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
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в автоматизированных системах управления технологическими процессами»

Направление подготовки
10.03.01 «Информационная безопасность»
Профиль
«Безопасность компьютерных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2024 г.

Разработчик(и):

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

Согласовано:
Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** дисциплины «Защита информации в автоматизированных системах управления технологическим процессом» 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** дисциплины «Защита информации в автоматизированных системах управления технологическим процессом» относится:

- 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 технологическим процессом» 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 безопасности для

	обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.
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 числу элективных дисциплин (Б1.2) основной образовательной программы (Б1.2.03).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Проектирование организационно-распорядительных документов по обеспечению информационной безопасности», «Стандартизация и сертификация в информационной безопасности», «Защищенные информационные системы», «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часов).

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			7
1	**Аудиторные занятия**	**72**	**7**
	В том числе:		**7**
1.1	Лекции	4	**7**
1.2	Семинарские/практические занятия	-	**7**
1.3	Лабораторные занятия	68	**7**
2	**Самостоятельная работа**	**72**	**7**
3	**Промежуточная аттестация**		**7**
	Экзамен		**7**
	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. Автоматизированные системы управления технологическим процессом.						
1.1	Тема 1. Промышленные протоколы. Особенности. Описание «типового» предприятия.	**18**	2	-	8	-	8
1.2	Тема 2. Проблематика защиты АСУ ТП; Классификация АСУ ТП.	**16**	-		8	-	8
1.3	Тема 3. Знакомство с контроллерами, система центрального управления и их уязвимостями	**16**	-	-	8	-	8
2	Раздел 2. Нормативно-правовая база защиты информации в АСУ ТП						
2.1	Тема 1. Нормативные акты. Международные стандарты и практики. Концепции ИБ АСУ ТП.	**14**	2		4	-	8

2.2	Тема 2. Формирование требований к защите информации в АСУ. Нормативное обеспечение системе защиты информации в АСУ ТП	**16**	-	-	8	-	8
2.3	Тема 3. Требования к мерам защиты информации в АСУ и их выбор	**16**	-	-	8	-	8
3	Раздел 3. Разработка системы защиты АСУ ТП.						
3.1	Тема 1. Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.	**16**	-	-	8	-	8
3.2	Тема 2. Внедрение системы защиты АСУ и ввод ее в действие.	**16**	-	-	8	-	8
3.3	Тема 3. Обеспечение защиты информации в ходе эксплуатации АСУ, а также при выводе АСУ из эксплуатации.	**16**	-	-	8	-	8
Итого		**144**	**4**		**68**		**72**

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 занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные работы

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)

Курсовое проектирование по дисциплине «Защита информации в автоматизированных системах управления технологическим процессом» не предусмотрено 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 материалы

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого, допускается использование студентом собственной вычислительной техники (ноутбук).

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно телекоммуникационной сети «Интернет». Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по

вопросам выполнения практических заданий. В процессе самостоятельной работы студентов предусмотрена возможность получения индивидуальных консультаций преподавателя с использованием электронной почты в сети Интернет.

Методические рекомендации

5.1 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.

3. При организации и проведения экзаменов в практико-ориентированной форме следует использовать утвержденные кафедрой Методические рекомендации.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.04.01 «Информационная безопасность»**

5.2 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 лабораторные занятия.

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

Самостоятельная работа включает изучение теоретических и практических разделов дисциплины.

Общие рекомендации по организации самостоятельной работы:

Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятий, другая –внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

Чтобы выполнить весь объем самостоятельной работы, необходимо заниматься по 1 – 4 часа ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра. Первые дни семестра очень важны для того, чтобы включиться в работу, установить определенный порядок, равномерный ритм на весь семестр. Ритм в работе –это ежедневные самостоятельные занятия, желательно в одни и те же часы, при целесообразном чередовании занятий с перерывами для отдыха.

Начиная работу, не нужно стремиться делать вначале самую тяжелую ее часть, надо выбрать что-нибудь среднее по трудности, затем перейти к более трудной работе. И напоследок оставить легкую часть, требующую не столько больших интеллектуальных усилий, сколько определенных моторных действий (черчение, построение графиков и т.п.).

Следует правильно организовать свои занятия по времени: 50 минут –работа, 5-10 минут –перерыв; после 3 часов работы перерыв –20-25 минут. Иначе нарастающее

утомление повлечет неустойчивость внимания. Очень существенным фактором, влияющим на повышение умственной работоспособности, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность.

Методические указания к отдельным видам деятельности:

Лекция: Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулировки, выводы. Помечать важные мысли. Выделять ключевые слова, термины. Делать пометки на вопросах, терминах, блоках в тексте, которые вызвали затруднения, после чего постараться найти ответ в рекомендуемой литературе. Если ответ не найден, то на консультации обратиться к преподавателю.

Лабораторная работа: Работа с конспектом лекций и методическими указаниями по выполнению лабораторной работы, просмотр рекомендуемой литературы, конспектирование основных мыслей и выводов, разработка плана выполнения лабораторной работы, предварительная формулировка возможных выводов по работе. Подготовка к практическим занятиям, проработка материала по вопросам, выносимым на практические занятия. Для более углублённого изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темой.

6 Фонд оценочных средств

6.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- экзамен.

6.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ПК-3. Способен проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: отечественные и международные стандарты информационной безопасности; основные принципы организации технического, программного и информационного	Обучающийся не знает или в недостаточной степени знает отечественные и международные стандарты информационной безопасности; основные принципы организации	Обучающийся демонстрирует частичное знание отечественных и международных стандартов информационной безопасности; основных принципов организации технического,	Обучающийся демонстрирует полное знание отечественных и международных стандартов информационной безопасности; основных принципов организации	Обучающийся демонстрирует полное знание отечественных и международных стандартов информационной безопасности; основных принципов

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.	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.	программного и информационного обеспечения защищенных информационных систем; основных методов и средств обеспечения безопасности операционных систем; основных методов и средств обеспечения сетевой безопасности; основных методов и средств обеспечения безопасности в системах управления базами данных. . Допускаются значительные ошибки	технического, программного и информационного обеспечения защищенных информационных систем; основных методов и средств обеспечения безопасности операционных систем; основных методов и средств обеспечения сетевой безопасности; основных методов и средств обеспечения безопасности в системах управления базами данных. . Допускаются незначительные ошибки, неточности	организации технического, программного и информационного обеспечения защищенных информационных систем; основных методов и средств обеспечения безопасности операционных систем; основных методов и средств обеспечения сетевой безопасности; основных методов и средств обеспечения безопасности в системах управления базами данных. . Допускаются незначительные неточности
уметь: обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта защиты; осуществлять выбор	Обучающийся не умеет или в недостаточной степени умеет обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	Обучающийся демонстрирует частичное умение обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности	Обучающийся демонстрирует полное умение обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности объекта	Обучающийся демонстрирует полное умение обосновывать принципы организации технического, программного и информационного обеспечения информационн

функциональной структуры системы обеспечения информационной безопасности.	объекта защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности.	объекта защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. . Допускаются значительные ошибки	защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. . Допускаются незначительные ошибки, неточности	ой безопасности объекта защиты; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности. . Допускаются незначительные неточности
владеть: навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.	Обучающийся не владеет или в недостаточной степени владеет навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.	Обучающийся демонстрирует частичное владение навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем. . Допускаются значительные	Обучающийся демонстрирует полное владение навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем защиты основных операционных систем.	Обучающийся демонстрирует полное владение навыками применения отечественных и международных стандартов информационной безопасности для обоснования состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты; навыками настройки подсистем

		ошибки	. Допускаются незначительные ошибки, неточности	защиты основных операционных систем. . Допускаются незначительные неточности
ПК-15. Способен организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.				
знать: методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности.	Обучающийся не знает или в недостаточной степени знает методы ввода в эксплуатацию систем и средства обеспечения информационной безопасности.	Обучающийся демонстрирует частичное знание методов ввода в эксплуатацию систем и средства обеспечения информационной безопасности. . Допускаются значительные ошибки	Обучающийся демонстрирует полное знание методов ввода в эксплуатацию систем и средства обеспечения информационной безопасности. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное знание методов ввода в эксплуатацию систем и средства обеспечения информационной безопасности. . Допускаются незначительные неточности
уметь: организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	Обучающийся не умеет или в недостаточной степени умеет организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.	Обучающийся демонстрирует частичное умение организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. . Допускаются значительные ошибки	Обучающийся демонстрирует полное умение организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. . Допускаются незначительные неточности

владеть: методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.	Обучающийся не владеет или в недостаточной степени владеет методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.	Обучающийся демонстрирует частичное владение методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. . Допускаются значительные ошибки	Обучающийся демонстрирует полное владение методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное владение методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности. . Допускаются незначительные неточности

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.

Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

6.3 Оценочные средства

7.3.1 Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ.

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена

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 билета.

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

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ»

Направление подготовки
10.03.01 Информационная безопасность

ВОПРОСЫ:

1. Система анализа защищённости.
2. Описание «типового» предприятия.
3. Объект информатизации (определение). Основные технические средства и системы (ОТСС).

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