Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 13.10.2023 16:48:01
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 6
3 Структура и содержание дисциплины 7
3.1 Виды учебной работы и трудоемкость 7
3.2 Тематический план изучения дисциплины 8
3.3 Содержание дисциплины 9
3.4 Тематика семинарских/практических и лабораторных занятий 10
4 Учебно-методическое и информационное обеспечение 11
4.1 Нормативные документы и ГОСТы 11
4.2 Основная литература 11
4.3 Дополнительная литература 11
4.4 Электронные образовательные ресурсы 11
4.5 Лицензионное и свободно распространяемое программное обеспечение 12
4.6 Современные профессиональные базы данных и информационные справочные материалы 12
5 Материально-техническое обеспечение 12
6 Методические рекомендации 12
6.1 Методические рекомендации для преподавателя по организации обучения 12
6.2 Методические указания для обучающихся по освоению дисциплины 12
7 Фонд оценочных средств 13
7.1 Методы контроля и оценивания результатов обучения 13
7.2 Шкала и критерии оценивания результатов обучения 13
7.3 Оценочные средства 14

1 Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины - получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем для успешной профессиональной деятельности.

Задачи дисциплины:

-изучение основ управления информационной безопасности информационных систем (ИС);

- изучение и анализ классификации угроз информационной безопасности ИС;

-изучение принципов действия основных видов сетевых атак и методов борьбы с ними;

- изучение структуры политики безопасности организации и основных этапов ее разработки;

- анализ оценочных стандартов в информационной безопасности;

- изучение подходов создания системы управления информационной безопасностью ИС на предприятии;

- анализ методик и технологий управления рисками;

- изучение современных методов и средств анализа и управления рисками ИС компаний;

- анализ правовых мер обеспечения информационной безопасности;

- анализ организационных мер обеспечения безопасности компьютерных ИС;

- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;

- изучение основных требований и рекомендаций по защите информации в ИС;

- изучение основных юридических законов в области защиты информации.

Планируемые результаты обучения

В результате освоения дисциплины «Управление информационной безопасностью» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	ИУК-5.1. Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, и обосновывает актуальность их использования при социальном и профессиональном взаимодействии. ИУК-5.2. Выстраивает социальное и профессиональное взаимодействие с учетом общих и специфических черт различных культур и религий, особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других наций и конфессий, различных социальных групп. ИУК-5.3. Обеспечивает недискриминационной

	взаимодействия при профессиональных задач, демонстрируя понимание особенностей различных культур и наций. создание среды выполнении
ПК-1. Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	ИПК-1.1. Применяет знания направлений развития информационных технологий, основных видов политик безопасности объектов защиты; ИПК-1.2. Умеет прогнозировать эффективность функционирования, оценивать затраты и риски объектов защиты; ИПК-1.3. Владеет навыками формирования политики безопасности объектов защиты
ПК-12. Способен организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения	ИПК-12.1. Знает: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно- технических решений, реализованных при построении ЭВМ и систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. ИПК-12.2. Умеет: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; -администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-12.3. Владеет: - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения

	режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные систем
ПК-13. Способен организовать управление информационной безопасностью	ИПК-13.1. Знает: современные подходы к управлению ИБ и направлениям их развития; основные стандарты, регламентирующие управление ИБ; принципы построения СУИБ; принципы разработки процессов управления ИБ; взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; подходы к интеграции СУИБ в общую систему управления предприятием. ИПК-13.2. Умеет: анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный подход к управлению ИБ в различных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. ИПК-13.3. Владеет: навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и систем процессов в целом

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части блока Б1 «Дисциплины (модули)».

Дисциплина «Управление информационной безопасностью» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.41):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Защищенные информационные системы».

Дисциплина обеспечивает изучение дисциплин «Аудит систем управления информационной безопасностью», «Методы и средства повышения осведомлённости персонала по вопросам информационной безопасности» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

3.1Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			7
1	**Аудиторные занятия**	**72**	7
	В том числе:		
1.1	Лекции		
1.2	Семинарские/практические занятия		7
1.3	Лабораторные занятия	72	7
2	**Самостоятельная работа**	**72**	**7**
3	**Промежуточная аттестация**		**7**
	Экзамен		7
	Итого:	**144**	

3.2Тематический план изучения дисциплины

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Основные понятия и анализ угроз информационной безопасности	**24**			12		12
2	Раздел 2. Проблемы информационной безопасности сетей	**16**			8		8
3	Раздел 3. Политика безопасности	**20**			10		10
4	Раздел 4. Криптографическая защита информации	**24**			12		12
5	Раздел 5. Технологии аутентификации	**16**			8		8
6	Раздел 6. Технологии межсетевых экранов	**12**			6		6

7	Раздел 7. Технологии защиты от вирусов	**12**			6		6
8	Раздел 8. Требования к системам защиты информации	**12**			6		6
9	Раздел 9. Основы правового обеспечения защиты информации	**8**			4		4
Итого		**144**			**72**		**72**

3.3 Содержание дисциплины

Раздел 1. Основные понятия и анализ угроз информационной безопасности.

Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности.

Раздел 2. Проблемы информационной безопасности сетей

Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг.

Раздел 3. Политика безопасности

Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности.

Раздел 4. Криптографическая защита информации

Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные криптосистемы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП).

Раздел 5. Технологии аутентификации

Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода.

Раздел 6. Технологии межсетевых экранов

Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий.

Раздел 7. Технологии защиты от вирусов

Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ.

Раздел 8. Требования к системам защиты информации

Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных.

Раздел 9. Основы правового обеспечения защиты информации

Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности.

3.4Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Раздел 1. Основные понятия и анализ угроз информационной безопасности.

Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.

Раздел 2. Проблемы информационной безопасности сетей

Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.

Раздел 3. Политика безопасности

Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети

Раздел 4. Криптографическая защита информации

Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.

Раздел 5. Технологии аутентификации

Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.

Раздел 6. Технологии межсетевых экранов

Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.

Раздел 7. Технологии защиты от вирусов

Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.

Раздел 8. Требования к системам защиты информации

Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите

информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

Раздел 9. Основы правового обеспечения защиты информации

Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

4 Учебно-методическое и информационное обеспечение

4.1Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов 10.05.03 «Информационная безопасность автоматизированных систем».

4.2Основная литература

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст: электронный

2. Горбунов, А. В. Проектирование защищённых оптических теле-коммуникационных систем : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст: электронный.

4.3Дополнительная литература

1.Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. – Воронеж : Во- ронежский государственный университет инженерных технологий, 2012. – 172 с. – URL: https://biblioclub.ru/index.php?page=book&id=141626 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный

2. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 222 с. – URL: https://biblioclub.ru/index.php?page=book&id=458204 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный

4.4Электронные образовательные ресурсы

1. ЭОР разрабатывается
2. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
3. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
4. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
5. Электронно-библиотечная система IQLib – http://www.iqlib.ru

6. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

4.5Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

4.6Современные профессиональные базы данных и информационные справочные материалы

1. https://doka.guide/
2. https://developer.mozilla.org/ru/
3. https://roadmap.sh/frontend

5 Материально-техническое обеспечение

Для проведения лабораторных работ и самостоятельной работы студентов подходят аудитории, оснащенные компьютерами с программным обеспечением в соответствии со списком в пункте 4.5 и подключенные к интернету.

Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

Рабочее место преподавателя должно быть оснащено компьютером с подключенным к нему проектором или иным аналогичным по функциональному назначению оборудованием.

6 Методические рекомендации

6.1Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции и самостоятельная работа.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

Приветствуется обсуждение самих заданий с другими студентами: можно как давать, так и получать советы по общей стратегии выполнения и изучения материала, давать и получать помощь в отладке. Однако писать код студент должен самостоятельно. Делиться кодом или писать его совместно запрещено.

7 Фонд оценочных средств

7.1Методы контроля и оценивания результатов обучения

Приведенные ниже правила выставления оценок и опозданий могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы студенты регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения.

Достижение компетенций оценивается с помощью лабораторных работ и рубежных контролей.

Каждый студент имеет право на 6 дней опоздания, которые могут быть потрачены на любые задания в течение семестра. Опоздания предназначены для решения особых ситуаций, таких как болезнь или чрезвычайные семейные обстоятельства.

Когда использованы все дни опоздания за каждый день просрочки начисляется штраф в размере 25% от максимального результата за задание. Задания, присланные позже, чем 4 дня, не будут оцениваться. В связи с зависимостью между работами студентам может потребоваться все равно выполнить предыдущие работы, даже если они не оцениваются.

После сдачи лабораторной работы студент должен ее защитить. Во время защиты лабораторной работы преподаватель проверяет репозиторий, хостинг и выполнение критериев и требований задания, а студент отвечает на вопросы преподавателя по его коду, а также теоретических вопросов, приведенных после текста задания лабораторной работы. Если студент отказывается отвечать на вопросы, или дает полностью неверные ответы, или ответы не по теме, то работа может считаться сданной, но при этом она не оценивается.

Работа должна быть выполнена студентом самостоятельно: в репозитории в системе контроля версий студента содержатся коммиты только за его авторством, по этим коммитам можно проследить как велась работа, студент может объяснить свой код и ход выполнения работы, если эти правила не соблюдаются, то работа не считается сданной и не оценивается.

Рубежные контроли пишутся в аудитории индивидуально по варианту задания, выданному преподавателем в назначенные дни. При отсутствии студента в день написания контрольной работы ему дается еще один шанс ее написать на последнем занятии в семестре, но обязательно очно.

Студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей задания или проекта. При наличии реальных причин задержки студентам следует как можно скорее связаться с преподавателем и обсудить возможные условия.

7.2Шкала и критерии оценивания результатов обучения

Лабораторная работа оценивается в процентах степени выполнения следующих критериев и для выставления оценки суммируются проценты за каждый из четырех критериев:

1. Полнота выполнения практического задания (30%): соответствует ли функциональность заданным требованиям и целям, насколько точно и без ошибок код

выполняет поставленные задачи, насколько эффективно задание отвечает требованиям целевой аудитории и обеспечивает приятное восприятие.

2. Качество и структура кода (10%): качество, читаемость и организация кода, рациональность выполнения задания, последовательность именования и соблюдение лучших практик.

3. Творчество и инновации (10%): творческий подход студентов к выполнению заданий, насколько студенты вышли за рамки основных требований и реализовали дополнительные возможности или использовали уникальные решения.

4. Ответы на вопросы по коду студента и теории (50%):

Дает краткий ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает неправильно (10% из 50%)

Дает развернутый ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает неверно (20% из 50%)

Дает развернутый ответ, содержащий ошибки или неточности. На наводящие вопросы отвечает правильно (30% из 50%)

Дает правильные и развернутые ответы на вопросы (50% из 50%).

R лабораторные рассчитывается как среднее результатов за все лабораторные работы. За полное и безошибочное выполнение всех лабораторных работ в срок и их защиту можно получить максимум 100 баллов (R лабораторные).

Рубежный контроль оценивается по следующим критериям:

Полнота выполнения практического задания: соответствует ли функциональность заданным требованиям и целям, насколько точно и без ошибок код выполняет поставленные задачи.

Качество и структура кода: качество, читаемость и организация кода, рациональность выполнения задания, последовательность именования и соблюдение лучших практик.

Творчество и инновации: творческий подход студентов к выполнению заданий, насколько студенты вышли за рамки основных требований и реализовали дополнительные возможности или использовали уникальные решения.

Пользовательский опыт: отзывчивость, доступность, насколько эффективно задание отвечает требованиям целевой аудитории и обеспечивает приятное восприятие.

Самостоятельность решения: в репозитории студента есть коммиты только за его авторством, по коммитам в репозитории можно проследить как велась работа, студент может объяснить свой код и ход выполнения работы, если эти правила не соблюдаются, то работа не считается сданной.

Более подробное описание критериев дается в тексте задания рубежного контроля.

За полностью выполненные рубежные контроли также можно получить 100 баллов (R контроль).

Также имеется коэффициент сданных работ K сданные, который равен 1 если все работы сданы и 0 если хотя бы одна работа не сдана.

Итоговый балл рассчитывается по формуле: R сем = (0,5 x R лабораторные + 0,5 x R контроль) * K сданные.

Итоговый балл пересчитывается по шкале ниже и на основании полученной оценки фиксируется результат промежуточной аттестации.

Соответствие баллов в 100 балльной рейтинговой системе оценке по 4-бальной шкале:

0-54 - неудовлетворительно

55-69 - удовлетворительно

70-84 - хорошо

85-100 – отлично

7.3 Оценочные средства

7.3.1 Текущий контроль

Примерный список вопросов:

1. Что такое политика информационной безопасности?

2. Какие организационные меры защиты существуют?

3. Назначение организационных мер?

4. Какие из них наиболее эффективны? Почему?

5. Перечислите основные нормативные документы, регламентирующие ИБ в России

6. Какой состав и организационная структура системы обеспечения информационной безопасности?

7. В чем заключается стандарт ISO 17799? 8. Опишите методику анализа рисков.

8. В чем заключаются основные принципы проектирования защищённых систем?

9. Перечислите показатели качества процесса проектирования.

10. Постановка проблемы комплексного обеспечения информационной безопасности защищённых систем.

11. Основы методологии многовариантного планирования процесса проектирования.

12. Методы и методики проектирования комплексных систем информационной безопасности от несанкционированного доступа

13. Проектирование защищенной информационной системы для предприятий нефтегазовой отрасли.

14. Проектирование защищенной информационной системы для органов местного самоуправления.

15. Проектирование защищенной информационной системы для предприятий банковской сферы.

16. Проектирование защищенной информационной системы для муниципальных предприятий.

17. Проектирование защищенной информационной системы для машиностроительной отрасли.

18. Проектирование защищенной информационной системы для энергети- ческой отрасли.

19. Проектирование защищенной информационной системы для военизированной отрасли.

20. Проектирование защищенной информационной системы для строительной отрасли.

21. Проектирование защищенной информационной системы для металлургической отрасли.

22. Проектирование защищенной информационной системы для жилищно-коммунального хозяйства.

23. Разработка модели угроз образовательного учреждения.

24. Разработка модели угроз образовательного учреждения.

25. Разработка модели угроз медицинского учреждения.

26. Разработка модели угроз муниципального учреждения.

27. Разработка модели угроз коммерческой организации.

28. Разработка модели угроз банка.

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации не требуется, так как оценка за промежуточную аттестацию выставляется по балльно-рейтинговой системе, описанной в пункте 7.2.