МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Защищенные информационные системы

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цель освоения дисциплины.

Дисциплина «Защищенные информационные системы» имеет целью подготовить выпускника к деятельности, связанной с разработкой, модернизацией и вводом в эксплуатацию комплексов, средств и технологий обеспечения информационной безопасности.

2. Место дисциплины в структуре образовательной программы.

Дисциплина «Защищенные информационные системы» относится к числу дисциплин базовой части профессионального цикла. Для лучшего усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе обучения в бакалавриате по направлениям 10.03.01, 11.03.02, 03.03.03, 11.03.01, а также в процессе изучения следующих дисциплин первого курса «Управление информационной безопасностью», «Технологии обеспечения информационной безопасности», «Техническая защита информации», «Аудит информационной безопасности», «Защита информации в беспроводных сетях», «Защита программ и данных».

Знания и практические навыки, полученные в результате изучении дисциплины «Защищенные информационные системы», используются студентами при подготовке дипломных работ и непосредственно в профессиональной деятельности.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	**И-ОПК-2_1.** Способен осуществлять разработку технического проекта системы (либо ее подсистемы, либо компонента) обеспечения информационной безопасности.	**Знать:** − Основные принципы организации технического и программного обеспечения защищенных информационных систем. **Уметь:** − Разрабатывать модели надежности, массового обслуживания и риска защищенных систем и средств хранения, обработки и передачи информации. **Владеть навыками:** − Формулировать и решать задачи моделирования защищенных информационных систем, в том числе средств и сетей хранения, обработки и передачи информации.

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	**И-ОПК-3_1.** Способен осуществлять разработку проектов рабочих, технических, организационно-распорядительных и эксплуатационных документов по обеспечению информационной безопасности в соответствии с действующими нормативными актами и государственными стандартами.	**Знать:** − Требования руководящих и нормативно-методических документов по созданию и эксплуатации АСЗИ. **Уметь:** − Разрабатывать техническую документацию на АСЗИ, нормативно-методические и организационно-распорядительные документы по созданию и эксплуатации АСЗИ. **Владеть навыками:** − Разработки проектов организационно-распорядительных документов на системы обеспечения информационной безопасности. − Организации работ по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.

4. Объем, структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 академических часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Введение в автоматизированные системы – общие понятия	3	2					2	Задание для самостоятельной работы
2	Автоматизированные системы в защищенном исполнении	3	8	8				2	Задание для самостоятельной работы
3	Создание автоматизированных систем	3	10	16				2	Задание для самостоятельной работы.

									Контрольная работа.
4	Сертификация средств защиты информации	3	10	8				2	Задание для самостоятельной работы
5	Средства обеспечения надежности АСЗИ	3	10	8				2	Задание для самостоятельной работы
6	Порядок ввода АСЗИ в эксплуатацию на объекте информатизации	3	8	8				2	Задание для самостоятельной работы. Контрольная работа.
7	Организация обработки конфиденциальной информации	3	8	8				2	Задание для самостоятельной работы
8	Организация технического обслуживания АСЗИ	3	8	8				2	Задание для самостоятельной работы
		3				2	0,5	33,5	Экзамен
	Всего	180	**64**	**64**		**2**	0,5	49,5	

Содержание разделов дисциплины:

Тема 1. Введение в автоматизированные системы – общие понятия

Термины и определения основных понятий в области автоматизированных систем (АС). Нормативно-правовые документы Российской Федерации в области определения, разработки и защиты АС.

Тема 2. Автоматизированные системы в защищенном исполнении

Автоматизированные системы в защищенном исполнении (АСЗИ). Функции системы защиты информации (СЗИ) АС: предупреждение о появлении угроз безопасности информации; обнаружение, нейтрализацию и локализацию воздействия угроз безопасности информации; управление доступом к защищаемой информации; восстановление системы защиты информации и защищаемой информации после воздействия угроз; регистрацию событий и попыток НСД к защищаемой информации и несанкционированного воздействия на нее; обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

Тема 3. Создание автоматизированных систем

Стадии и этапы создания АС (в соотв. с ГОСТ 34.601-90). Формирование требований к структуре АС. Разработка концепции АС. Техническое задание. Эскизный проект. Технический проект. Рабочая документация. Ввод в действие АС. Сопровождение АС.

Тема 4. Сертификация средств защиты информации

Сертификация технических средств защиты информации. Сертификация криптографических средств защиты информации. Сертификация антивирусных программ. Специальные исследования СВТ на ПЭМИН. Специальные технические проверки СВТ.

Тема 5. Средства обеспечения надежности АСЗИ.

Средства обеспечения надежности АСЗИ. Технологии создания отказоустойчивых систем.

Тема 6. Ввод в эксплуатацию АСЗИ на объекте информатизации.

Разработка схем расстановки основных технических средств и систем и вспомогательного оборудования на объекте информатизации. Определение условий расположения объекта информатизации относительно границ контролируемой зоны. Определение перечня сведений ограниченного доступа, подлежащих обработке на АСЗИ. Определение степени участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности. Определение режимов обработки информации в АС в целом и в отдельных компонентах. Классификация АС. Категорирование объекта информатизации. Анализ угроз безопасности информации на объекте информатизации. Разработка модели угроз безопасности информации. Настройка технических, программных и программно-аппаратных средств защиты информации. Разработка организационных мероприятий по защите информации. Разработка организационно-распорядительных документов. Аттестация объекта информатизации. Опытная эксплуатация АСЗИ. Приказ о вводе АСЗИ и СЗИ объекта информатизации в эксплуатацию.

Тема 7. Организация обработки конфиденциальной информации.

Порядок создания, учета, хранения и работы с электронными носителями конфиденциальной информации. Порядок уничтожения электронных носителей конфиденциальной информации. Порядок отправки электронных носителей конфиденциальной информации. Порядок печати конфиденциальных документов с электронных носителей, их регистрации и учета.

Тема 8. Организация технического обслуживания АСЗИ.

Виды технического обслуживания АСЗИ. Средства диагностирования АСЗИ. Содержание и порядок ведения эксплуатационной документации. Организация восстановления системы защиты информации и защищаемой информации после воздействия угроз.

Список лабораторных работ:

1. Защита АС с операционной системой Windows 10 с использованием штатных средств ОС.
2. Построение SIEM на основе MaxPatrol Security Information and Event Managemen.
3. Организация регулярного аудита безопасности сети с помощью сканера MaxPatrol.
4. Построение системы защищенного обмена данными на основе решений ViPNet Coordinator, Admin и Client.
5. Настройка разграничения доступа с помощью Dallas Lock 8.0-К.
6. Настройка изолированной программной среды с помощью Dallas Lock 8.0-К.
7. Настройка доверенной загрузки с помощью программно-аппаратного комплекса «Соболь» версии 4.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине.

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

1) Операционные системы.

1. ОС Windows по программе Microsoft Azure Dev Tools for Teaching.
2. ОС Linux, свободно распространяемые дистрибутивы.

2) Отечественные средства защиты информации.

1. Positive Technologies Application Firewal, конфигурация Education.
2. MaxPatrol, конфигурация Education
3. MaxPatrol Security Information and Event Management, конфигурация Education.
4. ПО Dallas Lock 8.0-К.
5. ПО ViPNet Client 4.
6. ПО ViPNet Administrator 4.5.
7. Программно-аппаратный комплекс (ПАК) ViPNet Coordinator 4.5.
8. ПАК Соболь, версия 4.

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины.

1) основная литература

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин - М.: ДМК Пресс, 2012. - 592 с.

2. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для вузов. / В. В. Платонов - 2-е изд., стер. - М.: Академия, 2014. - 331 с.

2) дополнительная литература

1. Борисов М. А. Основы организационно-правовой защиты информации: [учеб. пособие для вузов.]. / М. А. Борисов, О. А. Романов - 2-е изд. - М.: URSS; ЛИБРОКОМ, 2013. - 203 с.

2. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учеб.пособие для вузов. / В. И.Завгородний; Учеб.-метод.объединение по образованию в обл.статистики,прикладной информатики и мат.методов в экономике - М: Логос, 2001. - 263с.

3) ресурсы сети Интернет

1. Официальный сайт Центра по лицензированию, сертификации и защите государственной тайны ФСБ России. Перечень средств защиты информации, сертифицированных ФСБ России. [Электронный ресурс] // URL: http://clsz.fsb.ru/clsz/license.htm (дата обращения 19.01.2022)

2. Официальный сайт Федерального агентства по техническому регулированию и метрологии. [Электронный ресурс] // URL: http://www.gost.ru/ (дата обращения 19.01.2022)

3. Журнал «Хакер» [Электронный ресурс] // URL: https://xakep.ru (дата обращения 19.01.2022)

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

− учебные аудитории для проведения занятий лекционного типа, оборудованные персональной компьютерной техникой с установленными средствами визуализации текстов в формате DOC/DOCX, PDF, F2B, файлов изображений, презентаций и мультимедийных файлов, а также – видеопроектором и жалюзи на окнах;

− учебные аудитории для проведения практических занятий: лаборатория программно-аппаратных средств обеспечения информационной безопасности;

− учебные аудитории для проведения групповых и индивидуальных консультаций;

− учебные аудитории для проведения текущего контроля и промежуточной аттестации;

− помещения для самостоятельной работы;

− помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических и лабораторных занятий – списочному составу группы обучающихся.

Автор(ы):

Доцент кафедры компьютерной безопасности и математических методов обработки информации В.Н. Князев

Приложение №1 к рабочей программе дисциплины «Защищенные информационные системы»

Фонд оценочных средств для проведения текущей и промежуточной аттестации студентов по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости.

Тема 1. Введение в автоматизированные системы – общие понятия.

1. Задания для самостоятельной работы по теме 1.

1.1. Изучить основные нормативно-правовые документы Российской Федерации в области определения, разработки и защиты АС.

Тема 2. Автоматизированные системы в защищенном исполнении.

1. Задания для самостоятельной работы по теме 2.

1.1. Изучить основные нормативно-правовые документы Российской Федерации в области определения, разработки и защиты АСЗИ.

Тема 3. Создание автоматизированных систем.

1. Задания для самостоятельной работы по теме 3.

1.1. Изучить основные стадии и этапы создания АСЗИ в соответствии с ГОСТ 34.601-90.

2. Вопросы к контрольной работе по темам 1 – 3.

2.1. Дать определение автоматизированной системы.

2.2. Дать определение функции автоматизированной системы.

2.3. Дать определение задаче автоматизированной системы.

2.4. Перечислить основные компоненты автоматизированной системы.

2.5. Дать определение автоматизированного рабочего места.

2.6. Перечислить основные показатели автоматизированной системы.

2.7. Дать определение жизненного цикла автоматизированной системы.

2.8. Дать определение стадии создания автоматизированной системы.

2.9. Дать определение этапу создания автоматизированной системы.

2.10. Дать определение техническому заданию на автоматизированную систему.

2.11. Дать определение техническому проекту на автоматизированную систему.

2.12. Дать определение рабочей документации на автоматизированную систему.

2.13. Дать определение эксплуатационной документации на автоматизированную систему.

2.14. Дать определение общему программному обеспечению автоматизированной системы.

2.15. Дать определение специальному программному обеспечению автоматизированной системы.

2.16. Дать определение государственной тайны.

2.17. Дать определение служебной тайны.

2.18. Дать определение секретной информации.

2.19. Дать определение защищаемой информации.

2.20. Дать определение защите информации.

2.21. Дать определение автоматизированной системы в защищенном исполнении.

2.22. Дать определение системы защиты автоматизированной информации.

2.23. Перечислить функции системы защиты информации АСЗИ.

2.24. Дать определение несанкционированного доступа.

2.25. Перечислить классы защищенности АС от НСД.

2.26. Перечислить стадии создания АСЗИ.

2.27. Перечислить этапы работ, выполняемых на стадии формирования требований к АС.

2.28. Перечислить этапы работ, выполняемых на стадии разработка концепции АС.

2.29. Перечислить этапы работ, выполняемых на стадии ввода в действие.

Тема 4. Сертификация средств защиты информации.

1. Задания для самостоятельной работы по теме 4.

1.1. Изучить основные нормативно-правовые документы Российской Федерации о сертификации средств защиты информации.

Тема 5. Средства обеспечения надежности АСЗИ.

1. Задания для самостоятельной работы по теме 5.

1.1. Изучить основные средства и технологии создания отказоустойчивых систем.

Тема 6. Ввод в эксплуатацию АСЗИ на объекте информатизации.

1. Задания для самостоятельной работы по теме 6.

1.1. Изучить основные этапы и перечень документов, требуемых для ввода в эксплуатацию АСЗИ на объекте информатизации.

2. Вопросы к контрольной работе по темам 4 – 6.

2.1. Дать определение специальной проверки технических средств.

2.2. Дать определение специальным исследованиям технических средств.

2.3. Дать определение понятия объекта информатизации.

2.4. Дать определение основным техническим средствам и системам.

2.5. Дать определение вспомогательным техническим средствам и системам.

2.6. Дать определение границы контролируемой зоны объекта информатизации.

2.7. Охарактеризовать методы обеспечения отказоустойчивости автоматизированных систем.

2.8. Охарактеризовать способы обеспечения отказоустойчивости автоматизированных систем.

2.9. Охарактеризовать средства обеспечения отказоустойчивости автоматизированных систем.

2.10. Сформулировать основные требования ЕСКД по разработке эксплуатационной документации.

2.11. Сформулировать основные требования ЕСКД по разработке эксплуатационной документации.

2.12. Изложить порядок ввода АСЗИ в эксплуатацию на объекте информатизации.

Тема 7. Организация обработки конфиденциальной информации.

1. Задания для самостоятельной работы по теме 7.

1.1. Изучить основные нормативно-правовые документы по работе с конфиденциальной информацией.

Тема 8. Организация технического обслуживания АСЗИ.

1. Задания для самостоятельной работы по теме 8.

1.1. Изучить основные виды технического обслуживания АСЗИ. Изучить средства диагностирования АСЗИ.

9. Список вопросов и (или) заданий для проведения промежуточной аттестации.

Теоретические вопросы.

1. Назвать основные функции системы защиты информации (СЗИ) автоматизированной системы.

8. Назвать и охарактеризовать стадии создания автоматизированной информационной системы.

9. Представить классификацию автоматизированным системам в защищенном исполнении (АСЗИ) по требованиям защиты информации от НСД.

10. Дать характеристику автоматизированным системам в защищенном исполнении (АСЗИ). Назвать основные компоненты АСЗИ.

11. Описать процесс сертификации технических СЗИ.

12. Описать процесс сертификации криптографических СЗИ.

13. Описать процесс сертификации антивирусных СЗИ.

14. Назвать виды специальных проверок технических средств.

15. Дать характеристику свойствам и показателям АСЗИ. Описать жизненный цикл АСЗИ.

16. Охарактеризовать содержание и порядок разработки технического задания на проектирование АСЗИ.

17. Представить классификацию и дать характеристику основным угрозам безопасности информации в автоматизированных системах.

18. Представить классификацию программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей.

19. Назвать методы и способы разработки автоматизированных систем и подсистем безопасности автоматизированных систем.

20. Охарактеризовать средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.

21. Охарактеризовать методы и способы обеспечения отказоустойчивости автоматизированных систем.

22. Назвать и охарактеризовать средства обеспечения отказоустойчивости автоматизированных систем.

23. Основные методы проектирования .

24. Сформулировать основные требования ЕСКД по разработке конструкторской документации.

25. Сформулировать основные требования ЕСКД по разработке эксплуатационной документации.

26. Описать структуру и содержание технического задания на .

27. Дать определение, сформулировать принципы и порядок построения комплексной защиты .

28. Сформулировать основные требования по проектированию комплексной защиты информационной безопасности от НСД.

29. Дать понятие объекта информатизации, основных и вспомогательных технических средств и систем.

30. Изложить порядок ввода АСЗИ в эксплуатацию на объекте информатизации.

31. Описать порядок создания, учета, хранения и работы с электронными носителями конфиденциальной информации.

32. Описать виды технического обслуживания АСЗИ.

Практические вопросы.

1. Сформулировать назначение и возможности SIEM на основе MaxPatrol Security Information and Event Managemen.

33. Сформулировать назначение и возможности сетевого сканера MaxPatrol.

34. Сформулировать назначение и возможности решений ПАК ViPNet Coordinator и ПО Admin и Client.

35. Сформулировать назначение и возможности ПО Dallas Lock 8.0-К.

36. Настройка изолированной программной среды с помощью Dallas Lock 8.0-К.

37. Сформулировать назначение и возможности программно - аппаратного комплекса защиты на АРМ на примере Соболь 3.0.

38. Защита АС с операционной системой Windows 10 с использованием штатных средств ОС.

39. Назвать и охарактеризовать виды технического обслуживания АСЗИ.

Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код индикатора компетенции	Форма контроля	Этапы формирования (№ темы (раздела)	Показатели оценивания	Шкала и критерии оценивания компетенций на различных этапах их формирования		
				Пороговый уровень	Продвинутый уровень	Высокий уровень
Общепрофессиональные компетенции						
И-ОПК-2_1 Способен осуществлять разработку технического проекта системы (либо ее подсистемы, либо компонента) обеспечения информационной безопасности.	− Задания для самостоятельной работы − Контрольная работа − Экзамен	Темы 1 - 8	**Знать:** − основные принципы организации технического и программного обеспечения защищенных информационных систем **Уметь:** − разрабатывать модели надежности, массового обслуживания и риска защищенных систем и средств хранения, обработки и передачи информации **Владеть навыками:** − формулировать и решать задачи моделирования защищенных информационных систем, в том числе средств и сетей хранения, обработки и передачи информации	**Знает:** − основные принципы организации технического и программного обеспечения защищенных информационных систем	**Знает:** − основные принципы организации технического и программного обеспечения защищенных информационных систем **Умеет:** − разрабатывать модели надежности, массового обслуживания и риска защищенных систем и средств хранения, обработки и передачи информации	**Знает:** − основные принципы организации технического и программного обеспечения защищенных информационных систем **Умеет:** − разрабатывать модели надежности, массового обслуживания и риска защищенных систем и средств хранения, обработки и передачи информации **Владеет навыками:** − формулировать и решать задачи моделирования защищенных информационных систем, в том числе средств и сетей хранения, обработки и передачи информации
И-ОПК-3_1 Способен	− Задание для самостоя	Темы 1 - 8	**Знать:** − требования руководящих и	**Знает:** − требования руководящих и	**Знает:** − требования руководящих и	**Знает:** − требования руководящих и

осуществлять разработку проектов рабочих, технических, организационно-распорядительных и эксплуатационных документов по обеспечению информационной безопасности в соответствии с действующими нормативными актами и государственными стандартами.	тельной работы − Контрольная работа − Экзамен		нормативно-методических документов по созданию и эксплуатации АСЗИ. **Уметь:** − проектировать АСЗИ в соответствии с требованиями нормативных документов. **Владеть навыками:** − организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.	нормативно-методических документов по созданию и эксплуатации АСЗИ.	нормативно-методических документов по созданию и эксплуатации АСЗИ. **Умеет:** − проектировать АСЗИ в соответствии с требованиями нормативных документов.	нормативно-методических документов по созданию и эксплуатации АСЗИ. **Умеет:** − проектировать АСЗИ в соответствии с требованиями нормативных документов. **Владеет навыками:** − организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

Критерии оценивания степени овладения знаниями¸ умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

− владение основным объемом знаний по программе дисциплины;

− знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;

− владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;

− способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;

− усвоение основной литературы, рекомендованной рабочей программой дисциплины;

− знание базовых теорий, концепций и направлений по изучаемой дисциплине;

− самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

− достаточно полные и систематизированные знания в объёме программы дисциплины;

− использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

− владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;

− способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

− усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

− умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;

− самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

− систематизированные, глубокие и полные знания по всем разделам дисциплины;

− точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

− безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

− способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

− полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

− умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;

− активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Описание процедуры выставления оценки

Экзамен состоит из двух теоретических вопросов и одного практического задания, выполняемого на лабораторном оборудовании.

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины «Защищенные информационные системы»

Методические указания для студентов по освоению дисциплины

Студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Защищенные информационные системы». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым. Без упорных и регулярных самостоятельных занятий в течение семестра сдать экзамен практически невозможно. Изучение дисциплины предполагает уверенное владение компьютером, умение осуществлять поиск информации в сети Интернет. Кроме углубленного освоения основной и дополнительной литератур, рекомендуется отслеживать регулярно обновляемые материалы государственных стандартов России по управлению безопасности на официальном сайте Росстандарта России (http://www.standard.gost.ru/wps/portal, дата обращения 19.01.2022) в разделе «Уведомления об утверждении национальных стандартов».

Также, рекомендуется использовать ресурсы сети Интернет, указанные в разделе 7 программы.