МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Стратегии управления информационной безопасностью

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр

Формы обучения
Очная

Москва, 2023 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность» /И.В. Калуцкий/
к.т.н., доцент

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

Руководитель образовательной программы
Доцент. к.т.н. /С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Цель дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого, проектного и научно-исследовательского типов в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся с российскими нормативными правовыми документами, международными и отечественными стандартами в области обеспечения информационной безопасности;

- дать представление об угрозах, рисках и уязвимостях информационной безопасности;

- сформировать умение проводить анализ проблем информационной безопасности;

- сформировать навыки разработки концепции и политики информационной безопасности; -сформировать умение разрабатывать стратегию построения и внедрения системы

управления информационной безопасностью;

-сформировать практические навыки разработки технического задания на создание системы обеспечения информационной безопасности;

- научить выполнять оценку экономической эффективности системы обеспечения информационной безопасности предприятия.

Планируемые результаты обучения

В результате освоения дисциплины «Стратегии управления 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-2. Способен управлять проектом на всех этапах его жизненного цикла	ИУК-2.1. Разрабатывает концепцию управления проектом на всех этапах его жизненного цикла в рамках обозначенной проблемы: формулирует цель и пути достижения, задачи и способы их решения, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения. ИУК-2.2. Разрабатывает план реализации проекта в соответствии с существующими условиями, необходимыми ресурсами,

	возможными рисками и распределением зон ответственности участников проекта. ИУК-2.3. Осуществляет мониторинг реализации проекта на всех этапах его жизненного цикла, вносит необходимые изменения в план реализации проекта с учетом количественных и качественных параметров достигнутых промежуточных результатов
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1. Демонстрирует управленческую компетентность, необходимую для формирования команды и руководства ее работой на основе разработанной стратегии сотрудничества. ИУК-3.2. Планирует, организует, мотивирует, оценивает и корректирует совместную деятельность по достижению поставленной цели с учетом интересов, особенностей поведения и мнений ее членов. ИУК-3.3. Применяет способы, методы и стратегии оптимизации социально-психологического климата в коллективе, предупреждения и разрешения конфликтов, технологии обучения и развития профессиональной и коммуникативной компетентности членов команды
УК-6. Способен определять реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИУК-6.1. Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания. ИУК-6.2. Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. ИУК-6.3. Выстраивает собственную профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда
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 части, формируемой участниками образовательных отношений блока Б1 «Дисциплины (модули)».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Защита информации в системах обработки данных».

Дисциплина обеспечивает изучение дисциплин «Защита информации в автоматизированных системах управления технологическими процессами», «Защита информации от утечки по техническим каналам» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			3
1	**Аудиторные занятия**	**72**	3
	В том числе:		
1.1	Лекции	18	3
1.2	Семинарские/практические занятия		3
1.3	Лабораторные занятия	54	3
2	**Самостоятельная работа**	**72**	**3**
3	**Промежуточная аттестация**		**3**
	Экзамен		3

	Итого:	**144**	

3.2 Тематический 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. Ключевые вопросы информационной безопасности.		2		2		2
2	Раздел 2. Информационная безопасность в системе национальной безопасности России.		2		2		2
3	Раздел 3. Стандартизация процессов управления информационной безопасностью.		2		2		4
4	Раздел 4. Классификация угроз информационной безопасности.				2		2
5	Раздел 5. Модель нарушителя информационной безопасности.				2		6
6.	Раздел 6. Документальное обеспечение управления информационной безопасностью.		2		2		2
7.	Раздел 7. Система управления информационной безопасностью.		2		2		6
8.	Раздел 8. Корпоративная и частные политики информационной безопасности.		2		2		4
9.	Раздел 9. Процессы управления информационной безопасностью.				4		2
10.	Раздел 10. Организационные вопросы управления информационной безопасностью.		2		2		8
11.	Раздел 11. Технические аспекты управления информационной безопасностью.		2		2		4
12.	Раздел 12. Программные средства управления информационной безопасностью.				4		6
13.	Раздел 13. Идентификация и анализ информационных рисков.				4		8
14.	Раздел 14. Методы управления информационными рисками				4		4

15.	Раздел 15. Аудит информационной безопасности.		2		4		4
16.	Раздел 16. Оценка экономической эффективности деятельности по управлению информационной безопасностью.				8		4
17	Раздел 17 Измерение информационной безопасности. Оценка зрелости процессов управления информационной безопасностью.				6		4
Итого		**144**	**18**		**54**		**72**

3.3 Содержание дисциплины

Раздел 1. Ключевые вопросы информационной безопасности.
Тема раскрывает основные вопросы, касающиеся информационной безопсности.
Раздел 2. Информационная безопасность в системе национальной безопасности России.
Тема раскрывает основные моменты и нюансы в области информационной безопасности в системе национальной безопасности России.
Раздел 3. Стандартизация процессов управления информационной безопасностью.
Тема раскрывает стандартизацию процессов управления информационной безопасностью.
Раздел 4. Классификация угроз информационной безопасности.
Тема раскрывает основную классификацию угроз информационной безопасности.
Раздел 5. Модель нарушителя информационной безопасности.
Тема раскрывает основные аспекты модели нарушителя информационнойбезопасности.
Раздел 6. Документальное обеспечение управления информационной безопасностью.
Тема раскрывает основное документально обеспечение управления информационной безопасности.
Раздел 7. Система управления информационной безопасностью.
Тема раскрывает основы системы управления информационной безопасностью.
Раздел 8. Корпоративная и частные политики информационной безопасности.
Тема раскрывает основные моменты корпоративной и частной политики информационной безопасности.
Раздел 9. Процессы управления информационной безопасностью.
Тема раскрывает главные процессы управления информационной безопасности.
Раздел 10. Организационные вопросы управления информационной безопасностью.
Тема раскрывает основные организационные вопросы управления информационной безопасностью.
Раздел 11. Технические аспекты управления информационной безопасностью.
Тема раскрывает главные моменты технических аспектов управления информационной безопасностью.
Раздел 12. Программные средства управления информационной безопасностью.
Тема раскрывает главные программные средства управления информационной безопасностью.
Раздел 13. Идентификация и анализ информационных рисков.
Тема раскрывает идентификацию и анализ информационных рисков
Раздел 14. Методы управления информационными рисками.
Тема раскрывает основные методы управления информационной безопасностью.
Раздел 15. Аудит информационной безопасности.
Тема раскрывается основные моменты и нюансы аудита информационной безопасности.
Раздел 16. Оценка экономической эффективности деятельности по управлению информационной безопасностью.

Тема раскрывает оценку экономической эффективности деятельности по управлению информационной безопасностью.
Раздел 17. Измерение информационной безопасности. Оценка зрелости процессов управления информационной безопасностью.
Тема раскрывает основы измерения информационной безопасности.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

1. Анализ бизнес-процессов предприятия.
2. Анализ информационных потоков и ИТ-инфраструктуры предприятия.
3. Анализ внутренних и внешних угроз информационной безопасности.
4. Построение модели нарушителя.
5. Анализ информационных рисков предприятия.
6. Разработка концепции информационной безопасности предприятия.
7. Разработка политики информационной безопасности предприятия.
8. Разработка технического задания на создание системы обеспечения информационной безопасности предприятия.
9. Оценка экономической эффективности системы обеспечения информационной безопасности предприятия.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный государственный образовательный стандарт высшего образования (уровень магистратуры) по направлению подготовки 10.04.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1455.

2. Профессиональные стандарты:

- 06.032 Специалист по безопасности компьютерных систем и сетей. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 № 533н;
- 06.033 Специалист по защите информации в автоматизированных системах. Утвержден приказом Министерства труда и социальной защиты РФ от 14.09.2022 г. № 525н).

4.2 Основная литература

1. Парфёнов, Ю. П. Средства управления и защиты информационных ресурсов автоматизированных систем : учебное пособие / Ю. П. Парфёнов. — 2-е изд. — Москва : ФЛИНТА, 2022. — 120 с. — ISBN 978-5-9765-5016-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/231707. — Режим доступа: для авториз. пользователей.

2 Гультяева Т.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Т.А. Гультяева; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=574729

3 Шилов А.К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / А.К. Шилов; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной

безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=500065

4.3 Дополнительная литература

1 Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. – М.: ФЛИНТА, 2016. – 269 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=93245

2 Бекетнова Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем [Электронный ресурс]: учебное пособие / Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2018. – 173 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=494850

3 Веселов Г.Е. Менеджмент риска информационной безопасности [Электронный ресурс]: учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов; Министерство образования и науки РФ, Южный федеральный университет, Инженерно- технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 109 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=493331

4.4 Электронные образовательные ресурсы

ЭОР разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

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

4.6 Современные профессиональные базы данных и информационные справочные материалы

1. Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа: http://www.consultant.ru/online/
2. Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа: http://government.ru/department/387/events/
3. Официальный сайт Росстата [электронный ресурс] — Режим доступа: www.gks.ru/
4. 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа: http://geoline-tech.com/top-20-sites-about-information-security/
5. Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа: http://dorlov.blogspot.com/p/blog-page_3151.html
6. Информационная безопасность [электронный ресурс] — Режим доступа: http://www.securrity.ru/
7. 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа: https://proglib.io/p/information-security-guide/
8. Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа: https://habr.com/ru/hub/infosecurity/
9. База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа: http://wiki.informationsecurity.club/doku.php/main

10. Информационная безопасность. Защита данных [электронный ресурс] — Режим доступа: http://all-ib.ru/

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

6.1 Методические 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.

6.2 Методические 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

7.1 Методы 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.

7.2 Шкала 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. Понятие и задачи информационной безопасности.
2. Уровни обеспечения информационной безопасности.
3. Правовая защита информации.
4. Место информационной безопасности в системе национальной безопасности.
5. Политика обеспечения информационной безопасности Российской Федерации.
6. Современные проблемы информационной безопасности.
7. Модель информационной безопасности организации.
8. Стандартизация процессов управления информационной безопасностью.
9. Состав организационно-распорядительных документов по обеспечению информационной безопасности.
10. Концепция информационной безопасности. Корпоративная политика информационной безопасности.

11. Частные политики информационной безопасности.
12. Система управления информационной безопасностью.
13. Стратегии построения системы управления информационной безопасностью.
14. Процессный подход к управлению информационной безопасностью.
15. Ресурсы, результаты, владельцы процесса управления информационной безопасностью.
16. Программные средства управления информационной безопасностью.
17. Содержание технического задания на создание системы обеспечения информационной безопасности предприятия.
18. Организационные вопросы управления информационной безопасностью. Состав и основные функции службы безопасности организации.
19. Технические аспекты управления информационной безопасностью.
20. Классификация угроз информационной безопасности.
21. Классификация уязвимостей.
22. Классификация информационных рисков.
23. Идентификация и анализ информационных рисков.
24. Методы оценивания информационных рисков.
25. Обеспечение безопасности персональных данных.
26. Аудит информационной безопасности.
27. Экономическая оценка обеспечения информационной безопасности.
28. Методика совокупной стоимости владения компании Gartner Group
29. Измерение информационной безопасности.
30. Модели зрелости процессов управления информационной безопасностью.

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.