Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.08**
Трудоемкость в зачетных единицах:	**8 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**8 семестр - 28 часа;**
Практические занятия	**8 семестр - 28 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 семестр - 85,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование** **Контрольная работа** **Коллоквиум**	
Промежуточная аттестация:	
Экзамен	**8 семестр - 0,5 часа;**

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: освоение комплекса общекультурных и профессиональных компетенций, связанных с изучением назначения, целей, решаемых задач, структуры системы обеспечения информационной безопасности предприятия (организации) (СОИБ), организации ее функционирования, а также принципах и содержании управления данной системой.

Задачи дисциплины

- изучение теории по вопросам назначения, целей, решаемых задач, структуры СОИБ и организации ее функционирования по обеспечению информационной безопасности активов предприятия (организации);;
- формирование готовности и способности к активной профессиональной деятельности по организации и обеспечению функционирования СОИБ в условиях информационного противоборства;;
- приобретение практических навыков структурной многоуровневой декомпозиции СОИБ..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
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: - нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;; - комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности;. уметь: - организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины.
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		знать: - состав и перечень информационных активов предприятия, относящихся к защищаемой информации;; - теорию анализа и синтеза сложных организационной-иерархических систем;. уметь: - провести полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		средствам;; - выполнять работы по администрированию основных подсистем СОИБ предприятия малого и среднего бизнеса;.
ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности		знать: - комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия;. уметь: - применять системный подход к управлению информационной безопасностью предприятия;; - правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;.
ПСК-3 Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП		знать: - психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности. уметь: - на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основы организации и функционирования СОИБ предприятия	27	8	7	-	7	-	-	-	-	-	13	-	***Подготовка к практическим занятиям:*** Структура и функции подсистем СОИБ предприятия.
1.1	Роль и место информационной безопасности в обеспечении комплексной безопасности предприятия	8		2	-	2	-	-	-	-	-	4	-	***Подготовка к практическим занятиям:*** Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации); ***Подготовка к практическим занятиям:*** Организация функционирования СОИБ предприятия на основе системного подхода.
1.2	Система обеспечения информационной безопасности предприятия.	11		3	-	3	-	-	-	-	-	5	-	***Изучение материалов литературных источников:*** [1], 13-19 [2], 22-45 [3], 60-74 [4], 26-45
1.3	Перечень факторов, влияющих на организацию СОИБ предприятия:	8		2	-	2	-	-	-	-	-	4	-	
2	Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия	81		21	-	21	-	-	-	-	-	39	-	***Подготовка к практическим занятиям:*** Разработка программы аудита безопасности ИС объекта КВО энергетики Анализ сведений аудита.
2.1	Правовые основы функционирования СОИБ предприятия.	11		3	-	3	-	-	-	-	-	5	-	***Подготовка к практическим занятиям:*** Применение методов администрирования для настроек основных функций программно-аппаратного обеспечения функционирования СОИБ предприятия
2.2	Организационные основы	14		4	-	4	-	-	-	-	-	6	-	***Подготовка расчетных заданий:***

	функционирования СОИБ предприятия.													Экономическое обоснование проекта по технической защите информационной системы предприятия.
2.3	Кадровое обеспечение СОИБ предприятия.	8		2	-	2	-	-	-	-	-	4	-	***Подготовка реферата:*** Разработка элементов программы повышения осведомленности сотрудников организации банковской сферы в вопросах информационной безопасности
2.4	Финансово-экономическое обеспечение функционирования СОИБ предприятия.	8		2	-	2	-	-	-	-	-	4	-	***Подготовка домашнего задания:*** Разработка и оформление документов политики информационной безопасности предприятия.
2.5	Инженерно-техническое обеспечение СОИБ. .	8		2	-	2	-	-	-	-	-	4	-	***Подготовка реферата:*** Сбор и анализ исходных данных для разработки Документа Политики информационной безопасности предприятия
2.6	Программно-аппаратное обеспечение функционирования СОИБ предприятия.	8		2	-	2	-	-	-	-	-	4	-	***Изучение материалов литературных источников:*** [1], 64-66 [2], 56-68 [3], 88-95
2.7	Подсистема аудита информационной системы предприятия.	8		2	-	2	-	-	-	-	-	4	-	
2.8	Управление СОИБ предприятия. Понятие и цели управления.	16		4	-	4	-	-	-	-	-	8	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**28**	**-**	**28**	**-**	**2**	**-**	**-**	**0.5**	**52**	**33.5**	
	Итого за семестр	**144.0**		**28**	**-**	**28**	**2**		**-**		**0.5**	**85.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основы организации и функционирования СОИБ предприятия

1.1. Роль и место информационной безопасности в обеспечении комплексной безопасности предприятия

Основы системного подхода к обеспечению информационной безопасности предприятия малого и среднего бизнеса. Этапы реализации системного подхода..

1.2. Система обеспечения информационной безопасности предприятия.

Понятие, сущность, назначение и задачи СОИБ предприятия. Методологические основы организации СОИБ. Основные требования, предъявляемые к СОИБ и содержательная характеристика этапов ее разработки..

1.3. Перечень факторов, влияющих на организацию СОИБ предприятия:

форма собственности, организационно-правовая форма и характер основной деятельности хозяйствующего субъекта; состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение; режим функционирования, ресурсообеспечение и уровень автоматизации (цифровизации) основных информационных процессов. Политика информационной безопасности. Политика по управлению информационной безопасностью..

2. Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия

2.1. Правовые основы функционирования СОИБ предприятия.

Структура правового обеспечения ИБ. Стандартизация в области ИБ. Комплекс внутренней нормативно-организационной документации. Лицензирование, сертификация и аттестация в области информационной безопасности..

2.2. Организационные основы функционирования СОИБ предприятия.

Назначение, цели и задачи организационного обеспечения. Организация эффективного функционирования СОИБ на основе Политики информационной безопасности..

2.3. Кадровое обеспечение СОИБ предприятия.

Назначение, цели и задачи кадрового обеспечения. Основные мероприятия, проводимые при подборе, работе, увольнении сотрудников подразделений ИБ. Программы повышения осведомленности в области ИБ. Особенности профессиональной этики специалиста в области ИБ..

2.4. Финансово-экономическое обеспечение функционирования СОИБ предприятия.

Экономические основы СОИБ. Модели для оценки экономической эффективности инвестиций в СОИБ предприятия..

2.5. Инженерно-техническое обеспечение СОИБ. .

Инженерно-техническая защита территорий, зданий и помещений предприятия. Организация защиты информации от утечки по техническим каналам. Методы и средства защиты информации от утечки по техническим каналам.

2.6. Программно-аппаратное обеспечение функционирования СОИБ предприятия.

Назначение, цели и задачи подсистемы программно-аппаратного обеспечения СОИБ. Силы и программные средства защиты информации..

2.7. Подсистема аудита информационной системы предприятия.

Назначение, цели и задачи подсистемы аудита информационной безопасности. Направления деятельности подсистемы аудита. Технологии проведения аудита. Этапы проведения аудита ИБ. Особенности активного аудита..

2.8. Управление СОИБ предприятия. Понятие и цели управления.

Сущность процессов управления СОИБ. Принципы управления и анализ системы управления СОИБ. Структура и содержание управления СОИБ организации..

3.3. Темы практических занятий

1. Выявление состава информационных активов предприятия. Определение перечня информации, составляющей коммерческую тайну. Разработка проекта перечня сведений, составляющих коммерческую тайну.;
2. Направления деятельности подсистемы аудита информационной безопасности. Технологии проведения аудита. Этапы проведения аудита ИБ. Особенности активного аудита.;
3. Организация защиты компьютерной (цифровой) информации в информационной системе предприятию. Программно-аппаратное обеспечение функционирования СОИБ предприятия. .;
4. Организация инженерно-технической защиты территорий, зданий и помещений предприятия. Организация мероприятий защиты информации предприятия от утечки по техническим каналам.;
5. Моделирование и оценка экономической эффективности инвестиций в СОИБ предприятия.;
6. Кадровое обеспечение функционирования СОИБ. Особенности работы с персоналом СОИБ. Особенности профессиональной этики специалиста в области ИБ.;
7. Организация эффективного функционирования СОИБ на основе Политики информационной безопасности. Моделирование информационной системы предприятия с позиций безопасности.;
8. Правовые основы функционирования СОИБ предприятия. Структура законодательства РФ в сфере ИБ. Стандартизация в области ИБ. Комплекс внутренней нормативно-организационной документации СОИБ.;
9. Политика информационной безопасности предприятия. Основные положения и документы Политики ИБ. Разработка модели информационной системы предприятия с позиций безопасности.;
10. Внутренние организационно-распорядительные документы СОИБ, их состав и содержание.;
11. Сущность и задачи СОИБ предприятия, принципы организации, этапы разработки и факторы, влияющие на организацию СОИБ..

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Консультации проводятся по разделу "Основы организации и функционирования СОИБ предприятия"
2. Проводится по материалам раздела "Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия"

Текущий контроль (ТК)

1. Проводятся по разделу "Основы организации и функционирования СОИБ предприятия"
2. Проводятся по разделу "Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
Знать:				
комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности;	ОПК-7(Компетенция)	+	+	Контрольная работа/Контрольная работа
нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;	ОПК-7(Компетенция)		+	Контрольная работа/Контрольная работа
теорию анализа и синтеза сложных организационной-иерархических систем;	ПК-4(Компетенция)	+		Контрольная работа/Контрольная работа
состав и перечень информационных активов предприятия, относящихся к защищаемой информации;	ПК-4(Компетенция)	+	+	Коллоквиум/Коллоквиум
комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия;	ПК-14(Компетенция)		+	Тестирование/Тестирование
психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности	ПСК-3(Компетенция)	+	+	Тестирование/Тестирование
Уметь:				
организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины	ОПК-7(Компетенция)	+	+	Коллоквиум/Коллоквиум
выполнять работы по администрированию основных подсистем	ПК-4(Компетенция)		+	Контрольная

СОИБ предприятия малого и среднего бизнеса;				работа/Контрольная работа
провести полный перечень работы по классификации СОИБ организации по подсистемам, направлениям, силам и средствам;	ПК-4(Компетенция)		+	Контрольная работа/Контрольная работа
правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;	ПК-14(Компетенция)		+	Тестирование/Тестирование
применять системный подход к управлению информационной безопасностью предприятия;	ПК-14(Компетенция)	+		Контрольная работа/Контрольная работа
на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности.	ПСК-3(Компетенция)		+	Тестирование/Тестирование

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Защита задания

1. Коллоквиум (Коллоквиум)

Форма реализации: Письменная работа

1. Контрольная работа (Контрольная работа)
2. Тестирование (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

Итоговая оценка выставляется в соответствии с алгоритмом системы БАРС из семестровой и экзаменационной составляющей

В диплом выставляется оценка за 8 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Минзов, А. С. Методика выполнения дипломных работ : учебное пособие для института безопасности бизнеса / А. С. Минзов, А. Ю. Невский, Н. В. Унижаев ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2007 . – 100 с. - ISBN 978-5-383-00024-3 .;
2. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;
3. Минзов, А. С. Профессиональная этика в сфере информационной и экономической безопасности : [монография] / А. С. Минзов, Нац. исслед. ун-т "МЭИ", Ин-т информац. и экономич. безопасности . – М. : ВНИИгеосистем, 2013 . – 132 с. - ISBN 978-5-8481-0135-5 .;
4. А. А. Камардина- "Профессиональная этика", Издательство: "Оренбургский государственный университет", Оренбург, 2013 - (167 с.)
https://biblioclub.ru/index.php?page=book&id=258824.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;

4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных журналов издательства Elsevier** - https://www.sciencedirect.com/
6. **Электронные ресурсы издательства Springer** - https://link.springer.com/
7. **База данных Web of Science** - http://webofscience.com/
8. **База данных Scopus** - http://www.scopus.com
9. **Национальная электронная библиотека** - https://rusneb.ru/
10. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
11. **Журналы American Chemical Society** - https://www.acs.org/content/acs/en.html
12. **Журналы American Institute of Physics** - https://www.scitation.org/
13. **Журналы American Physical Society** - https://journals.aps.org/about
14. **База данных издательства Annual Reviews Science Collection** - https://www.annualreviews.org/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
Учебные аудитории для проведения лабораторных занятий	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба,

	обеспечение"	компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Система обеспечения информационной безопасности предприятия

(название дисциплины)

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Тестирование (Тестирование)
КМ-2 Контрольная работа (Контрольная работа)
КМ-3 Коллоквиум (Коллоквиум)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	12
1	Основы организации и функционирования СОИБ предприятия				
1.1	Роль и место информационной безопасности в обеспечении комплексной безопасности предприятия				+
1.2	Система обеспечения информационной безопасности предприятия.			+	
1.3	Перечень факторов, влияющих на организацию СОИБ предприятия:		+	+	+
2	Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия				
2.1	Правовые основы функционирования СОИБ предприятия.			+	
2.2	Организационные основы функционирования СОИБ предприятия.		+	+	+
2.3	Кадровое обеспечение СОИБ предприятия.		+		
2.4	Финансово-экономическое обеспечение функционирования СОИБ предприятия.				+
2.5	Инженерно-техническое обеспечение СОИБ. .			+	
2.6	Программно-аппаратное обеспечение функционирования СОИБ предприятия.			+	
2.7	Подсистема аудита информационной системы предприятия.		+		
2.8	Управление СОИБ предприятия. Понятие и цели управления.		+	+	
		Вес КМ, %:	30	30	40