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

УТВЕРЖДАЮ

Заведующий кафедрой
математического анализа

С.А. Шабров

(подпись)

18.03.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.15 Системы защиты информации от несанкционированного доступа и воздействия

Код и наименование дисциплины в соответствии с учебным планом

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

2. Профиль подготовки/специализация: Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: математического анализа

6. Составители программы: Найдюк Филипп Олегович, кандидат физико-математических наук, доцент кафедры математического анализа

7. **Рекомендована:** Научно-методическим Советом математического факультета, протокол № 0502-03 от 07.10.2025.

8. Учебный год: 2025/2026 **Семестр: 10**

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:
изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением современных систем защиты информации в операционных системах и вычислительных сетях; формирование компетенций в области персональных данных, принципов работы с ними и методов их защиты.

Задачи учебной дисциплины:
- раскрытие теоретические, практические и методические вопросы обеспечения информационной безопасности;
- рассмотрение методов защиты информации от несанкционированного доступа;
- изучение принципов построения подсистем защиты в сетях различной архитектуры;
- изучение средств, методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности;
- изучение принципов функционирования современных систем идентификации и аутентификации;
- изучение программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Системы защиты информации от несанкционированного доступа и воздействия» относится к учебным дисциплинам по выбору блока Б1 основной образовательной программы по направлению 10.05.04 «Информационно-аналитические системы безопасности».

Дисциплина «Системы защиты информации от несанкционированного доступа и воздействия» базируется на знаниях, полученных по безопасности программного обеспечения, безопасности сетей ЭВМ, безопасности операционных систем и теории алгоритмов.

Приобретенные в результате обучения знания, умения и навыки используются в рамках последующих предметов:

- Техническая защита информации;
- Криптографические протоколы и стандарты.

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	Коды	Индикаторы	Планируемые результаты обучения

ПК-1.2	Способен администрировать системы защиты информации от несанкционированного доступа и воздействия	ПК-1.2	Владеет способами решения типовых задач администрирования систем защиты информации от несанкционированного доступа и воздействия	Знать: средства, методы, алгоритмы, программно-аппаратных средств обеспечения информационной безопасности. Уметь: применять программные и аппаратные продукты от модификации, несанкционированного доступа в информационных системах. Владеть: принципами функционирования современных систем идентификации и аутентификации; навыками разработки и реализации организационных мер, обеспечивающих эффективность системы защиты информации.

12. Объем дисциплины в зачетных единицах/час. — 3/108.

Форма промежуточной аттестации зачёт.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			№ семестра: 10
Аудиторные занятия		64	64
в том числе:	лекции	32	32
	практические		
	лабораторные	32	32
Самостоятельная работа		44	44
в том числе: курсовая работа (проект)			
Форма промежуточной аттестации *(зачёт)*			
Итого:		108	108

13.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Нормативно правовые и технические требования к программно-аппаратным средствам защиты информации. Основные понятия и термины	Правовые и организационные методы защиты информации в АС. Защита информации в АС от случайных угроз. Методы и средства защиты информации в АС от промышленного шпионажа и диверсий. Методы и средства защиты от электромагнитных излучений и наводок. Методы защиты от несанкционированного изменения структур АС. Защита от внедрения аппаратных закладок на этапе разработки и производства. Защита информации в АС от несанкционированного доступа. Криптографические методы защиты информации. Компьютерные вирусы и механизмы борьбы с ними. Защита информации в распределенных АС.	https://edu.vsu.ru/course/view.php?id=32230
1.2	Средства защиты информации от несанкционированного доступа (НСД)	Понятие доступа, субъект и объект доступа. Понятие НСД. Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Назначение и возможности средств защиты информации от НСД. Системы идентификации и аутентификации: основные определения, типы, область применения, классификация. Идентификация субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации.	https://edu.vsu.ru/course/view.php?id=32230

1.3	Программно-аппаратные средства защиты информации от несанкционированного доступа	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	https://edu.vsu.ru/course/view.php?id=32230
1.4	Аппаратные средства защиты информации, криптографической защиты, биометрические средства идентификации	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Проведение аттестации объектов информатизации.	https://edu.vsu.ru/course/view.php?id=32230
2. Практические занятия			
3. Лабораторные занятия			
2.1	Защита от угрозы нарушения конфиденциальности на уровне содержания информации	Задачи и требования к способам и средствам защиты информации техническими средствами. Классификация способов и средств защиты информации.	https://edu.vsu.ru/course/view.php?id=32230
2.2	Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и	https://edu.vsu.ru/course/view.php?id=32230

		состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.	
2.3	Построение систем защиты от угрозы утечки по техническим каналам	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.	https://edu.vsu.ru/course/view.php?id=32230
2.4	Технические методы защиты информации от несанкционированного доступа. Основные направления и цели использования криптографических методов	Этапы эксплуатации. Диагностика и устранение отказов работоспособности технических средств аппаратной защиты. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	https://edu.vsu.ru/course/view.php?id=32230
2.5	Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ.	Этапы эксплуатации программных средств защиты информации. Установка и настройка программных средств защиты информации. Правила защиты от компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Настройка антивирусной защиты	https://edu.vsu.ru/course/view.php?id=32230

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Нормативно правовые и технические требования к программно-аппаратным средствам защиты информации. Основные понятия и термины	4		2	10	16

02	Средства защиты информации от несанкционированного доступа (НСД)	8		6	8	22
03	Программно-аппаратные средства защиты информации от несанкционированного доступа	8		16	16	40
04	Аппаратные средства защиты информации, криптографической защиты, биометрические средства идентификации	12		8	10	30
Итого		32		32	44	108

14. Методические указания для обучающихся по освоению дисциплины:

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях рассказывается теоретический материал, на лабораторных занятиях решаются задачи по теоретическому материалу, прочитанному на лекциях. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

В процессе освоения дисциплины «Системы защиты информации от несанкционированного доступа и воздействия» студенты должны посетить лекционные и лабораторные занятия и сдать зачёт.

Указания для освоения теоретического и практического материала:

1. Обязательное посещение лекционных и лабораторных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.

2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование рабочей программы с методическими рекомендациями, конспекта лекций.

3. Необходимо ознакомится со всеми необходимыми для усвоения курса материалами, размещёнными на платформе «Электронный университет ВГУ» по адресу: https://edu.vsu.ru/course/view.php?id=32230

4. Копирование (электронное) перечня вопросов к зачёту по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины.

5. При подготовке к лабораторным занятиям по дисциплине необходимо изучить рекомендованный лектором материал, иметь при себе конспекты соответствующих тем и необходимый справочный материал.

6. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет – поиск информации, по ключевым словам, курса и ознакомиться с найденной информацией при подготовке к зачёту по дисциплине.

Студент допускается к сдаче зачёта, если имеет на руках конспект основного теоретического материала, имеет отчёты по всем лабораторным работам.

Самостоятельная учебная деятельность студентов по дисциплине «Системы защиты информации от несанкционированного доступа и воздействия» предполагает изучение рекомендуемой преподавателем литературы по вопросам лекционных и лабораторных занятий (приведены ниже), самостоятельное освоение понятийного

аппарата и подготовку к текущим аттестациям (выполнению лабораторных заданий) (примеры см. ниже).

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 (10 семестр – зачёт).

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

а) основная литература:

№ п/п	Источник
1	Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения / О.В. Казарин, А.С. Забабурин. - Москва: Юрайт, 2018. - 311с.: ISBN 978-5-9916-9043-0
2	Мельников, В.П. Информационная безопасность / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева; под ред. В.П. Мельникова 2-е изд. - Москва: КноРус, 2018. - 371 с.: ISBN 978-5-406-04906-8
3	Рацеев, С.М. Математические методы защиты информации и их основы. Сборник задач [Электронный ресурс] / Рацеев С.М. Санкт-Петербург: Лань, 2023. - 140 с. - *URL:* https://e.lanbook.com/book/292910ISBN 978-5-507-45198-2

б) дополнительная литература:

№ п/п	Источник
4	Гашков, С.Б. Криптографические методы защиты информации / С.Б. Гашков, Э.А. Применко, М.А. Черепнев. -М.: Академия, 2010. - 297с.: ISBN 978-5-7695-4962-5
5	Маршаков, Д.В. Программно-аппаратные средства защиты информации [Электронный ресурс] / Д.В. Маршаков, Д.В. Фатхи. - Ростов-на-Дону: Донской ГТУ, 2021. - 228 с. - *URL:* https://e.lanbook.com/book/237770: ISBN 978-5-7890-1878-1
6	Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] / М.А. Иванов, И.В. Чугунков; Под редакцией Иванова М.А. - Москва: НИЯУ МИФИ, 2012. - 400 с. - *URL:* http://e.lanbook.com/books/element.php?pl1_id=75810: ISBN 978-5-7262-1676-8
7	Фефилов, А. Д. Методы и средства защиты информации в сетях: практическое пособие / А.Д. Фефилов. - Москва : Лаборатория книги,

	2011105 с. - *URL:* https://biblioclub.ru/index.php?page=book&id=140796: ISBN 978-5-504-00608-6
8	Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков . - Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. - *URL:* https://biblioclub.ru/index.php?page=book&id=480637
9	Майстренко, Н. В. Основы теории информации и криптографии / Н.В. Майстренко, А.В. Майстренко. - Тамбов: Тамбовский государственный технический университет (ТГТУ), 2018. - 81 с. - *URL:* https://biblioclub.ru/index.php?page=book&id=570354: ISBN 978-5-8265-1950-9
10	Богульская, Н.А. Модели безопасности компьютерных систем [Электронный ресурс] / Н.А. Богульская, М.М. Кучеров. - Красноярск: СФУ, 2019. - 206 с. - *URL:* https://e.lanbook.com/book/157578: ISBN 978-5-7638-4008-7
11	Семыкина, Н.А. Математические модели в информационной безопасности [Электронный ресурс] / Н.А. Семыкина. - Тверь: ТвГУ, 2020126 с. - *URL:* https://e.lanbook.com/book/217946: ISBN 978-5-7609-1573-3

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
12	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)
13	Электронно-библиотечная система "Консультант студента". – (http://www.studentlibrary.ru/)
14	Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)
15	Электронно-библиотечная система "РУКОНТ". – (https://rucont.ru/)
16	Научная электронная библиотека «Киберленинка». – (https://cyberleninka.ru/)
17	Федеральная служба по техническому и экспортному контролю (ФСТЭК России). – (www.fstec.ru/)

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	Рацеев, С. М. Криптографические методы защиты информации и их основы. Лабораторный практикум [Электронный ресурс]: учебное пособие для вузов / Рацеев С. М. Санкт-Петербург: Лань, 2025. -148 с. https://e.lanbook.com/book/460661. - ISBN 978-5-507-51866-1

Курс дисциплины построен таким образом, чтобы позволить студентам проявить способность к самостоятельной работе. Для успешной самостоятельной работы предполагается интерактивный диалог с преподавателем, осуществляемый с помощью удаленной связи через интернет на платформе образовательного портала «Электронный университет ВГУ»: https://edu.vsu.ru/course/view.php?id=32230

Самостоятельная работа студента, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый на лекции и в ходе лабораторных работ. Необходимо овладеть навыками библиографического поиска, уметь находить

подходящие источники, творчески и критически перерабатывать информацию, научиться определять методы исследований.

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

При осуществлении самостоятельной работы возможна интерактивная связь с преподавателем через сеть интернет на платформе образовательного портала «Электронный университет ВГУ»: https://edu.vsu.ru/course/view.php?id=32230.

Проводятся индивидуальные онлайн консультации и проверка контрольных работ.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО на системах с ОС: Ubuntu или Linux.

Выполненные самостоятельные работы согласуются дистанционно посредством образовательного портала «Электронный университет ВГУ»: https://edu.vsu.ru/course/view.php?id=32230.

18. Материально-техническое обеспечение дисциплины:

Для проведения лекционных занятий используется учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель. Для проведения лабораторных занятий используются компьютерные лаборатории факультета, оснащённые лицензионным и/или свободно распространяемым программным обеспечением: Ubuntu, Linux (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop); LibreOffice (GNU LesserGeneralPublicLicense (LGPL); MozillaFirefox (MozillaPublicLicense (MPL), бесплатное и/или свободное ПО, лицензия: https://www.mozilla.org/en-US/MPL/); специализированное антивирусное ПО DrWeb Enterprise Security Suite (лицензионное ПО), Wireshark (бесплатное и/или свободное ПО, лицензия GNU GPL), программное обеспечение для виртуализации персонального компьютера Oracle VM VirtualBox (бесплатное и/или свободное ПО, лицензия GPLv2). В ходе лабораторных занятий может задействоваться учебно-лабораторный стенд «Сетевая безопасность» и/или сертифицированный аппаратно-программный модуль «Соболь».

В самостоятельной работе обучающиеся используют ресурсы Зональной научной библиотеки ВГУ (электронный каталог: http://www.lib.vsu.ru).

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)	Компетенции	Индикаторы достижения компетенции	Оценочные средства
1.	Нормативно правовые и технические требования к программно-	ПК-1	ПК-1.2	Устный опрос

№ п/п	Наименование раздела дисциплины (модуля)	Компетенции	Индикаторы достижения компетенции	Оценочные средства
	аппаратным средствам защиты информации. Основные понятия и термины			
2.	Средства защиты информации от несанкционированного доступа (НСД)	ПК-1	ПК-1.2	Устный опрос, Лабораторный практикум
3.	Программно-аппаратные средства защиты информации от несанкционированного доступа	ПК-1	ПК-1.2	Устный опрос, Лабораторный практикум
4.	Аппаратные средства защиты информации, криптографической защиты, биометрические средства идентификации	ПК-1	ПК-1.2	Устный опрос, Лабораторный практикум
Промежуточная аттестация форма контроля - зачёт				*Перечень вопросов, Задания лабораторного практикума*

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- Тестовые задания;
- Лабораторные работы;
- Контрольная работа.

Примерный перечень заданий лабораторного практикума

1. Указать традиционные методы, технологии и средства защиты информации в ПЭВМ.
2. Найти недостатки традиционных методов и средств защиты информации в ПЭВМ.
3. Определить нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
4. Проанализировать модель канала утечки информации.
5. Провести исследование реестра Windows для нахождения следов активности вредоносного ПО.

6. Определить угрозу несанкционированного копирования информации методами, затрудняющими считывание скопированной информации.

7. Определить угрозу несанкционированного копирования информации методами, препятствующими использованию информации.

8. Проведите сравнительный анализ основных методов защиты от копирования.

9. Назовите основные этапы установки аппаратной части комплекса «Соболь».

10. Назовите основные этапы настройки программной части комплекса «Соболь».

11. Проведите классификацию настройки аппаратной идентификации.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

- Собеседование по билетам к зачету.

Примерный перечень вопросов к зачёту

1. Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации.
2. Понятие несанкционированного доступа (НСД) к информации
3. Концепция защиты от НСД к информации
4. Основные каналы утечки информации в локальной ПЭВМ
5. Модель нарушителя при локальном НСД
6. Основные каналы утечки информации в рабочей станции
7. Показатели защищенности средств ВТ от несанкционированного доступа.
8. Модель нарушителя при удаленном НСД
9. Классификация технических каналов утечки информации
10. Основные показатели технического канала утечки информации
11. Недостатки традиционных методов и средств защиты информации в ПЭВМ
12. Влияние стандартов безопасности на проектирование и разработку программно-аппаратных средств защиты информации
13. Принципы сертификации средств защиты информации
14. Ролевое управление доступом
15. Оценка профилей защиты и заданий по безопасности
16. Средства и методы ограничения доступа к файлам
17. Классификация средств хранения ключей и идентифицирующей информации
18. Основные понятия и классификация требований доверия безопасности
19. Методы защиты программ от исследования
20. Подходы к задаче защиты от копирования программ
21. Общая характеристика и классификация компьютерных вирусов.
22. Общая характеристика средств нейтрализации компьютерных вирусов.
23. Защита на уровне загрузчиков операционной среды
24. Оценочные уровни доверия безопасности
25. Биометрическая идентификация и аутентификация
26. Межсетевое экранирование
27. Регуляторы безопасности и реализуемые ими цели
28. Микроядерная архитектура с точки зрения создания защищенных операционных систем
29. Аутентификация пользователей при локальном и удаленном доступе к КС
30. Средства обеспечения целостности и конфиденциальности при передаче информации по каналам связи
31. Методы поиска уязвимостей
32. Требования к межсетевым экранам

33. Симметричные и асимметричные алгоритмы шифрования информации
34. Функции удостоверяющего центра
35. Структура удостоверяющего центра
36. Концепция иерархии ключей
37. Генерация и хранение ключей
38. Распределение ключей
39. Использование программно-аппаратных средств для защиты информации
40. Дискретное, мандатное и ролевое разграничение доступа к объектам КС
41. Способы идентификации и аутентификации субъектов КС
42. Способы фиксации фактов доступа к файлам. Журналы доступа
43. Способы защиты информации на съёмных дисках
44. Основные схемы резервного копирования
45. Программные закладки и их воздействие на компьютеры
46. Защита данных от разрушающих программных воздействий
47. Формирование и поддержка замкнутой программной среды
48. Классификация средств исследования программ
49. Методы и средства защиты от несанкционированного копирования
50. Юридические аспекты несанкционированного копирования программ
51. Защита массивов информации от изменения
52. Формирование хеш-функций, требования к построению и способы реализации
53. Формальные модели безопасности ОС
54. Реализация механизмов безопасности на аппаратном уровне.
55. Защита системной инфраструктуры
56. Создание защищенной операционной системы
57. Принцип работы систем обнаружения вторжений
58. Анализ защищенности системы при помощи сканера безопасности
59. Взаимная проверка подлинности пользователей
60. Программно-аппаратные средства криптографической защиты информации

Для оценивания результатов обучения на зачёте используются следующие показатели:

- Знание терминов и понятий, принятых в современной литературе, классификацию и назначение основных типов программных и аппаратных средств защиты вычислительных систем; средств, методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности.

- Умение применять программные и аппаратные продукты от модификации, несанкционированного доступа в информационных системах.

- Владение принципами функционирования современных систем идентификации и аутентификации; навыками разработки и реализации организационных мер, обеспечивающих эффективность системы защиты информации.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Достаточное владение материалом: правильные и конкретные, без грубых ошибок ответы на основные вопросы, с возможными неточностями в отдельных ответах;	Пороговый уровень и/или выше порогового	Зачтено

Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете	Ниже порогового уровня	Незачтено

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

1) закрытые задания (тестовые):

ПК-1.2.

1. Международная организация по стандартизации (ISO) под словом «система» в системе менеджмента информационной безопасности понимает:
1) действующее устройство;
2) приложение;
3) процесс, программу действий или методологию.

2. Политика информационной безопасности:
1) это система документированных управленческих решений по обеспечению ИБ организации;
2) это система документированных управленческих решений по обеспечению бизнес-процессов организации;
3) это исходный документ для разработки информационной системы организации.
3. Позиция руководства в соответствии с принципами безопасности и основными бизнес целями компании указывается в документах уровня:
1) политики ИБ;
2) частных политик, стандартов;
3) процедур, инструкций, стандартов конфигурации, журналов.

4. Аспекты информационной безопасности компании представлены в документах уровня:
1) политики ИБ;
2) частных политик, стандартов;
3) процедур, инструкций, стандартов конфигурации, журналов.

5. Методики обеспечения ИБ компании могут быть представлены документами уровня:
1) политики ИБ;
2) частных политик, стандартов;
3) процедур, инструкций, стандартов конфигурации, журналов.

6.Низкоуровневые документированные процедуры определяют:
1) стратегию ЗИ;
2) тактику ЗИ;
3) методики оперативного управления мерами снижения информационных рисков.

7. Объектам и защиты в системах и средствах информатизации и связи являются:
1) информационные ресурсы и средства и системы информатизации;
2) средства и системы информатизации и технические средства, и системы;
3) информационные ресурсы, технические средства и системы и средства и системы информатизации.

8. К Неквалифицированной ЭП относят подпись, которая:
1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2) дает возможность определить лицо, подписавшее электронный документ;
3) содержит ключ проверки ЭП, указанный в квалификационном сертификате.

9. В Федеральном законе №63-ФЗ приведены виды электронных подписей:
1) простая
2) сложная
3) усиленная.

10. В ГОСТ Р ИСО/МЭК 15408- 2013 систематизация и классификация требований к безопасности представлена в рамках иерархии:
1) «класс» - «семейство» - «компонент» - «элемент»;
2) «семейство» - «класс» - «компонент» - «элемент»;
3) «класс» - «семейство» - «элемент» - «компонент».

11. Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всему объему информации, размещенной на носителях одного уровня конфиденциальности содержит следующее количество классов:
1) 2 класса;
2) 5 классов;
3) 6 классов.
12. К событиям явной компрометации ключей НЕ относится:
1) утрата ключевого носителя;
2) нарушение печати на сейфе с ключевыми носителями;
3) утрата ключевого носителя с последующим обнаружением.

13. Правила парольной защиты:
1) регламентируют контроль над действиями пользователей при работе с паролями;
2) определяют требования к организации защиты автоматизированной системы от разрушающего воздействия вредоносного ПО;
3) регламентируют организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в автоматизированной системе.

14. Категорирование защищаемых ресурсов АС- необходимый элемент организации работ по обеспечению безопасности информации - предполагает:
1) типизацию принимаемых контрмер;
2) установление градаций важности (категорий) обеспечения защиты ресурсов;
3) отнесение конкретных ресурсов к соответствующим категориям.

15. Авторизация пользователей осуществляется с применением следующих механизмов реализации разграничения доступа:
1) избирательного управления доступом с помощью атрибутивных схем, списков разрешений и т.п.;
2) полномочного управления доступом с помощью меток конфиденциальности ресурсов и уровней допуска пользователей;
3) регистрации факта попытки доступа и его параметров в системном журнале (в том числе НСД с превышением полномочий).

16. При регистрации событий безопасности в системном журнале обычно фиксируют следующую информацию:

1) дату и время события;
2) идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
3) извещение владельца информации о НСД к его данным.

17. К числу недостатков криптографических методов относят:
1) значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
2) обеспечение высокой гарантированной стойкости защиты;
3) высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

18. Основные типы аппаратно-программных средств аутентификации:
1) на базе смарт-карт и USB-токенов;
2) на базе пассивных контактных и бесконтактных идентификаторов;
3) всё выше указанное.

19. Подключение к сетям общего пользования осуществляется организациями для решения следующих задач:
1) обеспечить взаимодействие с удаленными филиалами и отделениями;
2) организовать доступ к ресурсам внутренней сети мобильных пользователей;
3) всё выше указанное.

20. Классификация уязвимостей по методике CVSS:
1) базовые, временные, связанные со средой;
2) базовые, преходящие, связанные со средой;
3) основные, временные, связанные со средой.

2) открытые задания:

ПК-1.2.

1. Категория конфиденциальности защищаемой информации - _____.

2. Категория целостности защищаемой информации - _____

3. Категория доступности функциональных задач - _____

4. Из скольких уровней состоит общая структура нормативно-методических документов компании в области информационной безопасности? _____

5. Группа 1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всему объему информации, содержит _____ классов.

6. Группа 2, к которой относят АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всему объему информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности, объединяет _____ классов.

7. Комплекс организационно-технических мероприятий, в результате которых посредством специального документа – _____ подтверждается, что объект соответствует требованиям стандартов или иных нормативно технических документов по безопасности информации, утвержденных уполномоченными федеральными органами исполнительной власти.

8. Биометрические методы идентификации подразделяют на _____ группы.

9. К статическим биометрическим методам идентификации относится распознавание по _____

10. К динамическим биометрическим методам идентификации относится распознавание по _____

11. К разграничению доступа существует _____ подхода.

12. Любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы называется _____ (аббревиатура)

13. Действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей информационной системы называется _____

14. Процедура страхования информационных рисков состоит из _____ этапов.

15. Биометрические методы идентификации подразделяют на _____ группы. (название)

16. К разграничению доступа существует _____ подхода.

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.

2) Задания закрытого типа (множественный выбор):
- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):
- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):
- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):
- 2 балла – 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).