

**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 автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

**Рабочая программа дисциплины**  
**ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	Базовая
<b>№ дисциплины по учебному плану:</b>	Б1.Б.28
<b>Трудоемкость в зачетных единицах:</b>	8 семестр - 9;
<b>Часов (всего) по учебному плану:</b>	324 часа
<b>Лекции</b>	8 семестр - 16 часов;
<b>Практические занятия</b>	8 семестр - 16 часов;
<b>Лабораторные работы</b>	8 семестр - 8 часов;
<b>Консультации</b>	8 семестр - 16 часов;
<b>Самостоятельная работа</b>	8 семестр - 263,2 часа;
<b>в том числе на КП/КР</b>	8 семестр - 15,7 часов;
<b>Иная контактная работа</b>	8 семестр - 4 часа;
<b>включая:</b>	
<b>Отчет</b>	
<b>Промежуточная аттестация:</b>	
<b>Защита курсовой работы</b>	8 семестр - 0,3 часа;
<b>Экзамен</b>	8 семестр - 0,5 часа;
	<b>всего - 0,8 часа</b>

**Москва 2019**

**ПРОГРАММУ СОСТАВИЛ:**

Преподаватель

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Капгер И.В.
	Идентификатор	R5d33df1e-KapgerIV-059b09ee

И.В. Капгер

**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

Заведующий выпускающей  
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

А.Ю. Невский

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** освоение профессиональных компетенций по формированию готовности студентов разрабатывать системы защиты информации на основе применения методов и средств программно-аппаратной защиты информации

### Задачи дисциплины

- сформировать у студентов системные теоретические знания и практические навыки по организации и технологии программно-аппаратной защиты информации.

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-3 способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач		знать: - основные руководящие правовые, методические, и нормативные документы по программно-аппаратной защите информации.  уметь: - выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности.
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		знать: - основные теоретические сведения: сущность, цели, задачи и принципы программно-аппаратной защиты информации.  уметь: - устанавливать, настраивать и обслуживать программные, программно-аппаратные.
ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации		знать: - основные руководящие правовые, методические, и нормативные требования по оценке защищенности средств программно-аппаратной защиты информации.  уметь: - выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности.
ПК-6 способностью принимать участие в организации и проведении		знать: - перечень, классификацию, принцип действия программно-аппаратных

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации		<p>средств защиты информации.</p> <p>уметь:</p> <ul style="list-style-type: none"> <li>- выполнять действия по установке, конфигурированию и настройке программно-аппаратных средств защиты информации.</li> </ul>
ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		<p>знать:</p> <ul style="list-style-type: none"> <li>- основные характеристики технических средств защиты информации от несанкционированного доступа.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе.</li> </ul>
ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасного функционирования объектов энергетики с элементами АСУ ТП		<p>знать:</p> <ul style="list-style-type: none"> <li>- программно-аппаратные средства обеспечения защиты информации автоматизированных систем.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе.</li> </ul>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин основной профессиональной образовательной программе Безопасность автоматизированных 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 9 зачетных единиц, 324 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	Технологии идентификации, аутентификации, авторизации и управления доступом	129	8	8	3	8	-	-	-	-	-	110	-	<p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Технологии идентификации, аутентификации, авторизации и управления доступом"</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Технологии идентификации, аутентификации, авторизации и управления доступом" подготовка к выполнению заданий на практических занятиях</p>
1.1	Предмет и задачи программно-аппаратной защиты информации	11		1	-	-	-	-	-	-	-	10	-	
1.2	Средства программно-аппаратной защиты информации	11		1	-	-	-	-	-	-	-	10	-	
1.3	Автоматизированная система	11		1	-	-	-	-	-	-	-	10	-	
1.4	Идентификация и аутентификация	17		1	-	2	-	-	-	-	-	14	-	
1.5	Санкционированный и несанкционированный доступ	24		1	1	2	-	-	-	-	-	20	-	
1.6	Разграничение ресурсов в локальных автоматизированных системах	26		1	1	2	-	-	-	-	-	22	-	
1.7	Управление доступом при помощи средств защиты информации от	29		2	1	2	-	-	-	-	-	24	-	

	несанкционированног о доступа												
2	Обеспечение конфиденциальности, целостности и доступности информации	125	8	5	8	-	-	-	-	-	104	-	<b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Обеспечение конфиденциальности, целостности и доступности информации" подготовка к выполнению заданий на практических занятиях
2.1	Контрольные суммы. Целостность в АС	28	1	1	2	-	-	-	-	-	24	-	<b><u>Самостоятельное изучение</u></b>
2.2	Межсетевые экраны	28	1	1	2	-	-	-	-	-	24	-	<b><u>теоретического материала:</u></b> Изучение
2.3	Защищенные носители	33	2	1	2	-	-	-	-	-	28	-	дополнительного материала по разделу "Обеспечение конфиденциальности, целостности и доступности информации"
2.4	Централизованное управление средствами защиты информации	36	4	2	2	-	-	-	-	-	28	-	<b><u>Изучение материалов литературных источников:</u></b>  [3], 76-154 [4], 38-91
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	34.0	-	-	-	14	-	4	-	0.3	15.7	-	
	<b>Всего за семестр</b>	<b>324.0</b>	<b>16</b>	<b>8</b>	<b>16</b>	<b>14</b>	<b>2</b>	<b>4</b>	<b>-</b>	<b>0.8</b>	<b>229.7</b>	<b>33.5</b>	
	<b>Итого за семестр</b>	<b>324.0</b>	<b>16</b>	<b>8</b>	<b>16</b>	<b>16</b>	<b>4</b>	<b>0.8</b>			<b>263.2</b>		

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПП – 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. Технологии идентификации, аутентификации, авторизации и управления доступом

- 1.1. Предмет и задачи программно-аппаратной защиты информации
- 1.2. Средства программно-аппаратной защиты информации
- 1.3. Автоматизированная система
- 1.4. Идентификация и аутентификация
- 1.5. Санкционированный и несанкционированный доступ
- 1.6. Разграничение ресурсов в локальных автоматизированных системах
- 1.7. Управление доступом при помощи средств защиты информации от несанкционированного доступа

#### 2. Обеспечение конфиденциальности, целостности и доступности информации

- 2.1. Контрольные суммы. Целостность в АС
- 2.2. Межсетевые экраны
- 2.3. Защищенные носители
- 2.4. Централизованное управление средствами защиты информации

### **3.3. Темы практических занятий**

1. 8. Построение и анализ отказоустойчивости RAID-массивов различных типов;
2. 7. Практическое использование программы архивирования данных Backup;
3. 6. Изучение возможностей и настройка программного межсетевого экрана;
4. 5. Изучение возможностей и настройка аппаратного межсетевого экрана;
5. 1. Технология защиты документов в приложениях MS Office;
6. 3. Механизмы контроля целостности данных;
7. 2. Возможности операционных систем MS Windows по ограничению прав пользователей;
8. 9. Работа с программным обеспечением для резервного копирования Acronis® Backup

& Recovery™ 10 Workstation;

9. 4.Реализация аппаратного блокирования рабочей станции с использованием аппаратного модуля доверенной загрузки "Аккорд-АМДЗ";

10. 10.Проактивные технологии антивирусной защиты.

### 3.4. Темы лабораторных работ

1. 1.Анализ уязвимостей доступа к операционным системам MS Windows;

2. 2.Организация логического входа в операционные системы MS Windows с помощью аппаратных ключей;

3. 3.Изучение программно-аппаратного комплекса биометрической аутентификации (BioLink Authentication Center/ Biolink U-Match);

4. 4.Использование программно-аппаратного комплекса «Аккорд»;

5. 5.Механизмы контроля доступа специализированных средств защиты информации от НСД сетевых средств и ПЭВМ.

### 3.5 Консультации

### 3.6 Тематика курсовых проектов/курсовых работ 8 Семестр

Курсовая работа (КР)

Темы:

- 1.АМДЗ «Аккорд».

- 2.Программный продукт SecretNet

- 3.Программный продукт DeviceLock

- 4.Средство биометрической аутентификации BioLink

#### График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 15	Зачетная
Раздел курсового проекта	1	2, 3	4	Защита курсового проекта
Объем раздела, %	40	40	20	-
Выполненный объем нарастающим итогом, %	40	80	100	-

Номер раздела	Раздел курсового проекта
1	Описание объекта анализа
2	Описание объекта анализа
3	Разработка проекта программно-аппаратной защиты ЛВС
4	Заключение

### 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	
<b>Знать:</b>				
основные руководящие правовые, методические, и нормативные документы по программно-аппаратной защите информации	ОПК-3(Компетенция)		+	Отчет/Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail»
основные теоретические сведения: сущность, цели, задачи и принципы программно-аппаратной защиты информации	ПК-1(Компетенция)	+		Отчет/Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX»
основные руководящие правовые, методические, и нормативные требования по оценке защищенности средств программно-аппаратной защиты информации	ПК-5(Компетенция)		+	Отчет/Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail»
перечень, классификацию, принцип действия программно-аппаратных средств защиты информации	ПК-6(Компетенция)	+		Отчет/Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64K»
основные характеристики технических средств защиты информации от несанкционированного доступа	ПК-7(Компетенция)	+		Отчет/Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64K»
программно-аппаратные средства обеспечения защиты информации автоматизированных систем	ПСК-2(Компетенция)	+		Отчет/Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX»
<b>Уметь:</b>				

выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности	ОПК-3(Компетенция)	+		Отчет/Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64К»
устанавливать, настраивать и обслуживать программные , программно-аппаратные	ПК-1(Компетенция)	+		Отчет/Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX»
выявлять и оценивать угрозы безопасности информации в конкретных компьютерных системах, а также оценивать степень их актуальности	ПК-5(Компетенция)	+		Отчет/Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА»
выполнять действия по установке, конфигурированию и настройке программно-аппаратных средств защиты информации	ПК-6(Компетенция)	+		Отчет/Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА»
определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	ПК-7(Компетенция)		+	Отчет/Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail»
производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе	ПСК-2(Компетенция)	+		Отчет/Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX»

#### **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: Письменная работа

1. Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX» (Отчет)
2. Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64K» (Отчет)
3. Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА» (Отчет)
4. Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail» (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

Балльно-рейтинговая структура курсовой работы является приложением Б.

##### **4.2 Промежуточная аттестация по дисциплине**

Экзамен (Семестр №8)

Курсовая работа (КР) (Семестр №8)

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. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлению "Информационная безопасность" / П. Б. Хорев . – 2-е изд., испр. и доп . – М. : Форум : ИНФРА-М, 2017 . – 352 с. – (Высшее образование) . - ISBN 978-5-00091-004-7 .;
2. Хорев, П. Б. Использование криптографических интерфейсов : учебное пособие по курсам "Защита информации" и "Методы и средства защиты компьютерной информации" по специальностям "Прикладная математика" и "Информационные системы и технологии" / П. Б. Хорев ; Ред. М. М. Маран ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2007 . – 112 с. - ISBN 978-5-383-00032-8 .;
3. Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В.- "Программно-аппаратные средства обеспечения информационной безопасности", Издательство: "Горячая линия-Телеком", Москва, 2018 - (248 с.)  
<https://e.lanbook.com/book/111053>;
4. Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков- "Программно-аппаратные средства защиты информационных систем", Издательство: "Тамбовский государственный

технический университет (ТГТУ)", Тамбов, 2017 - (194 с.)  
<https://biblioclub.ru/index.php?page=book&id=499013>.

## 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](http://biblioclub.ru/index.php?page=main_ub_red)
3. Электронные ресурсы издательства Springer - <https://link.springer.com/>
4. База данных Web of Science - <http://webofscience.com/>
5. База данных Scopus - <http://www.scopus.com>
6. Национальная электронная библиотека - <https://rusneb.ru/>
7. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
8. Журнал Science - <https://www.sciencemag.org/>
9. Журналы издательства Wiley - <https://onlinelibrary.wiley.com/>
10. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
11. Портал открытых данных Российской Федерации - <https://data.gov.ru>
12. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>  
<http://docs.cntd.ru/>
13. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
14. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
15. Федеральный портал "Российское образование" - <http://www.edu.ru>

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	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	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения лабораторных занятий	М-503, Учебная лаборатория "Программно-аппаратная средства защиты"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер

	информации"	персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, 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 обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, 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	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, 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

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

### Программно-аппаратные средства защиты информации

(название дисциплины)

#### 8 семестр

#### Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Отчет по практической работе №1 «Установка и настройка средства доверенной загрузки «Аккорд-GX» (Отчет)
- КМ-2 Отчет по практической работе №2 «Установка и настройка программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-Win64K» (Отчет)
- КМ-3 Отчет по практической работе №3 Установка и настройка персонального средства криптографической защиты информации «ШИПКА» (Отчет)
- КМ-4 Отчет по практической работе №4 Установка и настройка средства криптографической защиты информации «Crypton ArcMail» (Отчет)

#### Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Технологии идентификации, аутентификации, авторизации и управления доступом					
1.1	Предмет и задачи программно-аппаратной защиты информации		+			
1.2	Средства программно-аппаратной защиты информации		+			
1.3	Автоматизированная система		+	+	+	
1.4	Идентификация и аутентификация			+	+	
1.5	Санкционированный и несанкционированный доступ			+	+	
1.6	Разграничение ресурсов в локальных автоматизированных системах			+	+	
1.7	Управление доступом при помощи средств защиты информации от несанкционированного доступа			+		
2	Обеспечение конфиденциальности, целостности и доступности информации					
2.1	Контрольные суммы. Целостность в АС					+
2.2	Межсетевые экраны					+
2.3	Защищенные носители					+

2.4	Централизованное управление средствами защиты информации				+
	Вес КМ, %:	25	25	25	25

**БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА  
КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ**

Программно-аппаратные средства защиты информации

(название дисциплины)

**8 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:**

КМ-1 Соблюдение графика выполнения КР

КМ-2 Оценка выполнения КР

КМ-3 Оценка оформления КР

**Вид промежуточной аттестации – защита КР.**

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	15
1	Описание объекта анализа		+		
2	Описание объекта анализа			+	
3	Разработка проекта программно-аппаратной защиты ЛВС			+	
4	Заключение				+
Вес КМ, %:			40	40	20