Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ
Директор института
_____ А.А. Галкин
«__1__» ____09____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи»

Профиль/программа подготовки «Мобильные средства связи»

Уровень высшего образования: бакалавриат

Форма обучения очная

Владимир 2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: получение представления о современном несанкционированном доступе к информации и защите от него; выработка у студентов основных навыков в информационной защите предприятий и физических лиц от несанкционированного доступа;ознакомление студентов с основными видами несанкционированного доступа к конфиденциальной информации; знакомство с аппаратурными и программными методами борьбы с несанкционированным доступом.
Задачи: подготовка в области получения первичных знаний, умений и навыков студентов по основным принципам и методологии применения в области информационной безопасности для профессиональной деятельности специалиста: научно-исследовательской.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Основы информационной безопасности» относится к обязательной части.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора*	Результаты обучения по дисциплине	
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности УК-1.3. Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений	Знает :методы системного подхода для решения поставленных задач . Умеет осуществлять поиск, критический анализ и синтез информации. Владеет навыками и методами для применения системный подход для решения поставленных задач.	Тестовые вопросы
ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.1. Знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом формате информации ОПК-3.2. Умеет решать задачи обработки данных с помощью современных средств автоматизации ОПК-3.3. Владеет навыками обеспечения информационной безопасности и навыками использования информационно-коммуникационных технологий при поиске необходимой информации	Знает назначение и возможности операционных систем Умеет создавать, редактировать и распечатывать текстовую информацию с помощью редактора Word, защищать документы Владеет поиском источников научно-технической информации (журналы, сайты Интернет), основными требованиями информационной безопасности	Тестовые вопросы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа

Тематический план

форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	в форме практической подготовки		
1.	Основные понятия и определения в области информационной безопасности	6	1,-3	6			1	4	
2.	Предмет и объект защиты информации	6	4,-6	6			1	5	Рейтинг-контроль (5нед)
3.	Угрозы информационной безопасности	6	7,-10	8		6	1	18	
4.	Методы защиты информации	6	11-15	10		6	1	18	Рейтинг-контроль (11нед)
5.	Модели защиты информации	6	16-18	6		6	1	18	Рейтинг-контроль (17нед)
Всего за 5 семестр:				36		18		63	экзамен
Наличие в дисциплине КП/КР					-				
Итого по дисциплине									экзамен

Содержание лекционных занятий по дисциплине

Раздел 1. Основные понятия и определения в области информационной безопасности

Тема 1 Термины, определяющие научную и предметную основы информационной безопасности.

Информация, коммуникация, конфликт, воздействие, угроза, опасность, безопасность, система, информатика, информатизация, информационная система, информационные технологии, информационные процессы, информационный объект, информационный ресурс, информационная инфраструктура, информационная сфера, информационный потенциал.

Тема 2 Термины, определяющие характер деятельности по обеспечению информационной безопасности.

Информационное противоборство, информационное превосходство, информационная безопасность, угрозы информационной безопасности, обеспечение информационной безопасности, система обеспечения информационной безопасности, информационная защищенность, безопасность информации, защита информации, объект защиты информации, носитель информации.

Раздел 2. Предмет и объект защиты информации

Тема 1 Предмет защиты информации

Предмет защиты информации, государственная тайна, уровень секретности

Тема 2 Информация как объект права собственности

Источники (поставщики) информации; пользователи (потребители) информации; собственники (владельцы, распорядители) информации;

Тема 3 Объект защиты информации

Объект защиты, информационная система.

Раздел 3. Угрозы информационной безопасности

Тема 1 Случайные угрозы

Стихийные бедствия и аварии , сбои и отказы, программные ошибки, ошибки пользователей, ошибки в проектировании.

Тема 2 Преднамеренные угрозы

Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение.

Раздел 4. Методы защиты информации

Тема 1 Минимизация ущерба от аварий и стихийных бедствий

Выбор места расположения, обучение персонала, своевременное оповещение..

Тема 2 Дублирование информации

Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение

Тема 3. Повышение надежности информационной системы.

Корректная постановка задачи на разработку, использование прогрессивных технологий программирования, контроль правильности функционирования.

Тема 4. Методы и средства защиты информации от традиционного шпионажа и диверсий.

Создание системы охраны объекта, организация работ с конфиденциальными информационными ресурсами на объекте, противодействие наблюдению, противодействие подслушиванию, защита от злоумышленных действий персонала.

Тема 5. Методы и средства защиты от электромагнитных излучений и наводок.

Пассивные методы (экранирование; снижение мощности излучений и наводок; снижение информативности сигналов.), активные методы (локальное пространственное зашумление, пространственное зашумление)

Тема 6. Защита информации от несанкционированного доступа.

Знания о информационной системе и умения работать с ней, сведения о системе защиты информации, сбои, отказы технических и программных средств, ошибки, небрежность обслуживающего персонала и пользователей.

Раздел 5. Модели защиты информации.

Модель Биба(BiBa), модель Гогена-Мезигера, модель защиты Кларка-Вильсона, криптографические методы защиты информации.

Содержание лабораторных занятий по дисциплине

Раздел 1. Основные понятия и определения в области информационной безопасности

Тема 2. Термины, определяющие характер деятельности по обеспечению информационной безопасности.

Анализ Доктрины информационной безопасности Российской Федерации.

Раздел 4. Методы защиты информации

Тема 6. Защита информации от несанкционированного доступа

Защита документов WORD. Защита документов EXCEL.

5.ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Вопросы рейтинг – контроля №1

1. _____ — цель прогресса внедрения и тестирования средств защиты.

• **Гарантировать правильностьреализации средств защиты**

2. _____ — это выделения пользователем и администраторам только тех прав доступа, которые им необходимы.

• **Принцип минимазации привилегий**

3. _____ — это гарнтия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные.

• **Целостность**

4. _____ — это недостаток систем шифрования с открытым ключом.

• **Относительно низкая производительность**

5. _____ — это политика информационной безопасности.

• **Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации**

6. _____ — это предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы.

• **Авторизация**

7. _____ — это присвоение субъектам и объектам доступа уникального номера, шифра,кода и т.п. с целью получения доступа к информации.

• **Идентификация**

8. _____ — это проверка подлинности пользователя по предъявленному им идентификатору.

• **Аутентификация**

9. _____ — это проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы.

• **Аутентификация**

10. _____ — это свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов.

• **Конфиденциальность**

11. _____ — это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования.

• **Безопасность информации**

12. _____ — это троянские программы.

• **Часть программы с известными пользователю функцичми, способная выполнять действия с**
целью причинения определенного ущерба

Вопросы рейтинг – контроля №2

13. _____ занимается обеспечением скрытности информации в информационных массивах.

• **Стеганография**

14. _____ называется запись определенных событий в журнал безопасности сервера.

• **Аудитом**

15. _____ называется конечное множество используемых для кодирования информации знаков.

• **Алфавитом**

16. _____ называется конфигурация из нескольких компьютеров, выполняющих общее приложение.

• **Кластером**

17. _____ называется метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации.

• **Мандатным**

18. _____ называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий.

• **Профилем защиты**

19. _____ называется оконечное устройство канала связи, через которое процесс может передавать или получать данные.

• **Сокетом**

20. _____ называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля.

• **Мониторингом**

21. _____ называется присоединяемое к тексту его криптографическое преобразование,которое позволяет при получении текста другим пользователем проверить

авторство и подлинность сообщения.

• **Электронной подписью**

22. _____ называется процесс имитации хакером дружественного адреса.

• **"Спуфингом"**

23. _____ называется процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска.

• **Управлением риском**

24. _____ называется система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую.

• **Брандмауэром**

25. _____ называется совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением.

• **Качеством информации**

26. _____ называется список объектов, к которым может быть получен доступ, вместе с доменом защиты объекта.

• **Перечнем возможностей**

27. _____ называется удачная криптоатака.

Вопросы рейтинг – контроля №3

28. _____ называются преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС.

• **Программными закладками**

29. _____ обеспечивается защита исполняемых файлов.

• **Обязательным контролем попытки запуска**

30. _____ обеспечивается защита от программных закладок.

• **Аппаратным модулем, устанавливаемым на системную шину ПК**

31. _____ обеспечивается защита от форматирования жесткого диска со стороны пользователей.

• **Аппаратным модулем, устанавливаемым на системную шину ПК**

32. _____ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

• **Криптоанализ**

33. _____ определяется как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных.

• **Причастность**

34. _____ режим тиражирования гарантирует полную согласованность баз данных.

• **Синхронный**

35. _____ режим тиражирования данных улучшает рабочие характеристики системы.

• **Асинхронный**

36. _____ создается для реализации технологии RAID.

• **Псевдодрайвер**

37. _____ составляет основу политики безопасности.

• **Способ управления доступом**

38. _____ управляет регистрацией в системе Windows 2000.

• **Процедура winlogon**

39. _____ уровень ОС определяет взаимодействие с глобальными ресурсами других организаций.

• **Внешний**

40. _____ уровень ОС связан с доступом к информационным ресурсам

внутри организации.

• **Сетевой**

41. _____ характеризует соответствие средств безопасности решаемым задачам.

• **Эффективность**

42. _____ является администратором базы данных.

• **Любой пользователь, создавший БД**

43. _____ является достоинством дискретных моделей политики безопасности.

• **Простой механизм реализации**

44. _____ является достоинством матричных моделей безопасности.

• **Легкость представления широкого спектра правил обеспечения безопасности**

5.2. Промежуточная аттестация по итогам освоения дисциплины

Вопросы к экзамену

1. Информация, коммуникация, конфликт, воздействие, угроза, опасность, безопасность, система, информатика, информатизация, информационная система, информационные технологии, информационные процессы, информационный объект, информационный ресурс, информационная инфраструктура, информационная сфера, информационный потенциал.
2. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
3. Информационное противоборство, информационное превосходство, информационная безопасность, угрозы информационной безопасности, обеспечение информационной безопасности, система обеспечения информационной безопасности, информационная защищенность, безопасность информации, защита информации, объект защиты информации, носитель информации.
4. Предмет защиты информации
5. Предмет защиты информации, государственная тайна, уровень секретности
6. Источники (поставщики) информации; пользователи (потребители) информации; собственники (владельцы, распорядители) информации;
7. Объект защиты, информационная система.
8. Стихийные бедствия и аварии , сбои и отказы, программные ошибки, ошибки пользователей, ошибки в проектировании.
9. Преднамеренные угрозы
10. Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение.
11. Минимизация ущерба от аварий и стихийных бедствий
12. Выбор места расположения, обучение персонала, своевременное оповещение..
13. Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение
14. Повышение надежности информационной системы.
15. Корректная постановка задачи на разработку, использование прогрессивных технологий программирования, контроль правильности функционирования.
16. Методы и средства защиты информации от традиционного шпионажа и диверсий.
17. Создание системы охраны объекта, организация работ с конфиденциальными информационными ресурсами на объекте, противодействие наблюдению, противодействие подслушиванию, защита от злоумышленных действий персонала.
18. Методы и средства защиты от электромагнитных излучений и наводок.
19. Пассивные методы (экранирование; снижение мощности излучений и наводок; снижение информативности сигналов.), активные методы (локальное пространственное зашумление, пространственное зашумление)
20. Защита информации от несанкционированного доступа.
21. Знания о информационной системе и умения работать с ней, сведения о системе защиты информации, сбои, отказы технических и программных средств, ошибки, небрежность обслуживающего персонала и пользователей.

22. Модель Биба(BiBa),
23. Модель Гогена-Мезигера,
24. Модель защиты Кларка-Вильсона,
25. Криптографические методы защиты информации.

5.3. Самостоятельная работа обучающегося

Темы для докладов:

Проблемы развития теории и практики обеспечения информационной Безопасности

Основные понятия и определения в области информационной Безопасности

Определение информационной безопасности в свете информационных проблем современного общества

Основные составляющие информационной безопасности

Значение информационной безопасности для субъектов информационных отношений

Составляющие национальных интересов российской федерации в информационной сфере

Стратегия национальной безопасности российской федерации

Доктрина информационной безопасности российской федерации

Международное сотрудничество в области информационной безопасности: проблемы и перспективы

Концептуальная модель информационной безопасности

Информация как объект права собственности

Случайные угрозы

Преднамеренные угрозы

Модель гипотетического нарушителя информационной безопасности

Минимизация ущерба от аварий и стихийных бедствий

Дублирование информации

Повышение надежности информационной системы

Создание отказоустойчивых информационных систем

Оптимизация взаимодействия пользователей и обслуживающего персонала

Методы и средства защиты информации от традиционного шпионажа и

Методы и средства защиты от электромагнитных излучений и наводок

Защита информации от несанкционированного доступа

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература*		
1. Азамов О.В. Информационная безопасность [Текст] / О. В. Азамов,К. Ю. Будылин, Е. Г. Бунев, С. А. Сакун, Д. Н. Шакин		http://www.naukaxxi.ru/materials/41/
2. Введение в информационную безопасность [Текст] / А.А. Малюк,В.С. Горбатов, В.И. Королев и др.; под ред. В.С. Горбатова. – М.:Горячая линия – Телеком, 2013. – 288 с.		https://e.lanbook.com/book/111075
n Гатчин Ю.А., Сухостат В.В. Теория информационной безопасностии методология защиты информации [Текст] / Ю.А. Гатчин, В.В.Сухостат – СПб., СПбГУ ИТМО, 2010. – 98 с.		https://books.ifmo.ru/book/587/teoriya_informacionnoy_bezopasnosti_i_metodologiya_zaschity_informacii.htm
Дополнительная литература		
1. ГОСТ Р 50922-2006: Защита информации. Основные термины иопределения		https://fintender.ru/star/gost/r-50922-2006

2. Доктрина информационной безопасности Российской Федерации[Текст]./ Указ Президента Российской Федерации от 5 декабря 2016г. №646		https://rg.ru/2016/12/06/doktrinainfobezopasnost-site-dok.html

6.2. Периодические издания

Отечественные журналы:

- Радиотехника;
- Радиотехника и электроника;
- Приборы и техника эксперимента;
- Цифровая обработка сигналов.

Реферативные журналы:

- Радиотехника;
- Электроника.

Зарубежные журналы:

- IEEE Transactions on Communications;
- IEEE Transactions on Signal Processing;
- IEEE Transactions on Instrumentation and Measurement.

6.3. Интернет-ресурсы

1. Журнал "Проектирование и технология электронных средств" - http://ptes.vlsu.ru
2. Журнал "Радиотехника" - http://radiotec.ru/catalog.php?cat=jr11
3. http://www.studentlibrary.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий практического типа. Лабораторные работы проводятся в компьютерных классах в ауд. 410-3 и 228-3.

Рабочую программу составили: к.т.н. доцент каф. РТ и РС _____ Н.Н.Корнеева

Рецензент:

Генеральный директор ОАО ВКБР к.т.н. _____ Богданов А.Е.

Программа рассмотрена и одобрена на заседании кафедры радиотехники и радиосистем

Протокол № 1 от 30.08.21 года

Заведующий кафедрой _____ Никитин О.Р.

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 11.03.02 - Инфокоммуникационные технологии и системы связи

Протокол № 1 от 1.09.21 года

Председатель комиссии _____ Никитин О.Р.

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

НАИМЕНОВАНИЕ

образовательной программы направления подготовки *код и наименование ОП*, направленность:

наименование (указать уровень подготовки)

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Зав. кафедрой_____/ _____

Подпись *ФИО*