Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
ОТДЕЛЕНИЕ ПРИКЛАДНОЙ ИНФОРМАТИКИ

кафедра Системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры Системного анализа и информатики

Протокол №6 от «2» сентября 2019г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.09 ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

направление подготовки
09.03.03 Прикладная информатика
направленность (профиль)
«Прикладная информатика в информационной безопасности»
квалификация
бакалавр
очная форма обучения

Год набора – 2020

Москва, 2020г.

Автор–составитель: к.т.н.
преподаватель кафедры Системного анализа и информатики Каширская Е.Н.

Заведующий кафедрой
Системного анализа и информатики Маруев С.А.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Технология построения защищенных автоматизированных систем» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-2	способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение	ПК-2.2	Способен выбирать и использовать языки программирования для разработки кода ИС и БД ИС
ПК-5	способен выполнять технико-экономическое обоснование проектных решений	ПК-5.3	Способен оценивать влияние вносимых заказчиком предложений по доработке ИС на сроки, стоимость и содержание работ

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
	ПК-2.2	на уровне знаний: • знать основы алгоритмизации и языки программирования;
		на уровне умений: уметь разрабатывать код ИС и БД ИС с использованием языков программирования;
		на уровне навыков: иметь навык разработки, внедрения и настройки прикладного ПО.
	ПК-5.3	на уровне знаний: знать современные проектные решения для математического и программного обеспечения информационных систем;
		на уровне умений: уметь выбирать с обоснованием проектные решения для конкретной информационной системы под нужную предметную область с учётом технических, технологических и экономических показателей;
		на уровне навыков: иметь навык анализа проектных решений для широкого спектра информационных систем;

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах– 3 ЗЕ (108/81ч).
Количество академических/астрономических часов, выделенных на контактную работу по очной форме обучения – 32/24 часа (в т.ч. лекц.-16 ч., практ.-16 ч.); на самостоятельную работу обучающихся на очной форме – 40/30 часов.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.09 «Технология построения защищенных автоматизированных систем» относится к обязательным дисциплинам вариативной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.

Дисциплина изучается на 4 курсе в 8 семестре (очная форма)

Дисциплины опирается на объём знаний области информатики, вычислительных систем, теории систем и системного анализа, баз данных, операционных систем, проектирования интерфейсов.

Форма промежуточной аттестации – экзамен

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Введение. Проблемы защиты информации в АС	4	1		1		2	О
Тема 2	Защита информации на технологическом уровне	9	2		2		5	О
Тема 3	Применение защищенных виртуальных сетей	9	2		2		5	О
Тема 4	Межсетевые экраны	6	1		1		4	О
Тема 5	Технология обнаружения вторжений	5	1		1		3	О
Тема 6	Централизованное управление средствами безопасности	9	2		2		5	О
Тема 7	Централизованное управление средствами безопасности	10	2		2		6	О
Тема 8	Защита от вирусов	5	1		1		3	О
Тема 9	Политики безопасности и профили защиты	11	3		3		5	О
Тема 10	Анализ безопасности функционирования АС. Заключение	4	1		1		2	О
Промежуточная аттестация		36						экзамен
Всего академ./астроном.часов:		**108/81**	**16/12**		**16/12**		**40/30**	**36/27**

Примечание* – формы текущего контроля успеваемости: опрос (О), тестирование (Т).

Содержание дисциплины

№ п/п	Название темы	Основные вопросы и положения, раскрывающие содержание темы
Тема 1.	*Введение. Проблемы защиты информации в АС*	Предмет, задачи и содержание дисциплины. Цели и задачи проектирования АС в защищенном исполнении. Вопросы экономичности и эффективности. Рекомендуемая литература. Угрозы информационной безопасности (ИБ): классификация, виды, происхождение и предпосылки появления угроз. Источники угроз. Оценка угроз. Обоснование структуры и содержания системы показателей, необходимых для исследования и практического решения всех задач, связанных с защитой информации. Обоснование структуры и содержания тех параметров, которые оказывают существенное влияние на значения показателей уязвимости информации.
Тема 2	*Защита информации на технологическом уровне*	Задачи и механизмы защиты информации на технологическом уровне. Идентификация, аутентификация и авторизация. Программные средства защиты информации (ЗИ). Технология многоуровневого шифрования для защиты рабочих станций и компьютерных сетей.: требования к криптографическим механизмам по производительности, размеру кода, доступа к зашифрованной информации. Функциональная схема комплексной программной системы компьютерной безопасности. Защита информации на различных уровнях 7-уровневой модели взаимодействия открытых систем ISO. Обеспечение целостности обрабатываемой информации.
Тема 3	Применение защищенных виртуальных сетей	Вопросы включения телекоммуникационные системы общего для объединения локальных вычислительных сетей. Виртуальные частные сети VPN (Virtual Private Networks). Применение криптографических механизмов ЗИ, аутентификации информации и контроля целостности информации. Стандарты Internet IPSec (IP Security). Универсальность и гибкость стандартов IPSec. Использование цифровых сертификатов и структуры открытых ключей PKI (Public Key Infrastructure). Использование средств VPN для поддержания защищенных каналов трех основных типов: с удаленными сотрудниками (защищенный удаленный доступ); с сетями филиалов предприятий (защита intranet); с сетями предприятий-партнеров (защита extranet). Клиентские части VPN для основных клиетских операционных систем. Использование гибридных криптосистем.
Тема 4	*Межсетевые экраны*	Применение межсетевых экранов (МЭ) для реализации простых схем доступа. Контроль доступа в одной точке

		на пути соединений внутренней сети с Internet или другой публичной сетью, являющейся источником потенциальных угроз. Контроль доступа с разделением все субъектов доступа на группы по IP-адресам, явно указанным в пакете. Контроль доступа внешних пользователей к внутренним ресурсам сети при использовании ограниченного числа сервисов Internet и отсечением трафика остальных сервисов. Применение МЭ в случае нескольких точек контроля доступа. Контроль доступа к нескольким внешним сетям (к публичной части Internet и IP-сети провайдера). Использование несколько связей с Internet через разных провайдеров (для повышения надежности). Повышение требований к защите обрабатываемой информации внутри сети и использование межсетевых экранов между внутренними подсетями. Координация работы МЭ на основе единой политики доступа. Обеспечение корректной обработки пакетов при их прохождении через несколько точек доступа распределенные межсетевые экраны. Агенты выполняющие функции МЭ. Контроль многоагентных МЭ из единого центра безопасности.
Тема 5	*Технология обнаружения вторжений*	Угрозы, атаки и вторжения. Средства обнаружения вторжений (СОВ) как механизм повышения уровня защищенности АС. Факторы обусловливающие актуальность применения средств обнаружения вторжений и внесения изменений в соответствующие настройки подсистемы информационной безопасности. Средства обнаружения вторжений как механизм дополнения защитных функций межсетевых экранов. Межсетевые экраны – механизм отсечения потенциально опасного трафика. Направленность средств обнаружения вторжений на анализ результирующего трафика. Использование СОВ в незащищенных сегментах АС. Использование экспертных системы и других элементов искусственного интеллекта в СОВ. Основные задачи и функции СОВ.
Тема 6	*Централизованное управление средствами безопасности*	Наличие средств централизованного управления средствами ИБ как важнейшее требование построения защищенных АС. Преимущества централизованного управления средствами ИБ. Единство политики безопасности предприятия. Правила функционирования для всех средств защиты информации в защищенной АС. Согласованное задание правила политик безопасности для различных устройств защиты. Использование администратором общей консоли управления для обеспечения непротиворечивость и эффективности политик безопасности. Взаимодействие индивидуальных устройств защиты, используемых в АС, с централизованной системой

		управления. Защищенная передача правил безопасности индивидуальным устройствам. Протоколы распределения правил безопасности по устройствам защиты.
Тема 7	*Управление доступом на уровне пользователей*	Категории пользователей, отличающиеся правами доступа. Принцип дифференцированного распознавания. Сотрудники предприятия, работающие во внутренней сети. Удаленные и мобильные сотрудники предприятия. Сотрудники предприятий-партнеров по бизнесу. Клиенты предприятия, получающие услуги по Internet. Проблемы классифицирования по IP-адресам пользователей. Контроль доступа на уровне пользователей с использованием в межсетевых экранах собственных средств работы с учетной информацией пользователей и средств аутентификации. Интеграция средств контроля доступа с применяемыми в ИС механизмами администрирования и аутентификации пользователей. Управление доступом на уровне пользователей как способ повышения эффективности аудита событий, связанных с безопасностью. Гарантированная аутентификация пользователей. Обеспечение единого логического входа пользователя в сеть. Использование электронных токенов (смарт-карт, устройств touch-memory, ключей для USB-портов) в качестве идентификаторов.
Тема 8	*Защита от вирусов*	Типы вредоносных программ. Компьютерные вирусы – серьезная угроза ИБ. Типы вредоносных воздействий вирусов на АС. Жизненный цикл вирусов. Антивирусная защита как один из важнейших компонентов комплексной системы ИБ. Используется комплексов антивирусной защиты. Современные антивирусные программы. Принципы распознавания вирусов. Сигнатуры и эвристический анализ. Динамический и статический режимы антивирусной защиты. Влияние выбора операционной системы на устойчивость и подверженность к вирусным атакам.
Тема 9	*Политики безопасности и профили защиты*	Понятие политики безопасности. Подходы к организации защиты информации и формирование политики безопасности. Комплексный подход как создание защищенной среды обработки информации в АС. Политика безопасности и архитектура системы защиты. Реализация комплексного применения административно-организационных мер, физических мер и программно-аппаратных средств. Влияние на политику безопасности способа управления доступом, определяющего порядок доступа к объектам АС. Основные виды политик безопасности: избирательная и полномочная. Избирательная политика безопасности как способ избирательного управления доступом.

		Избирательное (или дискреционное) управление доступом как задание администратором множеством разрешенных отношений доступа. Математическая модель правил доступа в виде матрицы доступа. Полномочная политика безопасности. Полномочное (мандатное) управление доступом как совокупность правил предоставления доступа, базирующихся на множестве атрибутов безопасности объектов и субъектов. Метки конфиденциальности информации и уровня допуска пользователя. Принцип рационального сочетания избирательного и полномочного управления доступом.
Тема 10	*Анализ безопасности функционирования АС. Заключение*	Экспертный анализ. Анализ стойкости криптографических протоколов. Безопасность криптографических механизмов. Экспертный анализ. Проверка соответствия нормативным требованиям безопасности к ИС в защищенном исполнении. Экспертный и формальный анализ защищенности. Средства автоматизированного анализа уязвимостей. Сканеры уязвимости. Анализ недекларированных возможностей системных и прикладных программ. Экспертные и интеллектуальные средства анализа безопасности. Многоагентные сканеры безопасности. Роль элементной базы в построении защищенных ИС. Перспективы расширения областей применения защищенных информационных систем. Системы тайного голосования через интернет. Задача обеспечения анонимности. Роль стандартизации в области ИБ.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости.

4.1.1. В ходе реализации дисциплины «Технология построения защищенных автоматизированных систем» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Опрос
Тема 2	Опрос
Тема 3	Опрос
Тема 4	Опрос
Тема 5	Опрос
Тема 6	Опрос
Тема 7	Опрос
Тема 8	Опрос
Тема 9	Опрос
Тема 10	Опрос

4.1.2. Экзамен проводится в форме устного ответа на билеты (по 2 вопроса в билете, 1 вопрос теоретический, 2 вопрос практический).

4.2. Материалы текущего контроля успеваемости обучающихся

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется при опросе на практических занятиях. Проведение контрольных работ в соответствии с п.4.1.1

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-2	способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение	ПК-2.2	Способен выбирать и использовать языки программирования для разработки кода ИС и БД ИС
ПК-5	способен выполнять технико-экономическое обоснование проектных решений	ПК-5.3	Способен оценивать влияние вносимых заказчиком предложений по доработке ИС на сроки, стоимость и содержание работ

4.3.2. Типовые оценочные средства

Промежуточный контроль проводится в форме устного опроса и заключительного теста по всем темам, устный ответ на вопросы по каждому изученному разделу в соответствии с п. 4.2

Код и наименование этапа освоения компетенции	Результаты обучения	Оценочное средство
ПК-2.2 Способен выбирать и использовать языки программирования для разработки кода ИС и БД ИС	на уровне знаний: знать основы алгоритмизации и языки программирования;	устный опрос
	на уровне умений: уметь разрабатывать код ИС и БД ИС с использованием языков программирования;	устный опрос
	на уровне навыков: иметь навык разработки, внедрения и настройки прикладного ПО.	устный опрос
ПК-5.3 Способен оценивать влияние вносимых	на уровне знаний: знать современные проектные решения для математического и программного обеспечения информационных	устный опрос

заказчиком предложений по доработке ИС на сроки, стоимость и содержание работ	систем;	
	на уровне умений: уметь выбирать с обоснованием проектные решения для конкретной информационной системы под нужную предметную область с учётом технических, технологических и экономических показателей;	устный опрос
	на уровне навыков: иметь навык анализа проектных решений для широкого спектра информационных систем;	устный опрос

Перечень вопросов к экзамену:

1. Классификация угроз ИБ.
2. Источники угроз.
3. Оценка угроз.
4. Показатели уязвимости информации.
5. Критерии и показатели защищенности объекта.
6. Механизмы защиты информации.
7. Программные средства ЗИ и их характеристика.
8. Криптографические механизмы шифрования информации.
9. Схема комплексной программной системы компьютерной безопасности.
10. Состав 7-уровневой модели взаимодействия открытых систем ISO.
11. Способы обеспечения целостности обрабатываемой информации в защищенных АС.
12. Частные сети VPN, способы их построения.
13. Порядок применения стандартов Internet IPSec.
14. Порядок использования цифровых сертификатов и структуры открытых ключей PKI.
15. Использование средств VPN.
16. Клиентские части VPN, их применение.
17. Понятие МЭ, порядок их применения.
18. Контроль доступа внешних пользователей к внутренним ресурсам сети.
19. Порядок применения МЭ в случае нескольких точек контроля доступа.
20. Использование связей с Internet через разных провайдеров.
21. Распределенные межсетевые экраны.
22. Средства обнаружения вторжений.
23. Применение МЭ, как механизма отсечения потенциально опасного трафика.
24. Анализ результирующего трафика на основе применения средств обнаружения вторжений.
25. Порядок использования СОВ в незащищенных сегментах АС.
26. Порядок использования экспертных систем и других элементов искусственного интеллекта в СОВ.
27. Централизованное управление средствами ИБ, положительные и отрицательные стороны.

28. Политика безопасности, структура и состав.
29. Порядок разработки согласованного задания правила политик безопасности для различных устройств защиты.
30. Функции администратора при работе с общей консолью управления для обеспечения непротиворечивости и эффективности политик безопасности.
31. Протоколы распределения правил безопасности по устройствам защиты.
32. Категории пользователей по допуску.
33. Организация работы с удаленными и мобильными сотрудниками предприятия.
34. Управление доступом на уровне пользователей.
35. Обеспечение гарантированной аутентификации пользователей.
36. Порядок использования электронных токенов.
37. Вирусы, определение, классификация.
38. Жизненный цикл вирусов.
39. Антивирусная защита как один из важнейших компонентов комплексной системы ИБ.
40. Порядок использования комплексов антивирусной защиты.
41. Выбор операционной системы.
42. Понятие политики безопасности, задачи, цели и порядок разработки.
43. Политика безопасности и архитектура системы защиты.
44. Основные виды политик безопасности, их характеристики.
45. Полномочная политика безопасности.
46. Метки конфиденциальности информации и уровня допуска пользователя, порядок разработки матрицы допуска.
47. Понятие экспертного анализа ИБ.
48. Проверка соответствия нормативным требованиям безопасности к ИС в защищенном исполнении.
49. Средства автоматизированного анализа уязвимостей.
50. Экспертные и интеллектуальные средства анализа безопасности.
51. Элементная база защищенных ИС.

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание лекционного материала

Критериями оценки ответа обучающихся на лекционном занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки **"отлично"** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки **"хорошо"** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **"удовлетворительно"** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **"неудовлетворительно"** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3. Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине

Экзамен принимается в устной форме, по билетам. Экзаменационный билет включает два теоретических вопроса и один практический. Оценка знаний обучающегося на экзамене носит комплексный характер и определяется его:

- ответом на экзамене;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на экзамене оцениваются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

Оценивание студента на экзамене по дисциплине «Технология построения защищенных автоматизированных систем»

Оценка	Требования к знаниям
Отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает на экзамене, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение. Учебные достижения в семестровый период демонстрируют высокую степень овладения программным материалом.
Хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает

	материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Учебные достижения в семестровый период демонстрируют хорошую степень овладения программным материалом.
Удовлетво-рительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Учебные достижения в семестровый период демонстрируют достаточную (удовлетворительную) степень овладения программным материалом.
Неудовлет-ворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. Учебные достижения в семестровый период не демонстрировали достаточную степень овладения программным материалом на пороговом уровне.

5. Методические указания для обучающихся по освоению дисциплины

5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на семинарском занятии. В случае необходимости обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки

к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

– использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;

– представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;

– грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.2.1. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий или лабораторных работ, для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

5.3. Методические рекомендации по подготовке к экзамену по дисциплине

Ответ на экзамене предусматривает устный ответ на теоретические вопросы и решение практической задачи.

При подготовке к экзамену обучающийся обращается к пройденному материалу, сосредоточенному в конспектах лекций, учебниках и других источниках информации. Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно-новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено в лекциях и на семинарских занятиях.

Экзамен как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

• что и как запоминать при подготовке к экзамену;
• по каким источникам и как готовиться;
• на чем сосредоточить основное внимание;
• каким образом в максимальной степени использовать программу курса;
• что и как записать, а что выучить дословно и т. п.

На экзамене, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными научными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом экзамене. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для экзамена.

Оптимальным для подготовки к экзамену является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к экзамену по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к экзамену следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, иллюстрированные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает.

В то же время подготовка по одним конспектам лекций недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и уточняющих вопросов на экзамене. Они, как правило, задаются или помимо экзаменационного вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Карпов В.В. Технология построения защищенных автоматизированных систем [Электронный ресурс] : учебное пособие / В.В. Карпов, В.А. Мельник. — Электрон. текстовые данные. — М. : Российский новый университет, 2009. — 232 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/21326..html

2. Информационная безопасность. Учебник и практикум для академического бакалавриата.: М. Юрайт, 2017 – 321с. Электронный ресурс: https://biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1

6.2. Дополнительная литература.

1. Барабаш П.А., Воробьев С.П., Курносов В.И., Советов Б.Я. Инфокоммуникационные технологии в глобальной информационной инфраструктуре /Под ред. Б.Я. Советева. СПб.: Наука,2008.-552с.

2. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. –СПб.: БХВ-Петербург, 2008. – 318 с.

3. Северин В.А. Комплексная защита информации на предприятии: Учебник для вузов/Под ред. проф. Б.И. Пугинского. М.:Изд. Дом «Городец», 2008.-368с.

4. Информационная безопасность и защита информации: Учебник для вузов/И.Л.Райкин; НГТУ им. Р.Е.Алексеева: Нижний Новгород, 2011.-256с.

5. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

6.3. Нормативные правовые документы.

Не предусмотрены.

6.4.Интернет-ресурсы.

http://itsec.ru
http://www.secuteck.ru
http://www.ispdn.ru
http://www.tssonline.ru
http://www.knigafund.ru
http://www.kladknig.ru

6.5. Иные источники.

Не предусмотрены.

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Название лаборатории/класса, оснащенного необходимым, в соответствии с требованиями ФГОС/ СУОС, оборудованием	**Наименование оборудования**	**Перечень лицензионного программного обеспечения**
учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Рабочие места студентов: столы и стулья – соответственно количеству студентов. Рабочее место для инвалида и лиц с ОВЗ: парта с телескопической столешницей на электромеханическом приводе - 1 шт., кресло-коляска для инвалидов 18" - 1 шт., индукционная петля - 1 шт., компьютер с версией для слабовидящих - 1 шт., кнопка вызова сотрудников - 1 шт. Рабочее место преподавателя: стол – 1 шт., стул – 1 шт, кафедра - 1 шт. Доска меловая и маркерная. Экран, ноутбук Lenovo ideapad 100/15, проектор	Мультимедийный проектор КонсультантПлюс
информационно-аналитическая лаборатория - учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций	Рабочие места: столы компьютерные – в соотвествии с количеством студентов, кресло Престиж Profi -B-20 Самба бордо в рубчик - 15 шт., подставка для ног Fellowes FS-48121 Standard черный - 15 шт. Рабочее место преподавателя: стол компьютерный - 1 шт., стул - 1 шт. Доска меловая или маркерная Персональные компьютеры	Мультимедийный проектор КонсультантПлюс
библиотека - помещение для самостоятельной работы	Рабочие места: столы и стулья. Рабочее место преподавателя: стол – 1 шт., стул - 1 шт., кафедра библиотечная - 1 шт. Телефон – 1 шт., цифровой многофункциональный копир - 1 шт.,	Мультимедийный проектор КонсультантПлюс

	копировальный аппарат МФУ – 1 шт., принтер - 1 шт., сканер – 1 шт. Шкаф – 7 шт, стеллаж-33 шт, библиотечная стойка – 2 шт., стенд – 2 шт. Меловая или маркерная доска. Персональные компьютеры	

Программное обеспечение:

В процессе лекционных и семинарских занятий используется следующее программное обеспечение:

- программы, обеспечивающие навигацию в сети Интернет: «Google chrome»;
- программы, демонстрации видео материалов: проигрыватель «Windows Media»;
- программы для демонстрации и создания презентаций: «Microsoft Power Point».

Информационные справочные системы:

Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: http://www.consultant.ru/

Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: http://www.garant.ru/