МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«05» июля 2018 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.01 Проектирование защищенных информационных систем

1.Шифр и наименование направления подготовки/специальности:
10.03.01 Информационная безопасность

2. Профиль подготовки/специализации: безопасность компьютерных систем

3. Квалификация (степень) выпускника: бакалавр

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Храмов Владимир Юрьевич, д.т.н., профессор

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол № 6 от 25.06.2018 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2021/2022 **Семестр(ы)**: 7

9. Цели и задачи учебной дисциплины: изучение теоретических основ проектирования защищенных компьютерных систем (ЗКС), методов формирования функций и задач защиты при создании ЗКС, методов и средств проектирования технологически безопасного программного обеспечения, технологии защиты межсетевого обмена данными, включая методы создания защищенных операционных систем, виртуальных защищенных сетей VPN, использование межсетевых экранов.

Основные задачи дисциплины:

- обучение студентов базовым методам формирования функций и задач защиты при создании ЗКС;
- обучение студентов структурным и объектно-ориентированным методам проектирования технологически безопасного программного обеспечения;
- обучение студентов базовым методам защиты межсетевого обмена данными, включая методы создания защищенных операционных систем, виртуальных защищенных сетей VPN, использование межсетевых экранов;
- овладение практическими навыками проектирования защищенных компьютерных систем;
- овладение практическими навыками работы с инструментальными средствами проектирования программного обеспечения (CASE-средствами) при создании ЗКС.

10. Место учебной дисциплины в структуре ООП: дисциплина относится к профессиональному циклу дисциплин и блоку дисциплин вариативной части. Для успешного освоения дисциплины необходимы входные знания в области стандартов информационной безопасности, формальных моделей безопасности, операционных систем, сетевых технологий, математического анализа, теории множеств, теории вероятностей, теории нечеткой логики, навыки программирования.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**Знать**: этапы, порядок проведения работ, используемые методы и средства проектирования защищенных компьютерных систем; методы формирования функций и задач защиты при создании ЗКС; методы и средства структурного и объектно-ориентированного проектирования программного обеспечения, используемые при создании ЗКС; базовые методы защиты межсетевого обмена данными. **Уметь**: обосновывать функции и задачи защиты при создании ЗКС; с использованием изученных методов и средств осуществлять проектирование ЗКС; разрабатывать схемы сетевой защиты с использованием межсетевых экранов и виртуальных сетей VPN. **Владеть**: практическими навыками применения инструментальных средств проектирования программного обеспечения (CASE-средств) на этапах создания КЗС; навыками формирования политики межсетевого взаимодействия, включая формирование схемы подключения межсетевых экранов, вариантов архитектуры VPN, применения алгоритмов управления доступом на различных уровнях модели OSI.
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении	**Знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); методы и средства структурного и объектно-ориентированного проектирования программного обеспечения, используемые при создании ЗКС; методы определения требований к защите информации. **Уметь:** определять классы защищенности автоматизиро-

	технико-экономического обоснования соответствующих проектных решений	ванных систем и средств вычислительной техники, применять методы и средства проектирования программного обеспечения, используемые при создании ЗКС, методы определения требований к защите информации. **Владеть:** практическими навыками использования инструментальных интеллектуальных систем для обоснования требований к защите информации; практическими навыками использования CASE-средств при анализе исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

12. Объем дисциплины в зачетных единицах/час — 4/144.
Форма промежуточной аттестации: *экзамен*.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 7	№ семестра	Итого
Аудиторные занятия	72	72		72
в том числе: лекции	36	36		36
практические	-	-		-
лабораторные	36	36		36
Самостоятельная работа	36	36		36
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*	36	36		36
Итого:	144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		1. Лекции
1.1	Методы определения требований к защите информации	1. Методы оценки параметров защищаемой информации. 2. Факторы, влияющие на требуемый уровень защиты. Методы деления поля значений факторов на типовые классы.
1.2	Функции и задачи защиты информации	3. Определение и анализ функций и задач защиты. Методы формирования функций защиты. 4. Структура и содержание полного множества задач защиты. Методы формирования задач защиты.
1.3	Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем (ЗКС)	5. Этапы создания ЗКС. Жизненный цикл и технологии проектирования технологически безопасного программного обеспечения при создании ЗКС. 6. Методы и средства структурного подхода к проектированию технологически безопасного программного обеспечения. 7. Методы и средства объектно-ориентированного подхода к проектированию технологически безопасного программного обеспечения.
1.4	Построение защищенных операционных систем (ОС)	8. Подходы к построению защищенных ОС. Архитектура подсистемы защиты ОС. 9. Микроядерные операционные системы. Модель безопасности Trusted Mach.
1.5	Технологии межсетевых экранов (МЭ)	10. Функции МЭ. Особенности функционирования МЭ на различных уровнях модели OSI. 11. Схемы сетевой защиты на базе МЭ.
1.6	Технологии виртуальных защищенных сетей VPN	12. Концепция построения виртуальных защищенных сетей VPN. Варианты построения виртуальных защищенных каналов. 13. Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей.

2. Практические занятия		
2.1	нет	
3. Лабораторные работы		
3.1	Методы определения требований к защите информации	1. Обоснование требований к защищенной системе обработки информации на основе параметров защищаемой информации с использованием оболочки экспертной системы с нечеткой логикой. 2. Обоснование требований к защищенной системе обработки информации на основе факторов, влияющих на требуемый уровень защиты с использованием оболочки ЭС с нечеткой логикой
3.2	Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем	3. Создание функциональной структурной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 4. Создание информационной структурной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 5. Создание функциональной объектно-ориентированной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 6. Создание информационной объектно-ориентированной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 7. Создание событийной объектно-ориентированной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio.
3.3	Технологии виртуальных защищенных сетей VPN	8. Средства обеспечения безопасности виртуальных защищенных сетей VPN 9. Исследование протоколов формирования защищенных виртуальных каналов на канальном, сетевом, сеансовом и прикладном уровнях модели OSI

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Методы определения требований к защите информации	6	8	4	18
2	Функции и задачи защиты информации	6	2	2	10
3	Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем	6	16	14	36
4	Построение защищенных операционных систем	6	2	4	10
5	Технологии межсетевых экранов	6	2	2	10
6	Технологии виртуальных защищенных сетей VPN	6	6	10	22
	Итого:	36	36	36	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;

- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Шаньгин В.Ф. Информационная безопасность систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «Форум»: ИНФРА-М, 2013. – 416 с.
2	Будников С.А. Безопасность операционных систем: учебник / С.А. Будников, В.П. Жуматий, А.В. Шабанов. – Воронеж: ВАИУ, 2009. – 360 с.
3	Орлов С.А. Технологии разработки программного обеспечения: учебник для вузов / С.А. Орлов. – СПб.: Питер, 2008. – 527 с.

б) дополнительная литература:

№ п/п	Источник
4	Хаулет Т. Защитные средства с открытыми исходными кодами. Практическое руководство по защитным приложениям: учебное пособие / Т. Хаулет. – М.: БИНОМ, 2007. – 608 с.
5	Будников, С.А. Информационная безопасность автоматизированных систем. Учебное пособие / С.А. Будников, Н.В. Паршин. – Воронеж: ГУП ВО «Воронежская областная типография», 2011. – 354 с.
6	Скляров И.С. Хакерские фишки / И.С. Скляров. – М.: ЛОРИ, 2008. – 384 с.

в) информационные электронно-образовательные ресурсы:

7	Электронный каталог Научной библиотеки Воронежского государственного университета. – (https // www.lib.vsu.ru/).
8	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
9	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	Будников С.А. Информационная безопасность автоматизированных систем / С.А. Будников, Н.В. Паршин. – Воронеж: ГУП ВО «Воронежская областная типография - издательство им. Е.А. Болховитинова», 2011. – 354 с.
2	Храмов В.Ю. Практикум по разработке и стандартизации программных средств и информационных технологий / В.Ю. Храмов, В.А. Скляров. – Воронеж, ВЭПИ, 2012. – 43 с.
3	Храмов В.Ю. Система поддержки принятия решений с нечеткой логикой / Свидетельство о государственной регистрации программы для ЭВМ № 2015613774, выданное Федеральной службой по интеллектуальной собственности, патентам и товарным знакам 25.03.15 г.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/BPH3739 и № 56036/BPH3739 от 07.10.2016.

2) Система поддержки принятия решений с нечеткой логикой / Свидетельство о государственной регистрации программы для ЭВМ № 2015613774, выданное Федеральной службой по интеллектуальной собственности, патентам и товарным знакам 25.03. 2015 г

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385),ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-7 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать этапы, порядок проведения работ, используемые методы и средства проектирования защищенных компьютерных систем; методы формирования функций и задач защиты при создании ЗКС; методы и средства структурного и объектно-ориентированного проектирования программного обеспечения, используемые при создании ЗКС; базовые методы защиты межсетевого обмена данными.	Разделы 1-6 Методы определения требований к защите информации. Функции и задачи защиты информации. Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем. Построение защищенных операционных систем. Технологии межсетевых экранов. Технологии виртуальных защищенных сетей VPN	Устный опрос, Тест
	Уметь обосновывать функции и задачи защиты при создании ЗКС; с использованием изученных методов и средств осуществлять проектирование ЗКС; разрабатывать схемы сетевой защиты с использованием межсетевых экранов и виртуальных сетей VPN.	Разделы 1, 2, 5, 6 Методы определения требований к защите информации. Функции и задачи защиты информации.Технологии межсетевых экранов. Технологии виртуальных защищенных сетей VPN.	Устный опрос, Тест
	Владеть практическими навыками применения инструментальных средств проек-	Раздел 1, 3, 6 Методы определения требований к защите	Лабораторные работы

	тирования программного обеспечения (CASE-средств) на этапах создания КЗС; навыками формирования политики межсетевого взаимодействия, включая формирование вариантов архитектуры VPN, применения алгоритмов управления доступом на различных уровнях модели OSI.	информации. Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем. Технологии виртуальных защищенных сетей VPN	
ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знать стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); методы и средства структурного и объектно-ориентирован-ного проектирования программного обеспечения, используемые при создании ЗКС; методы определения требований к защите информации.	Разделы 1, 2, 3 Методы определения требований к защите информации. Функции и задачи защиты информации. Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Уметь определять классы защищенности автоматизированных систем и средств вычислительной техники, применять методы и средства проектирования программного обеспечения, используемые при создании ЗКС, методы определения требований к защите информации.	Разделы 1, 4, 5, 6 Методы определения требований к защите информации. Построение защищенных операционных систем. Технологии межсетевых экранов. Технологии виртуальных защищенных сетей VPN.	Контрольная работа по соответствующим разделам или тест
	Владеть практическими навыками использования инструментальных интеллектуальных систем для обоснования требований к защите информации; практическими навыками использования CASE-средств при анализе исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.	Разделы 1, 3 Методы определения требований к защите информации. Методы и средства проектирования технологически безопасного программного обеспечения при создании защищенных компьютерных систем.	Лабораторные работы
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием мате-

матических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с компьютерными моделями алгоритмов обработки информации в среде Microsoft Office Visio и оболочки экспертной системы с нечеткой логикой в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей безопасности.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете с оценкой представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
3	Лабораторная работа	Содержит 11 лабораторных заданий, предусматривающих разработку моделей защищенных компьютерных систем и способность проводить инструментальный мониторинг защищенности компьютерных систем с использованием различных методов обучения.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к зачету с оценкой, в противном случае ставится оценка не зачтено и обучающийся не допускается к зачету.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к экзамену

№	Содержание
1	Понятие защищенной системы обработки информации и ее свойства
2	Методы создания безопасных систем обработки информации
3	Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты
4	Методы деления поля значений факторов на типовые классы
5	Методы формирования функций защиты.
6	Структура и содержание полного множества задач защиты. Методы формирования задач защиты.
7	Этапы создания ЗКС. Жизненный цикл и технологии проектирования технологически безопасного программного обеспечения при создании ЗКС.
8	Методы и средства структурного подхода к проектированию технологически безопасного программного обеспечения.
9	Методы и средства объектно-ориентированного подхода к проектированию технологически безопасного программного обеспечения
10	Подходы к построению защищенных ОС. Архитектура подсистемы защиты ОС.
11	Микроядерные операционные системы. Модель безопасности Trusted Mach.
12	Функции межсетевых экранов. Особенности функционирования МЭ на различных уровнях модели OSI.
13	Схемы сетевой защиты на базе МЭ.
14	Концепция построения виртуальных защищенных сетей VPN. Варианты построения виртуальных защищенных каналов.
15	Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей.
16	Протоколы формирования защищенных виртуальных каналов на канальном, сетевом, сеансовом и прикладном уровнях модели OSI
17	CASE-средство функционального моделирования информационных систем BPWin
18	CASE-средство информационного моделирования ERWin
19	CASE-средство объектно-ориентированного проектирования информационных систем Rational Rose

20	Система поддержки принятия решений в интересах обоснования требований к защите информации

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа № 1

«Обоснование требований к защищенной системе обработки информации на основе параметров защищаемой информации с использованием оболочки экспертной системы с нечеткой логикой»

Цель работы: привитие практических навыков обоснования требований к защищенной системе обработки информации на основе параметров защищаемой информации с использованием оболочки экспертной системы с нечеткой логикой.

Форма контроля: отчёт в письменном виде.

Количество отведённых аудиторных часов: 4

Задание:

Получить у преподавателя описание оболочки экспертной системы с нечеткой логикой (ЭСНЛ) и изучить его. Получить у преподавателя вариант задания и построить функции принадлежности для заданных параметров защищаемой информации (полнота, точность, своевременность, толерантность) с использованием треугольных и трапециевидных функций принадлежности, реализуемых блоком настройки на предметную область оболочки ЭСНЛ. Сформировать типовые (эталонные) ситуации, описывающие классы защищенности компьютерных систем (могут использоваться различные руководящие документы для формирования классов (задаются преподавателем): руководящие документы Гостехкомиссии России; Критерии безопасности компьютерных систем министерства обороны США; Европейские критерии безопасности информационных технологий), с использованием блока преобразования информации ЭСНЛ. Сформировать входную нечеткую ситуацию, характеризующую защищаемую систему, введя параметры полноты, точности, своевременности и толерантности. С использованием блока принятия решений ЭСНЛ определить класс ее защищенности. Поставить в соответствие полученному классу требования к системе защиты информации на основе определенного преподавателем стандарта.

Составить отчёт о проделанной работе, в котором отразить следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель практической работы.
3. Номер своего варианта.
4. Функции принадлежности параметров защищаемой информации.
5. Типовые ситуации для классов защищенности.
6. Требования к параметрам защищаемой информации.
7. Класс защищенности системы и требования по защите информации в ней .

Вариант задания. Определить требования к защищенной системе обработки информации с использованием оболочки экспертной системы с нечеткой логикой на основе следующих параметров защищаемой информации: полнота - высокая, точность - высокая, своевременность - высокая, толерантность – средняя. Классы защищенности определять в соответствии с Критериями безопасности компьютерных систем министерства обороны США (Оранжевая книга).

19.3.4. Пример заданий теста по разделам дисциплины

№	Вопрос	Ответы
1	Сколько основных шагов в процедуре построения безопасных систем обработки информации ?	а) 6 б) 7 в) 4 г) 3
2	Сколько классов защищенности СВТ от НСД к информации устанавливают руководящие документы ФСТЭК России ?	а) 5; б) 10; в) 12; г) 7.

3	К какому классу средств проектирования технологически безопасных информационных систем относится CASE-средство BPWin ?	а) структурно-функциональному б) структурно-событийному; в) объектно-ориентированному; г) структурно-информационному.
4	Сколько параметров защищаемой информации используется в методах оценки защищенности систем обработки информации?	а) 5; б) 3; в) 4.
5	…	

19.3.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2018

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.В.01 Проектирование защищенных информационных систем

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Понятие защищенной системы обработки информации и ее свойства.
2. Методы и средства объектно-ориентированного подхода к проектированию технологически безопасного программного обеспечения.

…

Контрольно-измерительный материал № 11

1. Структура и содержание полного множества задач защиты. Методы формирования задач защиты.
2. Концепция построения виртуальных защищенных сетей VPN. Варианты построения виртуальных защищенных каналов.

…

Преподаватель _____ В.Ю. Храмов

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы, тесты). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое

(ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.