МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационных технологий»
_____ / Д.Г. Демидов /
«26» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в автоматизированных системах управления технологическими процессами»

Направление подготовки
«10.05.03 Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист

Формы обучения
Очная

Москва, 2026 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»,
к.т.н.  /С.А. Кесель/

Ассистент кафедры «Информационная безопасность»  /А.В. Шорников/

Согласовано:
Заведующий кафедрой «Информационная безопасность»,
к.т.н., доцент  /И.В. Калуцкий/

Руководитель образовательной программы
ст. преподаватель кафедры «Информационная безопасность»  /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Защита информации в автоматизированных системах управления технологическими процессами» следует отнести:

- формирование у студентов теоретических знаний о необходимом комплексе мер ИБ, организационной структуре АСУ ТП, вероятных угрозах и внешних воздействиях на такие системы;
- развитие у студентов практических навыков и умений по организации и поддержании выполнения комплекса мер ИБ, управления процессом их реализации с учетом решаемых задач и организационной структуры АСУ ТП, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации; проведения анализа ИБ объектов и систем на соответствие требованиям стандартов в области защиты информации.

К **основным задачам** освоения дисциплины «Защита информации в автоматизированных системах управления технологическими процессами» следует отнести:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- изучение способов и средств защиты информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

Обучение по дисциплине «Защита информации в автоматизированных системах управления технологическими процессами» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	ИПК-3.1. Знает: отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные методы и средства обеспечения безопасности операционных систем; основные методы и средства обеспечения сетевой безопасности; основные методы и средства обеспечения безопасности в системах управления базами данных. ИПК-3.2. Умеет: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности.

	ИПК-3.3. Владеет: навыками применения отечественных и международных стандартов информационной
ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	ИПК-15.1. Знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности. ИПК-15.2. Умеет: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности ИПК-15.3. Владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

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: «Физические основы защиты информации», «Стандартизация и сертификация в информационной безопасности», «Методы и средства криптографической защиты», «Программно-аппаратные средства защиты информации».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	**7**	1-18
	В том числе:			
1.1	Лекции	4	7	1-18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	68	7	1-18
2	**Самостоятельная работа**	**72**	**7**	
3	**Промежуточная аттестация**		**7**	19-21
	Экзамен		7	19-21
	Итого	**144**		

3.1.2 Очно-заочная форма обучения

Не предусмотрена.

3.1.3 Заочная форма обучения

Не предусмотрена.

3.2 Тематический план изучения дисциплины
(по формам обучения)

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. Автоматизированные системы управления технологическим процессом.	**50**	**2**		**24**		**24**
1.1	Тема 1. Промышленные протоколы. Особенности. Описание «типового» предприятия.		2		8		8
1.2	Тема 2. Проблематика защиты АСУ ТП; Классификация АСУ ТП.				8		8
1.3	Тема 3. Знакомство с контроллерами, система центрального управления и их уязвимостями				8		8
2	Раздел 2. Нормативно-правовая база защиты информации в АСУ ТП	**46**	**2**		**20**		**24**
2.1	Тема 1. Нормативные акты. Международные стандарты и практики. Концепции ИБ АСУ ТП.		2		4		8
2.2	Тема 2. Формирование требований к защите информации в АСУ. Нормативное обеспечение системе защиты информации в АСУ ТП				8		8
2.3	Тема 3. Требования к мерам защиты информации в АСУ и их выбор				8		8
3	Раздел 3. Разработка системы защиты АСУ ТП.	**48**			**24**		**24**
3.1	Тема 1. Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.				8		8
3.2	Тема 2. Внедрение системы защиты АСУ и ввод ее в действие.				8		8

3.3	Тема 3. Обеспечение защиты информации в ходе эксплуатации АСУ, а также при выводе АСУ из эксплуатации.				8		8
	Итого	**144**	**4**		**68**		**72**

3.2.2 Очно-заочная форма обучения

Не предусмотрена

3.2.3 Заочная форма обучения

Не предусмотрена

3.3 Содержание дисциплины

Раздел 1. Автоматизированные системы управления технологическим процессом.

Тема 1. Промышленные протоколы. Особенности. Описание «типового» предприятия.

Типовое представление АСУ ТП в рамках процессов предприятия. Особенности АСУ ТП в промышленности. Создание модели условного «типового» предприятия.

Тема 2. Проблематика защиты АСУ ТП; Классификация АСУ ТП.

Наиболее актуальные вероятные угрозы информационной безопасности при обработке информации в АСУ ТП. Возможные недопустимые события в рамках работы АСУ ТП, возможные внешние события. Классификация АСУ ТП и информации, обрабатываемой АСУ ТП.

Тема 3. Знакомство с контроллерами, система центрального управления и их уязвимостями.

Актуальные угрозы и уязвимости для управляющих устройств АСУ ТП. Контроллеры, система центрального управления, структура АСУ ТП. Основные способы противодействия уязвимостям аппаратного обеспечения.

Раздел 2. Нормативно-правовая база защиты информации в АСУ ТП.

Тема 1. Нормативные акты. Международные стандарты и практики. Концепции ИБ АСУ ТП.

Нормативно-правовая база для функционирования системы защиты АСУ ТП. Обзор национальных и международных стандартов в сфере защиты информации в АСУ ТП. Возможные концепции и подходы к обеспечению информационной безопасности в АСУ ТП.

Тема 2. Формирование требований к защите информации в АСУ. Нормативное обеспечение системе защиты информации в АСУ ТП.

Минимально необходимый набор требований, предъявляемых федеральными органами исполнительной власти, в области обеспечения информационной безопасности, к АСУ ТП. Обязательная организационно-распорядительная документация, необходимая для ввода в эксплуатацию системы защиты информации в АСУ ТП.

Тема 3. Требования к мерам защиты информации в АСУ и их выбор.

Обоснование к выбранным мерам защиты информации в АСУ ТП. Методики и способы по оптимизации мер для поддержания необходимого уровня информационной безопасности на предприятии.

Раздел 3. Разработка системы защиты АСУ ТП.

Тема 1. Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.

Работа с профессиональными базами и профильными справочниками. Составление примера модели угроз для АСУ ТП. Особенности при моделировании угроз в зависимости от сферы деятельности предприятия.

Тема 2. Внедрение системы защиты АСУ и ввод ее в действие.

Организационно-правовое сопровождение системы защиты АСУ на всех этапах проектирования и разработки. Технико-экономическое обоснование для внедрения системы защиты АСУ. Техническое сопровождение системы защиты на этапе ввода в эксплуатацию.

Тема 3. Обеспечение защиты информации в ходе эксплуатации АСУ, а также при выводе АСУ из эксплуатации.

Необходимые мероприятия по работе с АСУ и персоналом, обслуживающим АСУ. Комплексное обеспечение информационной безопасности информации, обрабатываемой в АСУ ТП посредством системы защиты. Разработка необходимой документации для вывода системы защиты АСУ из эксплуатации. Замещение мер по исполнению требований в сфере деятельности организации.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

Раздел 1. Автоматизированные системы управления технологическим процессом.

Тема 1. Промышленные протоколы. Особенности. Описание «типового» предприятия.

Лабораторная работа №1.1. Промышленные протоколы, особенности.

Лабораторная работа №1.2. Описание «типового» предприятия.

Тема 2. Проблематика защиты АСУ ТП; Классификация АСУ ТП

Лабораторная работа №2.1. Проблематика защиты АСУ ТП.

Лабораторная работа №2.2. Классификация АСУ ТП.

Тема 3. Знакомство с контроллерами, система центрального управления и их уязвимостями.

Лабораторная работа №3.1. Структура АСУ ТП.

Лабораторная работа №3.2. Устройство системы центрального управления, основные уязвимости.

Раздел 2. Нормативно-правовая база защиты информации в АСУ ТП.

Тема 1. Нормативные акты. Международные стандарты и практики. Концепции ИБ АСУ ТП.

Лабораторная работа №4.1. Национальные стандарты и практики в области обеспечения ИБ в АСУ ТП.

Лабораторная работа №4.2. Международные стандарты и практики в области обеспечения ИБ в АСУ ТП.

Тема 2. Формирование требований к защите информации в АСУ. Нормативное обеспечение системе защиты информации в АСУ ТП.

Лабораторная работа №5.1. Формирование требований к защите информации в АСУ.

Лабораторная работа №5.2. Нормативное обеспечение системе защиты информации в АСУ ТП.

Тема 3. Требования к мерам защиты информации в АСУ и их выбор.

Лабораторная работа №6.1. Определение набора требований к мерам защиты информации.

Лабораторная работа №6.2. Выбор мер защиты информации, соответствующих требованиям.

Раздел 3. Разработка системы защиты АСУ ТП.

Тема 1. Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.

Лабораторная работа №7.1. Общее представление о модели угроз и процессе моделирования.

Лабораторная работа №7.2. Создание модели угроз для «типового предприятия».

Тема 2. Внедрение системы защиты АСУ и ввод ее в действие.

Лабораторная работа №8.1. Разработка сопровождающей документации.

Лабораторная работа №8.2. Процедура ввода в эксплуатацию системы защиты АСУ ТП.

Тема 3. Обеспечение защиты информации в ходе эксплуатации АСУ, а также при выводе АСУ из эксплуатации.

Лабораторная работа №9.1. Обеспечение защиты информации в ходе эксплуатации АСУ.

Лабораторная работа №9.2. Обеспечение защиты информации при выводе АСУ из эксплуатации.

3.5 Тематика курсовых проектов (курсовых работ)

Не предусмотрены учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», текст: электронный, – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102439340, режим доступа: свободный.

2. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Национальный стандарт РФ: введен 01.01.2022: - М.: Стандартинформ, 2021.- URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=10&month=12&year=2021&search=&id=242006. - Текст: электронный.

3. ГОСТ Р ИСО/МЭК 27004-2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Национальный стандарт РФ: введен 30.11.2021: - М.: Стандартинформ, 2021.- URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=521&month=6&year=2008&search=&id=240761. - Текст: электронный.

4.2 Основная литература

1. Шельпяков, А. Н. Автоматизированное управление технологическими системами и процессами : учебное пособие / А. Н. Шельпяков. — Вологда : Инфра-Инженерия, 2022. — 160 с. — ISBN 978-5-9729-1094-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/281201 — Режим доступа: для авториз. пользователей.

2. Шишов, О. В. Современные средства АСУ ТП : учебник / О. В. Шишов. — Вологда : Инфра-Инженерия, 2021. — 532 с. — ISBN 978-5-9729-0622-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/192348 — Режим доступа: для авториз. пользователей.

3. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян. — Ростов-на-Дону : ЮФУ, 2020. — 140 с. — ISBN 978-5-9275-3546-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/170355. — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

1. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889. — Режим доступа: для авториз. пользователей.

2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.

3. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184. — Режим доступа: для авториз. пользователей.

4.4 Электронные образовательные ресурсы

Разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

В рамках обучения по дисциплине, дополнительное программное обеспечение не предусмотрено.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. КонсультантПлюс: справочная правовая система [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.consultant.ru/.
2. Гарант: информационно-правовой портал [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.garant.ru/
3. eLIBRARY.RU: научная электронная библиотека [Электронный ресурс]. – Режим доступа: свободный. URL: https://elibrary.ru/.
4. Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/ – Режим доступа: для авториз. пользователей.
5. Образовательная платформа «Юрайт» : [сайт]. – URL: https://urait.ru/ – Режим доступа: для авториз. пользователей.
6. Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprsmart.ru/ – Режим доступа: для авториз. пользователей.
7. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
8. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

5 Материально-техническое обеспечение

Лабораторные работы и самостоятельная работа студентов должны проводиться в специализированной аудитории, оснащенной современной оргтехникой и персональными компьютерами с программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов. Рабочее место преподавателя должно быть оснащено современным компьютером с подключенным к нему проектором на настенный экран, 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 является самостоятельная работа, а также посещение аудиторных занятий.

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. Оценивание результатов обучения по дисциплине осуществляется на основе балльно-рейтинговой системы (далее – БРС). Максимальный совокупный балл за академический период составляет 100.

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 проверке гипотез и задумок. Однако выполнять задания и оформлять отчетные материалы студент должен самостоятельно. Делиться отчетными материалами или создавать их совместно запрещено.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Приведенные ниже правила выставления оценок могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы обучающиеся регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения. Достижение компетенций оценивается с помощью лабораторных работ и рубежных контролей. По усмотрению преподавателя студенту могут начисляться дополнительные баллы за активную работу в семестре, участие в научных мероприятиях, нестандартные решения задач и другие достижения. Такие баллы суммируются с основной оценкой, но итоговый результат не может превышать 100 баллов.

После сдачи (загрузки в СДО) лабораторной работы студент должен ее защитить. Во время защиты лабораторной работы преподаватель проверяет содержание отчета, таблиц, исходного кода и других отчетных материалов, а также выполнение критериев и требований задания, а студент отвечает на вопросы преподавателя по предоставленным отчетным материалам, а также теоретическим вопросам, приведенных после текста задания лабораторной работы (при их наличии). 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, либо оценка будет снижена на усмотрение преподавателя.

За каждую лабораторную работу устанавливается максимально возможное количество рейтинговых баллов в соответствии с пунктом 7.2. При несвоевременной сдаче работы (позднее срока, установленного в календарно-тематическом плане) количество начисляемых баллов может быть снижено:

- при сдаче работы с опозданием до 3 календарных дней – максимально возможное количество баллов снижается на 10% (оценка за лабораторную работу выставляется с коэффициентом – 0.9);
- при сдаче работы с опозданием от 4 до 7 календарных дней – максимально возможное количество баллов снижается на 25% (оценка за лабораторную работу выставляется с коэффициентом – 0.75);
- при сдаче работы с опозданием свыше 7 календарных дней – начисляется не более 50% от максимально возможного количества баллов за задание (оценка за лабораторную работу выставляется с коэффициентом – 0.5).

В случае наличия уважительных причин для несвоевременной сдачи работы, студент должен обратиться к преподавателю. При возможности, студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей лабораторной работы или иного полученного задания.

Работа должна быть выполнена студентом самостоятельно: в отчетных материалах должны содержаться результаты работы только за его авторством, по отчетным материалам можно проследить как велась работа, студент может объяснить ход выполнения работы, если же обозначенное выше не соблюдается, то такая работа не считается сданной и не оценивается.

Рубежные контроли выполняются 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 другом занятии в семестре (в том числе и в рамках консультаций преподавателя), но обязательно очно.

7.2 Шкала и критерии оценивания результатов обучения

За посещение аудиторных занятий начисляется до 9 баллов (по 0,5 балла за каждое занятие при условии регулярного посещения). При пропуске занятий количество баллов уменьшается пропорционально количеству пропусков.

За выполнение лабораторных работ начисляется до 47 баллов, более конкретное распределение баллов за лабораторные работы представлено ниже:

Лабораторные работы №1.1–№5.2 – до 2 баллов.

Лабораторные работы №6.1, №7.1, №8.1, №9.1, №9.2 – до 3 баллов.

Лабораторные работы №6.2, №7.2, №8.2 – до 4 баллов.

За прохождение рубежного контроля начисляется до 8 баллов. За первый и второй рубежный контроль можно получить до 2 баллов, за третий рубежный контроль можно получить до 3 баллов.

Итого, по результатам текущего контроля, не считая дополнительных баллов, студент может получить до 64 баллов.

В свою очередь, по результатам промежуточной аттестации студент может получить до 36 баллов. Студенты, получившие оценку «неудовлетворительно» в ходе промежуточной аттестации, сохраняют ранее накопленную оценку за текущий контроль.

Итоговая оценка по дисциплине (модулю) определяется по следующим критериям:

- «неудовлетворительно» (2) – 0-54 баллов;
- «удовлетворительно» (3) – 55-69 баллов;
- «хорошо» (4) – 70-84 баллов;
- «отлично» (5) – 85-100 баллов.

7.3 Оценочные средства

7.3.1 Текущий контроль

Оценочными средствами текущего контроля являются лабораторные работы, выложенные в курсе СДО по данной дисциплине (модулю), а также прохождение рубежных контролей.

7.3.2 Промежуточная аттестация

Формой оценки знаний в рамках промежуточной аттестации является: ***экзамен***.

В ходе промежуточной аттестации студенту выдается билет, содержащий 3 вопроса. За ответ на каждый вопрос студент может получить до 12 баллов. Билет формируется из перечня вопросов, расположенного ниже:

1. Автоматизированные системы управления технологическими процессами;
2. Промышленные протоколы. Особенности.
3. Описание «типового» предприятия;
4. Проблематика защиты АСУТП;
5. Знакомство с контроллерами, система центрального управления и их уязвимостями
6. Нормативные акты. Международные стандарты и практики.
7. Концепции ИБ АСУ ТП.
8. Формирование требований к защите информации в АСУ.
9. Нормативное обеспечение системе защиты информации в АСУ ТП.
10. Разработка системы защиты АСУ.
11. Внедрение системы защиты АСУ и ввод ее в действие.
12. Обеспечение защиты информации в ходе эксплуатации АСУ.
13. Обеспечение защиты информации при выводе из эксплуатации АСУ.
14. Требования к мерам защиты информации в АСУ и их выбор
15. Классификация АСУ ТП.
16. Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.
17. Разбор вариантов выбора требований и средств защиты информации в соответствии с моделью угроз.
18. Промышленные межсетевые экраны.
19. Система (двухфакторной/многофакторной) аутентификации
20. Системы контроля и мониторинга действий пользователей.
21. Система мониторинга и управления политиками межсетевых экранов.
22. Система анализа защищённости.
23. Система быстрого восстановления конфигураций и данных промышленных систем.
24. Объект информатизации (определение). Основные технические средства и системы (ОТСС).
25. Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации.

26. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).

27. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.

28. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.

29. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.

30. Методы обнаружения, идентификации радиозакладных устройств и определения их местоположения.

31. Порядок организации защиты информации на объектах информатизации.

32. Предварительное специальное обследование объекта информатизации.

Пример экзаменационного билета

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_
по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ»

Направление подготовки
10.05.03 Информационная безопасность автоматизированных систем

ВОПРОСЫ:

1. Разбор вариантов выбора требований и средств защиты информации в соответствии с моделью угроз.
2. Система анализа защищённости.
3. Формирование требований к защите информации в АСУ.

Утверждено: _____ / _____ / «__» _____ 20__г.