МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
Шабров С.А.
25.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.11 Анализ защищенности информационных систем

1. Код и наименование направления подготовки/специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Профиль подготовки/специализация: Информационная безопасность финансовых и экономических структур

Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра математического анализа

6. Составители программы: Шабров Сергей Александрович, доктор физико-математических наук, доцент

7. Рекомендована: Научно-методическим Советом математического факультета, протокол 25.05.2023, № 0500-06

8. Учебный год: 2026-2027 **Семестр(ы): 8**

9. **Цели и задачи учебной дисциплины**

Цель дисциплины: Изучение принципов проектирования и анализа защищенности информационных систем

Задачи дисциплины: проектирование, эксплуатация и совершенствование системы управления информационной безопасностью информационной системы участие в проведении аттестации объектов информатизации по требованиям безопасности информационных систем

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Анализ защищенности информационных систем» относится к обязательной части Блока Б1. В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, самостоятельной работы и лабораторных работ, ориентированных на освоение студентами современных методологий проектирования, разработки и сопровождения информационно-аналитических систем, а также методов и способов их применения в профессиональной деятельности. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.1	Способен анализировать безопасность информации с помощью формальных моделей	Знает устройство и функционирование современных информационных систем, современные стандарты информационного взаимодействия систем, программные средства и языки программирования, платформы инфраструктуры информационных технологий организаций, требования безопасности информационных систем. Обладает навыками управления содержанием проекта: документирование требований, анализ продукта, организация моделируемых совещаний. Умеет использовать современное прикладное программное обеспечение для векторной или растровой компьютерной графики.
		ПК-2.3	Способен анализировать защищенность информационных систем	Знает подходы к выявлению требований потребителей, определению источников информации для требований Умеет осуществлять выбор методов разработки требований, проводить выбор типов и атрибутов требований, определять состава работ по разработке требований. Обладает специальными знаниями в области разработки планов аналитических работ по отдельным частям системы, интегрирования планов аналитических работ по отдельным частям системы, передачи и согласования плана аналитических работ с менеджером проекта.

12. Объем дисциплины в зачетных единицах/час. — 5 / 180.

Форма промежуточной аттестации экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			8	№ семестра	…
Аудиторные занятия					
в том числе:	лекции	48	48		
	практические				
	лабораторные	48	48		
Самостоятельная работа		48	48		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*		36	36		
Итого:		180	180		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Обзор стандартов информационных систем	Особенности анализа и управления безопасностью информационных систем. Классификация стандартов по безопасности. Серия ISO/IEC 27000. Менеджмент информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США. Классы защищенности компьютерных систем.	
1.2	Уязвимости информационных систем	Анализ угроз ИБ ресурсам информационной системы и причины их реализации. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы.	
1.3	Атаки на информационные системы	Удаленные атаки на информационные системы. Типичные сценарии и уровни атак. Классические и современные методы, используемые нападающими для проникновения в информационные системы.	
1.4	Обеспечение информационной безопасности в информационных системах	Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408. Разработка политики безопасности для информационных систем. Сервисы безопасности: идентификация/ аутентификация, разграничение доступа, протоколирование и аудит, экрани-ро- вание, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление. Средства обеспечения информационной безопасности в ин-формационных системах. Создание комплексной системы обеспечения безопасности информационных систем.	
2. Практические занятия			
2.1			
2.2			
3. Лабораторные занятия			
3.1	Обеспечение информационной безопасности в информационных системах	ISO/ IEC 27000 Использование антивирусных программ	
3.2	Уязвимости информационных	Сканирование уязвимостей информационной системы	

	систем		
3.3	Уязвимости информационных	Сетевые вирусы	
3.4	Атаки на информационные системы	Атака отказ в обслуживании	
3.5	Обеспечение информационной безопасности в информационных системах	Создания защищенных средств связи объектов на основе стандартов ISO 7498-2, 17799, 15408.	
3.6	Обеспечение информационной безопасности в информационных системах	Разработка политики и правил информационной безопасности	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Обзор стандартов информационных систем	12		12	12	36
2	Уязвимости информационных систем	12		12	12	36
3	Атаки на информационные системы	12		12	12	36
4	Обеспечение информационной безопасности в информационных системах	12		12	12	36
	Итого:	48		48	48	144

14. Методические указания для обучающихся по освоению дисциплины: *(рекомендации обучающимся по освоению дисциплины: указание наиболее сложных разделов, работа с конспектами лекций, презентационным материалом, рекомендации по выполнению курсовой работы, по организации самостоятельной работы по дисциплине и др.)*

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях излагается теоретический материал, на лабораторных занятиях решаются задачи по теоретическому материалу, прочитанному на лекциях.

При изучении курса обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все понятия и ГОСТы. Перед следующей лекций обязательно повторить материал предыдущей лекции.

2. Перед лабораторным занятием обязательно повторить лекционный материал.

3. При подготовке к лабораторным занятиям повторить основные понятия по темам. Выполняя работу, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить задачи.

3. Выбрать время для работы с литературой по дисциплине в библиотеке.

Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций и лабораторных занятий) и активную работу на них, но и самостоятельную учебную деятельность в семестрах, на которую отводится 48 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Анализ защищенности информационных систем» предполагает изучение рекомендуемой преподавателем литературы по вопросам лекционных и лабораторных занятий, самостоятельное освоение понятийного аппарата и подготовку к текущим аттестациям.

Вопросы лекционных и лабораторных занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и лабораторным занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольной работы и лабораторных заданий) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации (8 семестр – зачет).

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	*Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с*
2	*Кугаевских, А. В. Проектирование информационных систем. Системная и бизнес-аналитика: учебное пособие: [16+] / А. В. Кугаевских ; Новосибирский государственный технический университет. – Новосибирск, 2018. – 256 с*

б) дополнительная литература:

№ п/п	Источник
1	*Щелоков, С. А. Проектирование распределенных информационных систем: курс лекций по дисциплине «Проектирование распределенных информационных систем» / С. А. Щелоков, Е. Чернопрудова ; Оренбургский государственный университет – Оренбург, 2012. – 195 с.*
2	*Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с.*

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)
2	ЭБС «Университетская библиотека онлайн»
3	http://www.math.vsu.ru – официальный сайт математического факультета ВГУ

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных), курсовых работ и др.)*

№ п/п	Источник
1	*Казарин, О. В. Программно- аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации. Лабораторные занятия ведутся с привлечением мультимедийных технологий.

Microsoft Windows 10, Foxit Reader, 7-Zip, Mozilla Firefox

---

18. Материально-техническое обеспечение дисциплины:

Для проведения лекционных и лабораторных занятий используются аудитории и компьютерные лаборатории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для самостоятельной работы используются классы с компьютерной техникой, оснащенные необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

---

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Обзор стандартов информационных систем	**ПК-2**	ПК-2.1	Контрольная работа № 1
2.	Уязвимости информационных систем	ПК-2	ПК-2.3	Контрольная работа № 1
3.	Атаки на информационные системы	ПК-2	ПК-2.1	Контрольная работа № 2
4.	Обеспечение информационной безопасности в информационных системах	ПК-2	ПК-2.3	Контрольная работа № 2
Промежуточная аттестация форма контроля – зачет				Вопросы к зачету

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контрольная работа № 1

1. На каких принципы основывается информационная безопасность информационных систем?

2. Опишите средства защиты используемые в информационных системах.

3. Сетевые вирусы.

Контрольная работа № 2

1. Удаленные атаки на распределенные системы.

2. Типичные сценарии и уровни атак.

3. Классические и современные методы, используемые нападающими для проникновения в открытые системы.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Вопросы к зачету

1. На каких принципы основывается информационная безопасность информационных систем?
2. Опишите средства защиты используемые в информационных системах.
3. Сетевые вирусы.
4. Удаленные атаки на распределенные системы.
5. Типичные сценарии и уровни атак.
6. Классические и современные методы, используемые нападающими для проникновения в открытые системы.
7. Специфика защиты ресурсов распределенных систем на примере интранета.
8. Принципы создания защищенных средств связи объектов в распределенных систе-мах.
9. Средства обеспечения информационной безопасности в распределенных системах.
10. Управление безопасностью распределенных систем.
11. Организационно-правовые методы защиты распределенных систем.
12. Аутентификация субъектов и объектов взаимодействия в распределенных системах.
13. Системы анализа защищенности.
14. Системы обнаружения и предотвращения вторжений
15. Политика безопасности для информационных систем.
16. Создание комплексной системы обеспечения безопасности для информационных систем.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Выделите верное утверждение в отношении информационной безопасности.

(1) наступление нового этапа развития ИТ приводит к быстрому повышению уровня информационной безопасности

(2) наступление нового этапа развития ИТ приводит к быстрому падению уровня информационной безопасности

(3) уровень информационной безопасности не зависит от этапов развития ИТ

2. Какой термин определяет фактические расходы, понесенные субъектом в результате нарушения его прав, утраты или повреждения имущества, а также расходы, которые он должен будет произвести для восстановления нарушенного права и стоимости поврежденного или утраченного имущества?

(1) угроза

(2) риск

(3) ущерб

(4) утрата

3. Чем регулируется ответственность за нарушение информационной безопасности во внешней среде с целью нанести вред владельцу информации, а также вопросы взаимоотношений между различными субъектами?

(1) внутренними корпоративными документами

(2) федеральными законами РФ, региональными, муниципальными и пр. нормативными актами

(3) международными стандартами в области информационной безопасности

(4) Доктриной информационной безопасности

4. Выделите утверждение, верное в отношении защиты сетей.

(1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена

(2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев

(3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена

(4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

5. Какие две группы документов выделяют на верхнем уровне стандартизации в области информационной безопасности?

(1) инструкции и руководства

(2) оценочные стандарты и спецификации

(3) политики и практики

(4) федеральные законы и нормативные акты

6. Какой подход к обеспечению информационной основывается на решении локальных задач обеспечения информационной безопасности?

(1) частный

(2) комплексный

(3) интегральный

7. К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»?

(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

8. На какие категории делятся угрозы по способу осуществления?

(1) угрозы доступности, целостности, конфиденциальности

(2) случайные или преднамеренные действия

(3) внешние и внутренние

9. За что отвечает программа информационной безопасности нижнего уровня в организации?

(1) контроль за тем, чтобы действия организации не противоречили федеральным и региональным законам и нормативным актам

(2) выработка стратегии организации в области информационной безопасности

(3) обеспечение надежной и экономичной защиты информационных подсистем, конкретных сервисов или групп однородных сервисов

10. Какие компоненты присутствуют в модели системы защиты с полным перекрытием?

(1) область угроз

(2) область рисков

(3) защищаемая область

(4) система защиты

(5) область безопасности

11. К какому типу документов относятся руководящие документы Гостехкомиссии РФ?

(1) федеральные законы

(2) оценочные стандарты

(3) нормативные акты

(4) спецификации

12. Какой подход к обеспечению информационной безопасности является наименее эффективным, но достаточно часто используется, так как не требует больших финансовых и интеллектуальных затрат?

(1) частный
(2) комплексный
(3) интегральный

13. К какому уровню обеспечения ИБ относятся конкретные методики, программно-аппаратные, технологические и технические меры?

(1) законодательный
(2) административный
(3) процедурный
(4) научно-технический

14. Какие составляющие относятся к информационно-технологическому ресурсу современного предприятия?

(1) внешняя и внутренняя информация
(2) обслуживающие системы и технологии
(3) весь персонал
(4) ИТ-специалисты и персонал ИТ-подразделений
(5) финансовый капитал

15. Как называется модель ИБ, которая представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей и ответных мер?

(1) функциональная модель
(2) математическая модель
(3) концептуальная модель
(4) теоретическая модель

16. Чем характеризуется степень сопротивляемости механизма защиты?

(1) вероятностью его преодоления
(2) количеством угроз, которым этот механизм препятствует
(3) величиной потерь в случае успешного прохождения
(4) стоимостью механизма защиты

17. Как в соответствии со стандартом ISO 15408-1999 «Общие критерии оценки безопасности информационных технологий» называются требования, предъявляемые к технологии и процессу разработки и эксплуатации компонентов системы информационной безопасности?

(1) функциональные
(2) технические
(3) требования доверия
(4) требования надежности

18. К какой составляющей интегральной безопасности информационных систем относится защита зданий, помещений, подвижных средств, людей, а также аппаратных средств?

(1) физическая безопасность

(2) безопасность сетей и телекоммуникационных устройств

(3) безопасность системного и прикладного программного обеспечения

(4) безопасность данных

19. Какой термин определяет защищенность жизненно важных интересов государственного или коммерческого предприятия от внутренних и внешних угроз, защиту кадрового и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, которая обеспечивается системой мер правового, экономического, организационного, информационного, инженерно-технического и социального характера?

(1) стратегическая безопасность

(2) информационная безопасность

(3) экономическая безопасность

(4) корпоративная безопасность

20. Выделите охраняемую информацию, оборот которой контролируется:

(1) персональные данные

(2) объекты промышленной собственности

(3) государственная тайна

(4) коммерческая тайна

(5) объекты авторского права

(6) несекретные информационные ресурсы, имеющие государственное значение

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).