МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО

Декан факультета

Информационных технологий

_____ / А.Ю. Филиппович /

«_28_» __мая_____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в автоматизированных системах управления технологическими процессами»

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)

«Обеспечение информационной безопасности

распределенных информационных систем»

Квалификация (степень) выпускника

Специалист по защите информации

Форма обучения

Очная

Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины

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

- теоретическую и практическую подготовленность специалиста к организации и поддержании выполнения комплекса мер по 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.

2. Место дисциплины в структуре ООП

Дисциплина «Защита информации в автоматизированных системах управления технологическими процессами» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1) основной образовательной программы (Б.1.54).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Математический анализ», «Теория вероятностей» и «Математическая статистика», «Электроника и схемотехника», «Основы информационной безопасности», «Физические основы информационной безопасности».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее	**знать:** • особенности и способы применения программных и программно-аппаратные средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

	реализации	• типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; • основные понятия криптографии и типовых криптографических методов и средств защиты информации; **уметь:** • устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; • проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; • осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. владеть: • иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе; • иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; • иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лекции – 36 часов, лабораторные занятия – 36 час, самостоятельная работа - 72 часа, форма контроля – экзамен) в 9 семестре.

Структура и содержание дисциплины «Защита информации в автоматизированных системах управления технологическими процессами» по срокам и видам работы отражены в приложении.

5. Образовательные технологии

Методика преподавания дисциплины «Защита информации в автоматизированных системах управления технологическими процессами» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся:

- выполнение лабораторных работ в лабораториях вуза;

- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы;
- посещение профильных конференций и работа на мастер-классах экспертов и специалистов индустрии;

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к текущей аттестации;
- подготовки к промежуточной аттестации.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

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

- экзамен.

Образцы вопросов к экзамену приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-14 Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ЗНАТЬ	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.
УМЕТЬ	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

ВЛАДЕТЬ	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации*: экзамен.*

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. 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.

Фонды оценочных средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

1. Основная литература:

- Юсупов, Р.Х. Основы автоматизированных систем управления технологическими процессами : учебное пособие / Р.Х. Юсупов. – Москва ; Вологда : Инфра-Инженерия, 2018. – 133 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=493900 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-9729-0229-3. – Текст : электронный.
- Мякишев, Д.В. Разработка программного обеспечения АСУ ТП на основе объектно-ориентированного подхода: теория, модели, методы : методическое пособие : [16+] / Д.В. Мякишев. – Москва ; Вологда : Инфра-Инженерия, 2019. – 129 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=564227 (дата обращения: 19.08.2019). – Библиогр.: с. 100. – ISBN 978-5-9729-0305-4.

2. Дополнительная литература:

- Глазырин, М.В. Автоматизированные системы управления тепловыми электростанциями : учебное пособие : в 2-х ч. / М.В. Глазырин ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2011. – Ч. I. Основы функционирования АСУ ТП ТЭС. – 42 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=228766 (дата обращения: 19.08.2019). – ISBN 978-5-7782-1704-1. – Текст : электронный.

8. Материально-техническое обеспечение дисциплины

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.

Оборудование и аппаратура:

1. Офисные приложения, MicrosoftOffice.
2. Операционная система Windows.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

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

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: доц. Кесель С.А.

Программа утверждена на заседании кафедры “Информационная безопасность” «28» мая 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

Структура и содержание дисциплины «Защита информации в автоматизированных системах управления технологическими процессами»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	9 семестр														
1	Введение. Автоматизированные системы управления технологическими процессами;	9	1	2		2	4								
2	Промышленные протоколы. Особенности. Описание «типового» предприятия;		2	2		2	4								
3	Проблематика защиты АСУТП;		3	2		2	4								
4	Знакомство с контроллерами, система центрального управления и их уязвимостями		4	2		2	4								
5	Нормативные акты. Международные стандарты и практики. Концепции ИБ АСУ ТП.		5	2		2	4								
6	Формирование требований к защите информации в АСУ. Нормативное обеспечение системе защиты информации в АСУ ТП.		6	2		2	4								

7	Разработка системы защиты АСУ.		7	2		2	4								
8	Внедрение системы защиты АСУ и ввод ее в действие.		8	2		2	4								
9	Обеспечение защиты информации в ходе эксплуатации АСУ.		9	2		2	4								
10	Обеспечение защиты информации при выводе из эксплуатации АСУ.		10	2		2	4								
11	Требования к мерам защиты информации в АСУ и их выбор		11	2		2	4								
12	Классификация АСУ ТП.		12	2		2	4								
13	Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.		13	2		2	4								
14	Разбор вариантов выбора требований и средств защиты информации в соответствии с моделью угроз.		14	2		2	4								
15	Промышленные межсетевые экраны.		15	2		2	4								
16	Система быстрого восстановления конфигураций и данных промышленных систем.		16	2		2	4								
17	Система анализа защищённости.		17	2		2	4								
18	Система мониторинга и управления политиками межсетевых экранов.		18	2		2	4								
	Форма аттестации	9	19-21							.				Э	
	Всего часов по дисциплине во девятом семестре			36		36	72								
	Всего часов по дисциплине			36		36	72								

Приложение к
рабочей программе

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

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем» ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Защита информации в автоматизированных системах управления технологическими процессами»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
список вопросов к зачету.

Составители: доц. Кесель С.А.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Защита информации в автоматизированных системах управления технологическими процессами					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**знать:** • особенности и способы применения программных и программно-аппаратные средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; • типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; • основные понятия криптографии и типовых криптографических методов и средств защиты информации; **уметь:** • устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; • проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; • осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. владеть: • иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе; • иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; • иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе	самостоятельная работа, лабораторные занятия	зачет	**Базовый уровень:** **знать:** особенности и способы применения программных и программно-аппаратные средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **уметь:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **владеть:** иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе; **Повышенный уровень:** иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Список вопросов к зачету по дисциплине

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. Концепции ИБ АСУ ТП.
7. Формирование требований к защите информации в АСУ. Нормативное обеспечение системе защиты информации в АСУ ТП.
8. Разработка системы защиты АСУ.
9. Внедрение системы защиты АСУ и ввод ее в действие.
10. Обеспечение защиты информации в ходе эксплуатации АСУ.
11. Обеспечение защиты информации при выводе из эксплуатации АСУ.
12. Требования к мерам защиты информации в АСУ и их выбор
13. Классификация АСУ ТП.
14. Моделирование угроз безопасности информации. Пример модели угроз безопасности АСУ ТП.
15. Разбор вариантов выбора требований и средств защиты информации в соответствии с моделью угроз.
16. Промышленные межсетевые экраны.
17. Система (двухфакторной/многофакторной) аутентификации
18. Системы контроля и мониторинга действий пользователей.
19. Система мониторинга и управления политиками межсетевых экранов.
20. Система анализа защищённости.
21. Система быстрого восстановления конфигураций и данных промышленных систем.
22. Объект информатизации (определение). Основные технические средства и системы (ОТСС).
23. Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации.
24. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
25. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.
26. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.
27. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.
28. Методы обнаружения, идентификации радиозакладных устройств и определения их местоположения.
29. Порядок организации защиты информации на объектах информатизации.
30. Предварительное специальное обследование объекта информатизации.

31. Аналитическое обоснование необходимости создания СТЗИ объекта (содержание, порядок проведения).
32. Замысел создания СТЗИ. Техническое задание на разработку СТЗИ объекта информатизации.
33. Организация аттестации объекта информатизации по требованиям безопасности информации.
34. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.
35. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.
36. Заключение по результатам аттестационной проверки объекта информатизации.
37. Аттестат соответствия объекта информатизации требованиям безопасности информации.