

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»

направленность (профиль) подготовки:

Связь, информационные и коммуникационные технологии

г. Владимир
2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Основы информационной безопасности» является 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» радиоволн относится к обязательной части дисциплин.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

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

Формируемые компетенции	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	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 Проектно-ориентированные задания

<p>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</p>	<p>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 информационнокоммуникационных технологий при поиске необходимой информации.</p>	<p>Знает методы сбора и анализа научно-технической информации отечественного и зарубежного опыта по тематике исследования Умеет использовать информационно-поисковые системы для сбора научно-технической информации. Владеет технологиями сбора, обработки и анализа информации.</p>	<p>Тестовые вопросы Проектно-ориентированные задания</p>
---	---	---	--

3. 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
				Лекции	Практические занятия	Лабораторные работы	в форме практической подготовки		
1.	Основные понятия и определения в области информационной безопасности.	5	1-3	6			1	4	
2.	Предмет и объект защиты информации		4-6	6			1	5	Рейтинг-контроль-1
3.	Угрозы информационной безопасности		7-10	8		6	1	18	
4.	Методы защиты информации		11-16	10		6	1	18	Рейтинг-контроль-2

5.	Государственная политика информационной безопасности	17-18	6	6	1	18	Рейтинг-контроль-3
Всего за 5 семестр			36	18		63	
Наличие в дисциплине КП, КР							
Итого по дисциплине							Экзамен

Содержание лекционных занятий по дисциплине

Раздел 1. Основные понятия и определения в области информационной безопасности

Определения, характеризующие научную и предметную части информационной безопасности. Определения, характеризующие характер деятельности по обеспечению информационной безопасности. Определения, характеризующие предметную часть информационной безопасности. ГОСТ Р 50922-96 "Защита информации. Основные термины и определения".

Раздел 2. Предмет и объект защиты информации

Предмет защиты информации, государственная тайна, уровень предоставления информации Источники (поставщики) информации; пользователи (потребители) информации; собственники (владельцы, распорядители) информации; Объект защиты, информационная система.

Раздел 3. Угрозы информационной безопасности

Случайные угрозы. Стихийные бедствия и аварии, сбои и отказы, программные ошибки, ошибки пользователей, ошибки в проектировании. Преднамеренные угрозы .Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение.

Раздел 4. Методы защиты информации

Минимизация ущерба от аварий и стихийных бедствий. Выбор места расположения, обучение персонала, своевременное оповещение. Дублирование информации. Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение. Повышение надежности информационной системы. Корректная постановка задачи на разработку, использование прогрессивных технологий программирования, контроль правильности функционирования. 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. 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) 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. Государственная политика информационной безопасности

Место информационной безопасности в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности. Функции и задачи органов обеспечения ИБ.

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. Перечислите и поясните определения, характеризующие научную часть информационной безопасности.
2. Перечислите и поясните определения, характеризующие предметную часть информационной безопасности.
3. Перечислите и поясните определения, характеризующие характер деятельности по обеспечению информационной безопасности
4. Что представляет собой канал утечки информации
5. Поясните термин информационное противоборство
6. Что представляет собой доступность информации
7. Что представляет собой целостность информации
8. Что представляет собой конфиденциальность информации
9. Поясните термин защита информации от несанкционированного доступа
10. Чем отличается защита информации от несанкционированного воздействия от защиты информации от непреднамеренного воздействия
11. Что является предметом защиты информации
12. Какие сведения могут содержать государственную тайну
13. Сколько уровней секретности имеет государственная тайна
14. Поясните влияние времени на ценность информации
15. Энтропийный подход для измерения количества информации
16. Тезаурусный подход для измерения количества информации
17. Практический подход для измерения количества информации
18. Что является объектом защиты информации
19. Информация как объект права собственности
20. Уровни представления информации

Вопросы рейтинг – контроля №2

1. Виды случайных угроз
2. Виды преднамеренных угроз
3. Что относится к методам шпионажа и диверсий
4. Что представляет собой канал несанкционированного доступа
5. Что такое наблюдение в теории информационной безопасности?
6. Что такое подслушивание в теории информационной безопасности?
7. Что такое перехват в теории информационной безопасности?
8. Что такое вредоносное программное обеспечение
9. Способы обнаружения угроз
10. Способы предупреждения угроз
11. Каковы основные действия способа ликвидации угроз
12. Поясните разницу между нарушителем и злоумышленником
13. Классификация нарушителя по уровню знаний
14. Классификация нарушителя по уровню возможностей
15. Классификация нарушителя по времени действия
16. Классификация нарушителя по месту действия
17. Какими способами может быть достигнута минимизация ущерба от аварий и стихий-

ных бедствий

18. Как разделяются методы дублирования по времени восстановления
19. Как разделяются методы дублирования по используемым средствам
20. Как разделяются методы дублирования по числу копий

Вопросы рейтинг – контроля №3

1. Как разделяются методы дублирования по процедуре дублирования
2. Как разделяются методы дублирования по процедуре дублирования
3. На каких этапах достигается надежность системы?
4. Поясните понятие отказоустойчивость
5. Какие существуют подходы к созданию отказоустойчивых систем
6. Простое резервирование
7. Помехоустойчивое кодирование
8. Создание адаптивных систем
9. Задачи для защиты объектов информационных ресурсов
10. Рубежи защиты объекта, с конфиденциальной информацией
11. Система охраны объекта
12. Что включает в себя система охраны объекта
13. Требования к системам охранной сигнализации
14. Виды датчиков
15. Субъекты доступа
16. Противодействие наблюдению в оптическом диапазоне
17. Методы борьбы с прослушиванием
18. Методы защиты от электромагнитных излучений
19. Стратегия национальной безопасности РФ
20. Доктрина информационной безопасности РФ

5.2. Промежуточная аттестация по итогам освоения дисциплины

Вопросы к экзамену

1. Что представляет собой канал утечки информации
2. Поясните термин информационное противоборство
3. Что представляет собой доступность информации
4. Что представляет собой целостность информации
5. Что представляет собой конфиденциальность информации
6. Поясните термин защита информации от несанкционированного доступа
7. Чем отличается защита информации от несанкционированного воздействия от защиты информации от непреднамеренного воздействия
8. Что является предметом защиты информации
9. Какие сведения могут содержать государственную тайну
10. Сколько уровней секретности имеет государственная тайна
11. Поясните влияние времени на ценность информации
12. Энтропийный подход для измерения количества информации
13. Тезаурусный подход для измерения количества информации
14. Практический подход для измерения количества информации
15. Что является объектом защиты информации
16. Информация как объект права собственности
17. Уровни представления информации
18. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
19. Предмет защиты информации
20. Предмет защиты информации, государственная тайна, уровень секретности

21. Источники (поставщики) информации; пользователи (потребители) информации; собственники (владельцы, распорядители) информации;
22. Объект защиты, информационная система.
23. Стихийные бедствия и аварии, сбои и отказы, программные ошибки, ошибки пользователей, ошибки в проектировании.
24. Преднамеренные угрозы
25. Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение.
26. Минимизация ущерба от аварий и стихийных бедствий
27. Выбор места расположения, обучение персонала, своевременное оповещение..
28. Шпионаж; несанкционированный доступ, побочные электромагнитные излучения и наводки, вредоносное программное обеспечение
29. Повышение надежности информационной системы.
30. Корректная постановка задачи на разработку, использование прогрессивных технологий программирования, контроль правильности функционирования.
31. Методы и средства защиты информации от традиционного шпионажа и диверсий.
32. Создание системы охраны объекта, организация работ с конфиденциальными информационными ресурсами на объекте, противодействие наблюдению, противодействие подслушиванию, защита от злоумышленных действий персонала.
33. Методы и средства защиты от электромагнитных излучений и наводок.
34. Пассивные методы (экранирование; снижение мощности излучений и наводок; снижение информативности сигналов.), активные методы (локальное пространственное шумление, пространственное шумление)
35. Защита информации от несанкционированного доступа.
36. Стратегия национальной безопасности РФ
37. Доктрина информационной безопасности РФ

5.3. Самостоятельная работа обучающегося

Темы для докладов:

- Информационная безопасность 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
- Европейские стандарты безопасности
- Безопасность информационных технологий США
- Международные стандарты 270000
- Информационная война

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		

Гульятеева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гульятеева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.	2018	https://biblioclub.ru/index.php?page=book&id=574729
Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с. – ISBN 978-5-238-02857-6	2018	https://biblioclub.ru/index.php?page=book&id=562348
Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации [Текст] / Ю.А. Гатчин, В.В.Сухостат – СПб., СПбГУ ИТМО, 2010. – 98 с.	2010	https://books.ifmo.ru/book/587/teoriya_informacionnoy_bezopasnosti_i_metodologiya_zaschity_informacii.htm
Вострецова Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова. - Екатеринбург : Уральский федеральный университет, 2019. - 204 с. - ISBN 978-5-7996-2677-8. - Текст: электронный.	2019	https://ibooks.ru/bookshelf/381669/reading
Дополнительная литература		
1. ГОСТ Р 50922-2006: Защита информации. Основные термины и определения		https://internet-law.ru/gosts/gost/5737/
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

1. Отраслевой lifestyle-журнал по теме безопасности «Рубеж». Режим доступа: <http://ru-bezh.ru/>;
2. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: <http://inside-zi.ru/pages/about.html>;

6.3. Интернет-ресурсы

1. Внутривузовские издания ВлГУ. Режим доступа: <http://e.lib.vlsu.ru/>
2. ИНТУИТ. Национальный открытый университет. Режим доступа: <http://www.intuit.ru/>
3. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" – <https://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 составил Корнеева Н.Н. доцент каф. РТ и РС Н.Н. Корнеева

Рецензент

ОАО «Владимирское КБ радиосвязи», Генеральный директор, А.Е.Богданов А.Е. Богданов

Программа одобрена на заседании каф. РТ и РС

Протокол № 15 от 26.06.2019

Заведующий кафедрой РТ и РС Никитин О.Р. О.Р. Никитин

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

Протокол № 4 от 28.06.2019 года

Председатель комиссии Никитин О.Р, зав. каф. РТ и РС О.Р. Никитин

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20/21 учебный год

Протокол заседания кафедры № 1 от 31.08.2020 года

Заведующий кафедрой О.Р. Никитин

Рабочая программа одобрена на 21/22 учебный год

Протокол заседания кафедры № 1 от 30.08.2021 года

Заведующий кафедрой О.Р. Никитин

Рабочая программа одобрена на 22/23 учебный год

Протокол заседания кафедры № 1 от 29.08.2022 года

Заведующий кафедрой Н.Н. Корнеева

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

«Основы информационной безопасности»

образовательной программы направления подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи»

направленность: «Связь, информационные и коммуникационные технологии»

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

Зав. кафедрой _____ /Никитин О.Р.