дисциплины в целом	0-30 баллов
Итоговая оценка		0-100 баллов

Примерный перечень вопросов к экзамену по всему курсу (контролируемая компетенция . ОК-4, ОПК-5, ОПК-7)

1. Цели и задачи информационной безопасности, основные понятия
2. Интересы государства в информационной сфере, основные документы РФ по информационной безопасности
3. Основные законы РФ по обеспечению информационной безопасности
4. Меры законодательного уровня информационной безопасности
5. Закон «Об информации, информатизации и защите информации»
6. Закон «О лицензировании отдельных видов деятельности»
7. Закон №1-ФЗ «Об электронной цифровой подписи»
8. Оценочные стандарты в области информационной безопасности в США, «Оранжевая книга»
9. Классы безопасности и защищенности компьютерных систем по «Оранжевой книге»
10. Механизмы безопасности «Оранжевой книги»
11. Требования к безопасности информационных систем в России, руководящие документы Гостехкомиссии РФ
12. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», виды требований «Общих критериев»
13. Нормативная документация определения профиля защиты на основе «Общих критериев» информационной безопасности
14. Функциональные требования «Общих критериев» информационной безопасности
15. Требования доверия безопасности на основе «Общих критериев»
16. Порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
17. Объекты защиты авторских прав и основные права автора в отношении его произведения.
18. Свойства безопасности информации и систем ее обработки
19. Конфиденциальность информации
20. Свойства безопасности информации: целостность, достоверность, доступность
21. Противодействие средствам информационной разведки
22. Понятие «Информационная война»
23. Угрозы информационной безопасности
24. Анализ угроз информационной безопасности

25. Понятие угрозы информационной безопасности, угрозы проникновения
26. Причины возникновения угроз, виды их классификации.
27. Классификация угроз по степени преднамеренности проявления.
28. Три вида основных угроз для автоматизированных систем
29. Классификация угроз по непосредственному источнику угроз и по положению источника угроз
30. Классификация угроз по степени воздействия и по степени зависимости от активности автоматизированных систем
31. Классификация угроз по этапам и способу доступа пользователей или программ к ресурсам автоматизированных систем
32. Классификация угроз по текущему месту расположения информации, хранимой и обрабатываемой в автоматизированных систем
33. Основные виды реализации угроз с точки зрения владельца информации и в зависимости от цели воздействия
34. Утечка, причины утечки информации, каналы утечки информации и типы каналов
35. Уничтожение, искажение, блокирование информации
36. Понятие и особенности несанкционированного доступа к информации
37. Категории методов защиты от несанкционированного доступа
38. Идентификация: понятие и особенности
39. Аутентификация: понятие и особенности
40. Парольные системы для защиты от несанкционированного доступа, общие подходы к их построению
41. Типы угроз безопасности парольных систем
42. Оценка стойкости парольных систем
43. Информационная защита электронного бизнеса
44. Понятие коммерческой тайны, порядок установления ее режима и основные права ее субъектов.
45. Электронный документооборот и обеспечение его безопасности
46. Электронная цифровая подпись, основные понятия
47. Сертификат ключа электронной цифровой подписи
48. Условия использования электронной цифровой подписи
49. Удостоверяющие центры, их назначение и основная деятельность
50. Аппаратно-программные средства защиты информации
51. Физическая защита территории и помещений предприятия и ее основные элементы.
52. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.
53. Вредоносное программное обеспечение, его классификация
54. Компьютерные вирусы, классификация и последствия их воздействия на информацию.
55. Основные антивирусные программы и описание их назначения.
56. Криптографические методы защиты информации
57. Требования к криптосистемам, криптоанализ, атаки на криптосистемы.
58. Основные алгоритмы шифрования.
59. Шифрование с открытым ключом
60. Шифрование с закрытым ключом

В экзаменационный билет входят 2 теоретических вопроса и одно практическое задание.
Пример задания

1. Закон «Об информации, информатизации и защите информации»
2. Три вида основных угроз для автоматизированных систем
3. Зашифровать шифром RSA слово COD

Критерии формирования оценок по промежуточной аттестации:

«отлично» (5 баллов) – получают обучающиеся, которые свободно ориентируются в материале и отвечают без затруднений. Обучающийся способен к выполнению сложных заданий, постановке целей и выборе путей их реализации. Работа выполнена полностью без ошибок, решено 100% задач;

«хорошо» (4 балла) – получают обучающиеся, которые относительно полно ориентируются в материале, отвечают без затруднений, допускают незначительное количество ошибок. Обучающийся способен к выполнению сложных заданий. Работа выполнена полностью, но имеются не более одной негрубой ошибки и одного недочета, не более трех недочетов. Допускаются незначительные неточности при решении задач, решено 70% задач;

«удовлетворительно» (3 балла) – получают обучающиеся, у которых недостаточно высок уровень владения материалом. В процессе ответа на экзамене допускаются ошибки и затруднения при изложении материала. Обучающийся правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой. Обучающийся затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, решено 55% задач;

«неудовлетворительно» (2 балла) – получают обучающиеся, которые допускают значительные ошибки. Обучающийся имеет лишь начальную степень ориентации в материале. В работе число ошибок и недочетов превысило норму для оценки 3 или правильно выполнено менее 2/3 всей работы. Обучающийся дает неверную оценку ситуации, решено менее 50% задач.

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Максимальная сумма (100 баллов), набираемая студентом по дисциплине включает две составляющие:

– *первая составляющая* – оценка регулярности, своевременности и качества выполнения студентом учебной работы по изучению дисциплины в течение периода изучения дисциплины (семестра, или нескольких семестров) (сумма – не более 70 баллов). Баллы, характеризующие успеваемость студента по дисциплине, набираются им в течение всего периода обучения за изучение отдельных тем и выполнение отдельных видов работ.

– *вторая составляющая* – оценка знаний студента по результатам промежуточной аттестации (не более 30 –баллов).

Критерием оценки уровня сформированности компетенций в рамках учебной дисциплины «Основы информационной безопасности» в 3 семестре является экзамен.

Общий балл текущего и рубежного контроля складывается из следующих составляющих приложение 2. В течение учебного процесса студент обязан отчитаться по теоретическому материалу и освоению практических навыков на лабораторных занятиям: опросы, индивидуальные задания, отчеты по лабораторным работам.

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Критерии оценки качества освоения дисциплины

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат

незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

Типовые задания, обеспечивающие формирование компетенций ОК-4, ОПК-5 и ОПК-7 представлены в таблице 9. Компетенции формируются во время всех видов занятий: на лекциях, практических (лабораторных) занятиях, в процессе самостоятельной работы студентов, написании курсовых работ (проектов), при проведении практик и подготовке выпускной квалификационной работы. Этапы освоения компетенции связаны с увеличением доли самостоятельности студента в организации того или иного вида работы.

Изложение материала на лекциях, закрепление в ходе выполнения домашних заданий.

Использование методических материалов в печатном (методические указания) и электронном виде (презентация).

Консультирование студентов при выполнении домашнего задания и при подготовке к его защите, совместная работа на семинарских занятиях.

Изложение материала на лекциях, закрепление на семинарских занятиях.

Консультирование студентов при выполнении домашнего задания, оценка защиты домашней работы.

Таблица 9. Результаты освоения учебной дисциплины, подлежащие проверке

Результаты обучения (компетенции)	***Основные показатели оценки результатов обучения***	***Вид оценочного материала, обеспечивающие формирование компетенций***
ОК-4 - Способностью использовать основы правовых знаний в различных сферах деятельности	***Знать:*** основные правовые и этические нормы при оценке последствий своей профессиональной деятельности;	Типовые оценочные материалы для устного опроса*;* типовые тестовые*;* примерные темы рефератов с типовые оценочные материалы к экзамену *(раздел 5)*
	Уметь: самостоятельно осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных по свойствам, технологии получения и размещения информации об объекте информатизации, представлять ее в требуемом формате с использованием информацион-	Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); типовые тестовые задания (раздел 5.2.2.)

	ных технологий локализованных, распределенных и облачных баз, банков и хранилищ данных;	
	Владеть: методами и способами самостоятельно приобретать и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, связанных с технологической подготовкой размещения информации в базах данных;	примерные темы рефераты (раздел 5.1.3).;
ОПК-5 - способностью использовать нормативные правовые акты в профессиональной деятельности	***Знать:*** - основные концепции баз данных, типовые задачи, выполняемые при создании серверных баз данных и их администрировании;	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)*
	Уметь: - проектировать и создавать базы данных и приложения пользователя в клиент-серверной архитектуре, эффективно выполнять задачи их администрирования;	Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); типовые тестовые задания (раздел 5.2.2.)
	Владеть: - способностью использовать нормативные правовые акты в профессиональной деятельности	примерные темы рефераты (раздел 5.1.3).;
ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	***Знать***: - основные правовые и этические нормы при оценке последствий своей профессиональной деятельности; жизненный цикл программ, оценку качества программных продуктов, технологии разработки программных комплексов, CASE-средства;	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)*
	Уметь: **-** самостоятельно осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных об объекте информатизации, представлять ее в требуемом формате с использованием информационных технологий;	Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.);
	Владеть: способностью определять ин-	примерные темы рефераты (раздел 5.1.3).;

	формационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	

Таким образом, выполнение типовых заданий, представленных в разделе 5 «Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации» позволит обеспечить способность:

- использовать основы правовых знаний в различных сферах деятельности (*ОК-4)*;
- использовать нормативные правовые акты в профессиональной деятельности (*ОПК-5*);
- определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (*ОПК-7)*.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Основная литература

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 c.— Режим доступа: http://www.iprbookshop.ru/72444.html.— ЭБС «IPRbooks»

2. Баяндин Н.И. Информационно-аналитическое обеспечение безопасности бизнеса. Деловая разведка [Электронный ресурс]: учебник/ Баяндин Н.И.— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 264 c.— Режим доступа: http://www.iprbookshop.ru/66801.html.— ЭБС «IPRbooks»

Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 195 c.— Режим доступа: http://www.iprbookshop.ru/72345.html.— ЭБС «IPRbooks»

4. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: Учебник для бакалавриата и магистратуры. – М.: Юрайт, 2017

7.2 Дополнительная литература

1. Основы информационной безопасности: учеб. пособ. для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М.: Горячая линия - Телеком, 2006. - 544 с.: ил.

2. Основы информационной безопасности/В.А. Галатенко. - М.: ИНТУИТ, 2003. - 280 с.

3. Методы и технологии информационных войн / С.Н. Бухарин, В.В. Цыганов. - М.: Академический Проект, 2007. - 382 с.

4. Основы информационной безопасности. Курс лекций: учебное пособие. Третье издание/ В.А. Галатенко/М.: Интернет - Унивеститет Информационных Технологий, www.intuit.ru, 2006. - 200 с.

5. Аудит информационной безопасности/ А.П. Курило, С.Л. Зефиров, В.Б. Голованов/ М: Издательская группа "БДЦ - пресс", 2006. - 305 с.

6. Техническая защита информации/ А.П. Зайцев, А.А. Шелупанов/ М: Горячая линия Телеком, 2007. - 616 с.

7. Расторгуев С.П. Основы информационной безопасности: учеб. по-соб. / С.П. Расторгуев. - М.: Академия, 2007. - 192 с.

8. Доктрина информационной безопасности Российской Федерации.

7.3. Периодические издания

"Открытые системы / СУБД": Журнал. – АО "Открытые системы"

Журнал – Информационная безопасность

7.4. Интернет-ресурсы

-профессиональные базы:

1. PCI Security Standards Council – http://www.pcisecuritystandards.org.
2. Стандарты информационной безопасности в кредитно-финансовой сфере. Стандарты Банка России – http://www.abiss.ru/doc
3. **Threatpost** https://threatpos Сайт об информационной безопасности от Kaspersky Lab. Авторитетный источник, на который ссылаются ведущие новостные агентства, такие как The New York Times и The Wall Street Journal.
4. **Security Lab** http://www.securitylab.ru/ Проект компании Positive Technologies. Помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.
5. **Anti-Malware** https://www.anti-malware.ru/ Информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме.
6. **SO27000.RU** http://www.iso27000.ru/ Интернет-портал ISO27000.RU – это площадка для общения специалистов по ИБ. Есть тематический каталог ссылок на ресурсы по информационной безопасности и защите информации.
7. **Naked Security** https://nakedsecurity.sophos.com/ Сайт компании Sophos, цитируемый крупными изданиями. Освещается широкий круг вопросов: последние события в мире информационной безопасности, новые угрозы, обзор самых важных новостей недели.
8. **Dark Reading** http://www.darkreading.com/ Сообщество профессионалов, где обсуждаются кибер-угрозы, уязвимости и методы защиты от атак, а также ключевые технологии и методы, которые могут помочь защитить данные в будущем.
9. http://**InfoBez.com** Дайджест материалов по безопасности информационных систем со всего света для сотрудников государственных организаций и коммерческих структур – от менеджеров до руководителей
10. **Информационная безопасность банков** **https://ib-bank.ru/** Отраслевой портал
11. http://**VOID.RU** Сайт VOID.RU представляет собою независимую прессу, освещающую вопросы информационной безопасности - уязвимостей в программном обеспечении, технологий сбора информации, технологий сохранения целостности систем.
12. http://**Security.NNOV.ru** Security.NNOV является одним из наиболее посещаемых Российских ресурсов посвященных информационной безопасности и безопасности IT технологий и доступен как на русском, так и на английском языках.
13. http://**ISO 27001 security** Проект компании IsecT Ltd. Некоммерческий информационный портал, посвященный международным стандартам в области управления информационной безопасностью серии ISO 27000.

14. http://**International ISO 17799 / 27001 Community Forum** Информационный портал, на котором публикуются новости, статьи и другая информация, имеющая отношение к стандартам ISO 27000. Портал предназначен для свободного обмена информацией между сообществом, заинтересованном во внедрении стандартов по управлению информационной безопасностью.
15. http://**VOID.RU** Сайт освещает вопросы информационной безопасности уязвимостей в программном обеспечении, технологий сбора информации, технологий сохранения целостности систем.
16. http://**Security.NNOV.ru** Security.NNOV является одним из наиболее посещаемых Российских ресурсов посвященных информационной безопасности и безопасности IT технологий и доступен как на русском, так и на английском языках.
17. **ISO 27001 security** Проект компании IsecT Ltd. Некоммерческий информационный портал, посвященный международным стандартам в области управления информационной безопасностью серии ISO 27000.
18. **International ISO 17799 / 27001 Community Forum** Информационный портал, на котором публикуются новости, статьи и другая информация, имеющая отношение к стандартам ISO 27000. Портал предназначен для свободного обмена информацией между сообществом, заинтересованном во внедрении стандартов по управлению информационной безопасностью.
19. http://**Anti-Malware.ru** Первый в России независимый информационно-аналитический портал, посвященный программным средствам защиты от вредоносных программ.

- общие информационные, справочные и поисковые:

1. Scopus http://scopus.com Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.
2. Web of Science http://apps.webofknowledge.com Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.
3. zbMATH http://zbmath.org самая полная математическая база данных, охватывающая материалы с конца 19 века. zbMath содержит около 4 000 000 документов, из более 3 000 журналов и 170 000 книг по математике, статистике, информатике, а также машиностроению, физике, естественным наукам и др.
4. Справочная правовая система «Гарант». URL: http://www.garant.ru.
5. Справочная правовая система «КонсультантПлюс». URL: http://www. consultant.ru
6. Полнотекстовая база данных ScienceDirect: URL: http://www. sciencedirect.com.
7. Реферативная база данных зарубежных изданий по экономике EconLit: URL: http://www. ebscohost.com
8. Economics online http://www.econline.h1.ru - целью данного проекта является создание коллекции ссылок на ресурсы WWW, предоставляющие экономическую и финансовую информацию бесплатно в режиме онлайн. На сайте вы найдете каталог ссылок на лучшие экономические ресурсы, новости, информацию по экономической теории, финансам, статистике, архивы научных работ по экономике и т. д.
9. Электронная библиотека по бизнесу и финансам http://www.finbook.biz/ - сайт предоставляет бесплатный доступ к электронным книгам по бизнесу, финансам, экономике.
10. Служба тематических толковых словарей http://glossary.ru/
11. Защита от компьютерных вирусов. Антивирусные программы [Электронный ресурс] – www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html

12. Антивирусная защита информации: способы и средства- https://www.google.ru/webhpsourceid=chrome-instant&ion=1&espv

Интернет-ресурс «Интернет университет информационных технологий» www.intuit.ru

Документация по Oracle Database 10*g* XE http://st-curriculum.oracle.com/tutorial/ DBXETutorial/index.htm

www.ihtika.lib.ru/ Библиотека учебной и методической литературы

www.osp.ru/ Журнал «Открытые системы»

www.window.edu.ru/ Библиотека учебной и методической литературы

www.tests.specialist.ru/ Центр компьютерного обучения МГТУ им. Н.Э.Баумана.

www.microinform.ru/ Учебный центр компьютерных технологий «Микроинформ».

www.rsl.ru/ Российская государственная библиотека.

www.nns.ru/ Национальная электронная библиотека.

www.nlr.ru/ Российская национальная библиотека.

www.gpntb.ru/ Государственная публичная научно-техническая библиотека.

7.5. Методические указания к лабораторным занятиям

1. Л.А. Москаленко, А.А. Ксенофонтов. Администрирование SQL Server 2000. Часть 1. Управление базами данных: Методические указания для выполнения лабораторного практикума. – Нальчик: Каб.-Балк. ун-т, 2004. – 55 с.
2. Л.А. Москаленко, А.А. Ксенофонтов, А.С. Ксенофонтов. Администрирование SQL Server 2000. Часть 2. Восстановление баз данных: Методические указания для выполнения лабораторного практикума. – Нальчик: Каб.-Балк. ун-т, 2007. – 26 с.
3. Л.А. Москаленко, А.С. Ксенофонтов, А.Н. Зубков, Е.Ю. Мильшин. Администрирование SQL Server 2000. Часть 3. Репликация данных: Методические указания для выполнения лабораторного практикума. - Нальчик: Каб-Балк. ун-т, 2008. – 45 с.
4. Москаленко Л.А., Ксенофонтов А.С., Губжокова С.А. Технология доступа к базам данных в сети Интернет: Методические указания для выполнения лабораторных работ . - Нальчик: Каб-Балк. ун-т, 2011. – 29 с.
5. Москаленко Л.А., Ксенофонтов А.С., Дажигова В.А. Защита данных в MS SQL Server: Методические указания для выполнения лабораторных работ . - Нальчик: Каб-Балк. ун-т, 2015. – 31 с.
6. Москаленко Л.А., Ксенофонтов А.С., Хаширова Т.Ю. Облачные технологии в базах данных: Методические указания по выполнению лабораторных работ и для самостоятельной работы студентов. – Нальчик: Каб-Балк. ун-т, 2016. – 28 с.

7.6. Методические указания к практическим занятиям – не предусмотрены

7.7. Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы.

Учебная работа по дисциплине «Основы информационной безопасности» состоит из контактной работы (лекции, практические занятия) и самостоятельной работы. Доля контактной учебной работы в общем объеме времени, отведенном для изучения дисциплины, составляет 51 % (в том числе лекционных занятий – 30,6%, практических занятий – 20,4%), доля самостоятельной работы – 49 %. Соотношение лекционных, семинарских, лабораторных и практических занятий к общему количеству часов соответствует учебному плану Направления 10.03.01 – Информационная безопасность, профиль «ИСФАМ»

Для подготовки к практическим занятиям необходимо рассмотреть контрольные вопросы, при необходимости обратиться к рекомендуемой литературе, записать непонятные моменты в вопросах для уяснения их на предстоящем занятии.

Методические рекомендации по изучению дисциплины «Основы информационной безопасности» для обучающихся

Цель курса «Основы информационной безопасности» - подготовка обучающихся, обладающих знаниями в области оценки риска, управления рисками финансовых активов, выбора эффективных управленческих решений, критической оценки вариантов управленческих решений, расчета рисков и возможных последствий

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться с тематическим планом занятий, списком рекомендованной учебной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий, занести в свою рабочую тетрадь темы и сроки проведения семинаров, написания учебных и творческих работ. При изучении дисциплины обучающиеся выполняют следующие задания: изучают рекомендованную учебную и научную литературу; пишут контрольные работы, готовят доклады и сообщения к практическим занятиям; выполняют самостоятельные творческие работы, участвуют в выполнении практических заданий. Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий

Курс изучается на лекциях, лабораторных работах, при самостоятельной и индивидуальной работе обучающихся. Обучающийся для полного освоения материала должен не пропускать занятия и активно участвовать в учебном процессе. Лекции включают все темы и основные вопросы теории и практики страхования. Для максимальной эффективности изучения необходимо постоянно вести конспект лекций, знать рекомендуемую преподавателем литературу, позволяющую дополнить знания и лучше подготовиться к семинарским занятиям.

В соответствии с учебным планом на каждую тему выделено необходимое количество часов лабораторных занятий, которые проводятся в соответствии с вопросами, рекомендованными к изучению по определенным темам. Обучающиеся должны регулярно готовиться к лабораторным занятиям и участвовать в обсуждении вопросов. При подготовке к занятиям следует руководствоваться конспектом лекций, методическими рекомендациями по выполнению лабораторной работы и рекомендованной литературой. Тематический план дисциплины, учебно-методические материалы, а также список рекомендованной литературы приведены в рабочей программе

В ходе изучения дисциплины обучающийся имеет возможность подготовить реферат по выбранной из предложенного в Рабочей программе списка теме. Выступление с докладом по реферату в группе проводится в форме презентации с использованием мультимедийной техники.

Методические рекомендации при работе над конспектом во время проведения лекции

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации по подготовке к лабораторным занятиям

Лабораторные занятия – составная часть учебного процесса, групповая форма занятий при активном участии студентов. Лабораторные занятия способствуют углубленному изучению

наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся. Целью лабораторных занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к лабораторному занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем задания. При этом учесть рекомендации преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы.

Желательно при подготовке к лабораторным занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

На лабораторных занятиях обучающиеся учатся грамотно излагать проблемы, свободно высказывать свои мысли и суждения, рассматривают ситуации, способствующие развитию профессиональной компетентности. Следует иметь в виду, что подготовка к лабораторному занятию зависит от формы, места проведения занятия, конкретных заданий и поручений. Это может быть написание доклада, эссе, реферата (с последующим их обсуждением), коллоквиум.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа (по В.И. Далю «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

– оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;

– широкое внедрение компьютеризированного тестирования;

– совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;

– модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит студента к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

– развивающую;
– информационно-обучающую;
– ориентирующую и стимулирующую;
– воспитывающую;
– исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разноуровневых задач и заданий;
3. Работа с тестами и вопросами для самопроверки;
4. Выполнение итоговой контрольной работы.

Студентам рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые студент получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала. Самостоятельная работа студентов предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости студент может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания.

Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.
2. Прием постановки вопросов к тексту имеет следующий алгоритм:
   - медленно прочитать текст, стараясь понять смысл изложенного;
   - выделить ключевые слова в тексте;
   - постараться понять основные идеи, подтекст и общий замысел автора.
3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

Методические рекомендации по написанию рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность,

научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения. Общий объем реферата 20 листов.

Технические требования к оформлению реферата следующие. Реферат оформляется на листах формата А4, с обязательной нумерацией страниц, причем номер страницы на первом, титульном, листе не ставится. Поля: верхнее, нижнее, правое, левое – 20 мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль. На титульном листе реферата нужно указать: название учебного заведения, факультета, номер группы и фамилию, имя и отчество автора, тему, место и год его написания. Рекомендуемый объем работы складывается из следующих составляющих: титульный лист (1 страница), содержание (1 страница), введение (1 – 2 страницы), основная часть, которую можно разделить на главы или разделы (10 – 15 страниц), заключение (1 – 3 страницы), список литературы (1 страница), приложение (не обязательно). Если реферат содержит таблицу, то ее номер и название располагаются сверху таблицы, если рисунок, то внизу рисунка.

Содержательные части реферата – это введение, основная часть и заключение. Введение должно содержать рассуждение по поводу того, что рассматриваемая тема актуальна (то есть современна и к ней есть большой интерес в настоящее время), а также постановку цели исследования, которая непосредственно связана с названием работы. Также во введении могут быть поставлены задачи (но не обязательно, так как работа невелика по объему), которые детализируют цель. В заключении пишутся конкретные, содержательные выводы.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения обучающемуся выставляется соответствующая оценка.

Методические рекомендации по написанию курсовой работы

Курсовая работа – самостоятельная научная творческая работа студента, выполняемая в процессе обучения, имеющая своей основной целью развитие навыков теоретических и экспериментальных исследований. Выполнение курсовой работы преследует несколько целей:

показать особенности защиты данных как одной из основных новых информационных технологий, с тем, чтобы студенты понимали тенденции развития современных информационных технологий, видели их преимущества и недостатки, особенности работы в условиях конкретных технологий в их профессиональной деятельности;

сориентировать студентов во множестве современных средств и методов защиты информации и связанных с ними технологий;

осветить теоретические и организационно-методических вопросы построения и функционирования систем, основанных на концепции безопасности данных, в том числе различные методологии моделирования угроз и нарушителей;

показать возможности защиты информации средствами автоматизированных систем;

показать возможности современных высокоуровневых языков и средств создания защищенных приложений;

научить практической работе со средствами защиты информации.

Задание на курсовую работу нацелено на разработку защиты информации автоматизированного рабочего места.

Выполнение курсовой работы состоит в последовательной реализации следующих этапов:

1) изучение литературных источников по выбранному направлению исследований;

2) анализ вариантов решения поставленной задачи на основе изученного теоретического материала;

3) изложение в краткой форме основных теоретических положений, характеризующих выбранное направление исследований;

4) разработка подхода к решению поставленной конкретной задачи;

5) оформление курсовой работы в соответствии с предъявляемыми к оформлению требованиями.

Выбор темы курсовой работы осуществляется из утвержденного кафедрой перечня. Заведующий кафедрой назначает научного руководителя. После консультаций с научным руководителем разрабатывается план курсовой работы. Помимо рекомендованной литературы возможно использование любых доступных источников. Это, в первую очередь, техническая документация, статьи в периодических изданиях и научные публикации. Их изучение в контексте выбранной темы служит расширению научно-технического кругозора, повышению качества и обоснованности использованных решений. В процессе выполнения возможна конкретизация поставленной задачи с тем, чтобы объем работы не превысил допустимых размеров.

Содержание курсовой работы определяется: содержанием соответствующего учебного курса; современным состоянием выбранного направления исследований; доступными литературными источниками; собранным для выполнения курсовой работы фактическим материалом.

Курсовая работа имеет следующую структуру:

1) титульный лист;

2) задание;

3) аннотация;

4) содержание;

5) введение(актуальность, значение темы, цель работы);

6) основная часть (состоящая, как правило, из двух разделов: теоретические основы разрабатываемой темы; практическая часть);

7) заключение (выводы);

8) список используемой литературы;

9) приложения.

Во введении дается обоснование темы работы, определяется ее практическая или теоретическая значимость для специальности, формулируются цели и задачи курсовой работы, а также приводится ее краткая аннотация (количество страниц, рисунков, таблиц, приложений, литературных источников).

В теоретической части раскрывается современное состояние выбранного направления исследований со ссылками на литературные источники, а также рассматривается конкретная система, использование которой стимулировало развитие данного направления защищенных информационных технологий.

В списке литературы в алфавитном порядке приводятся цитируемые литературные источники.

Для оценки результатов курсовой работы используются следующие критерии. Результаты защиты курсовой работы оцениваются по пятибалльной системе оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»). При защите курсовой работы знания и умения каждого слушателя оценивается:

а) качество доклада (по существу рассматриваемых вопросов и с методической стороны);

б) правильность ответов на вопросы;

в) качество выполнения пояснительной записки;

г) качество разработки системы или выполненного анализа для предметной области.

Итоговая оценка за защиту курсовой работы определяется:

«отлично» - если разработанная система оценена на «отлично», а остальные показатели по среднему баллу оценены не ниже «хорошо»;

«хорошо» - если разработанная система оценена не ниже «хорошо», а остальные показатели по среднему баллу оценены не ниже «удовлетворительно»;

«удовлетворительно» - если разработанная система оценена на «удовлетворительно», а

остальные показатели по среднему баллу оценены не ниже «удовлетворительно»;

«неудовлетворительно» - если не выполнены условия получения положительной оценки.

Методические рекомендации для подготовки к экзамену:

Экзамен в 3м семестре является формой итогового контроля знаний и умений обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой К экзамену допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к экзаменц включает три этапа:

– самостоятельная работа в течение семестра;
– непосредственная подготовка в дни, предшествующие экзамену по темам курса;
– подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в письменной / устной форме.

При проведении экзамена в письменной (устной) форме, ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенных до сведения обучающихся накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 40 минут.

При проведении письменного экзамена на работу отводиться 60 минут.

Результат устного (письменного) экзамена выражается оценками:

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные

ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины

8. Материально-техническое обеспечение дисциплины

8.1. Требования к материально-техническому обеспечению

Лекционные занятия проходят в мультимедийной аудитории, оснащенной компьютером и проектором. Каждая лекция сопровождается презентацией, содержащей теоретический материал и иллюстративный материал.

Лабораторные работы проводятся в дисплейном классе на PC-совместимых персональных компьютерах с установленным лицензионным и свободно-распространяемым программным обеспечением.

Минимально необходимый для реализации ОПОП перечень материально-технического обеспечения включает в себя: лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном и имеющие выход в сеть Интернет), помещения для проведения занятий оборудованные учебной мебелью, компьютерные классы имеют достаточное количество посадочных мест и снабжены необходимым программным обеспечением.

По дисциплине «Основы информационной безопасности» имеются презентации по всем темам курса, позволяющие наиболее эффективно освоить представленный учебный материал.

При проведении занятий лекционного типа, практических и лабораторных занятий используются:

лицензионное программное обеспечение:

– Продукты Microsoft (Desktop EducationALNG LicSaPk OLVS Academic Edition Enterprise) подписка (Open Value Subscription);

– Антивирусное программное обеспечение Kaspersky Endpoint Security Стандартный Russian Edition;

– AltLinux (Альт Образование 8);

свободно распространяемые программы:

– WinZip для Windows - программ для сжатия и распаковки файлов;

– Adobe Reader для Windows – программа для чтения PDF файлов;

– Far Manager - консольный файловый менеджер для операционных систем семейства Microsoft Windows.

8.2. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;
2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):
   - присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;
   - задания для выполнения на экзамене зачитываются ассистентом;

– письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

– на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
– зачет/экзамен проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
– по желанию студента экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Лист переутверждения рабочей программы дисциплины

Рабочая программа:

одобрена на 2017/2018 учебный год. Протокол № __ заседания кафедры

от «__» __ 2017 г.

В рабочую программу внесены следующие изменения:

1. В части раздела «Учебно-методическое и информационное обеспечение дисциплины»

_____

_____

Разработчик программы_____

Зав. кафедрой_____

Одобрена на 2018-2019 учебный год.

Протокол № __ заседания кафедры от «__» __ 2018 г.

В рабочую программу внесены следующие изменения:

1. В части раздела «Учебно-методическое и информационное обеспечение дисциплины»
2. В части УП в связи с утверждением порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования, программам бакалавриата, программам специалитета, программам магистратуры (Приказ Минобрнауки №31 от 05.04.2017 г.)

_____

_____

_____

_____

_____

_____

Разработчик программы_____

Зав. кафедрой_____

Одобрена на 2019/2020 учебный год.

Протокол №___ заседания кафедры от «__» _____ 20__ г.

В рабочую программу внесены следующие изменения:

_____

_____

_____

_____

Приложение 2

Распределение баллов текущего и рубежного контроля

№п/п	*Вид контроля*	*Сумма баллов*			
		Обшая сумма	*1-я точка*	*2-я точка*	*3-я точка*
1-	***Посещение занятий***	***до 10 баллов***	***до 3 б.***	***до 3б.***	***до 4б.***
2-	***Текущий контроль:***	***до 30 баллов***	***до 10 б.***	***до 10 б.***	***до 10 б.***
	Ответ на 5 вопросов	*от 0 до15 б.*	*от 0 до 5 б.*	*от0 до 5 б.*	*от0 до 5 б.*
	Полный правильный ответ	до 15 баллов	5 б.	5 б.	5 б.
	Неполный правильный ответ	от 3 до15 б.	от1 до 5 б.	от 1 до 5 б.	от 1 до 5 б.
	Ответ, содержащий неточности, ошибки	0б.	0б.	0б.	0б.
	Выполнение самостоятельных заданий (решение задач, написание рефератов, доклад, эссе)	*от 0 до15 б.*	*от 0 до 5 б.*	*от 0 до 5 б*	*от 0 до 5 б*
1.	***Рубежный контроль***	***до 30 баллов***	***до 10 б.***	***до 10 б.***	***до 10 б.***
	тестирование	от 0- до 12б.	от 0- до 4б.	от 0- до 4б.	от 0- до 4б.
	коллоквиум	от 0 до 18б.	от 0 до 6 б.	от 0 до 6 б.	от 0 до 6 б.
	Итого сумма текущего и рубежного контроля	***до 70баллов***	***до 23б.***	***до 23б***	***до 24б***
	Первый этап (базовый ровень) – оценка «удовлетворительно»	не менее 36 б.	не менее 12 б.	не менее 12 б	не менее 12 б
	Второй этап (продвинутый ровень) – оценка «хорошо»	менее 70 б. (51-69 б.)	менее 23 б	менее 23 б	менее 24б
	Третий этап (высокий уровень) - оценка «отлично»	не менее 70 б.	не менее 23 б.	не менее 23 б	не менее 24б