



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.04 Основы информационной безопасности

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	1		
Семестр	2		

Лекции	18		
Лабораторные занятия	18		
Практические (семинарские) занятия	18		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	зачет		
Контроль			
Иные формы работы			
Самостоятельная работа	90		

Всего часов: 144

Трудоемкость: 4 зачетные единицы.

Разработчик(и) рабочей программы:

к.п.н., доцент

Н.А. Гнездилова

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи изучения дисциплины:

- развитие творческих подходов при решении сложных научно технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений;
- расширение кругозора.

Место дисциплины в структуре ОПОП: реализуется в рамках обязательной части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-8	Знать: - принципы и методы подбора, изучения, систематизации и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; - методы поиска и обобщения информации, информационно-коммуникационные технологии для поиска и обработки необходимой информации, актуальные источники информации.	Знает: - основные правила регламентации системы управления информационной безопасности и оформления соответствующей документации.
	Уметь: - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; - обобщать общие объемы информации, полученные в результате изучения различных источников, проводить подробное и всестороннее рассмотрение проблемы, оценивать ее	Умеет: - оформлять документацию по информационной безопасности объекта; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью организаций.

значимость, ценность для науки и практики.	
<p>Владеть:</p> <ul style="list-style-type: none"> - навыками осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; - навыками работы с библиографическими источниками и информационно-коммуникационными технологиями для обработки массивов информации. 	<p>Владеет:</p> <ul style="list-style-type: none"> - навыками применения правил регламентации системы управления информационной безопасностью и оформления соответствующей документации в организациях.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
2 семестр						
Раздел 1. «Информационная безопасность в системе национальной безопасности»		62	8	8	8	38
1	Тема 1. Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности	30	4	4	4	18
2	Тема 2. Системные связи информационной безопасности с другими видами национальной безопасности	32	4	4	4	20
Раздел 2. «Информационные уязвимости объектов»		62	8	8	8	38
3	Тема 3. Антропогенные информационные уязвимости. Техногенные информационные уязвимости.	30	4	4	4	18
4	Тема 4. Организационно-правовые и комбинированные информационные уязвимости	32	4	4	4	20
Раздел 3. «Угрозы информационной безопасности и их источники»		20	2	2	2	14
5	Тема 5. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной	20	2	2	2	14

	безопасности					
	<i>Форма отчетности</i>	<i>зачет</i>				
	ИТОГО	144	18	18	18	90
	в т.ч. практическая подготовка					

Очно-заочная форма обучения
не реализуется

Заочная форма обучения
не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы.

Типовой вариант контрольной работы

1. Информационная безопасность в системе национальной безопасности
2. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
3. Виды национальной безопасности и их краткая характеристика.
4. Системные связи информационной безопасности с другими видами национальной безопасности.
5. Информационные уязвимости объектов.
6. Антропогенные информационные уязвимости.
7. Техногенные информационные уязвимости.
8. Организационно-правовые информационные уязвимости.
9. Комбинированные информационные уязвимости
10. Угрозы информационной безопасности и их источники.
11. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
12. Эндогенные и экзогенные, угрозы информационной безопасности, их классификация.
13. Антропогенные и техногенные угрозы информационной безопасности, их классификация.
14. Системная классификация угроз информационной безопасности.
15. Угрозы конфиденциальности, целостности и доступности информации.
16. Информационная война как высшая форма угрозы информационной безопасности.
17. Категорирование информации.
18. Допуск к информационным ресурсам.
19. Основные принципы защиты информации от несанкционированного доступа.
20. Средства обеспечения информационной безопасности.
21. Аппаратные средства обеспечения информационной безопасности.
22. Программные средства обеспечения информационной безопасности.
23. Криптографические средства обеспечения информационной безопасности.
24. Стеганографические средства обеспечения информационной безопасности.
25. Организационно-правовые средства обеспечения информационной безопасности,
26. Государственная политика в области информационной безопасности.
27. Государственные органы обеспечения информационной безопасности.

28. Приоритетные направления обеспечения информационной безопасности в условиях информационного общества.
29. Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества.
30. Технические каналы утечки конфиденциальной информации. Основные методы защиты.
31. Пассивные средства противодействия техническим разведкам.
32. Активные средства противодействия техническим разведкам.
33. Базовые стратегии организации защиты информации.
34. Полное множество функций защиты информации.
35. Задачи защиты информации. Репрезентативное множество задач защиты.
36. Формирование политики обеспечения информационной безопасности объекта.
37. Проектирование оптимальных систем защиты информации.
38. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.
39. Риски информационной безопасности
40. Статистика инцидентов информационной безопасности.
41. Основные макропроцессы управления функционированием комплексной системы защиты информации

Промежуточная аттестация обучающихся осуществляется в форме экзамена с использованием следующих оценочных материалов: *перечень вопросов к экзамену.*

Вопросы к зачету (2 семестр, очная форма обучения)

1. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
2. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности;
3. Виды национальной безопасности и их краткая характеристика.
4. Проблема социальной значимости профессии, высокой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
5. Системные связи информационной безопасности с другими видами национальной безопасности.
6. Определение места и роли информационной безопасности в системе национальной безопасности России.
7. Антропогенные информационные уязвимости.
8. Методика изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.
9. Техногенные информационные уязвимости.
10. Проблема технических каналов утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.
11. Организационно-правовые и комбинированные информационные уязвимости.
12. Проблема использования естественнонаучных законов и применения математического аппарата в профессиональной деятельности при выявлении сущности проблем, возникающих в задачах обеспечения информационной безопасности.
13. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.

14. Проблема определения видов и форм информации, подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
15. Угрозы, целостности, доступности и конфиденциальности информации.
16. Классификация правонарушений в сфере компьютерной информации.
17. Роль информации в развитии современного общества, применение достижений информатики и вычислительной техники в задачах переработки больших объемов информации и проведения целенаправленного поиска в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных сетях,
18. Противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 277 с. – (Высшее образование). – ISBN 978-5-534-16450-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/531084> (дата обращения: 18.04.2024).

4.2. Дополнительная литература

1. Вострецова, Е. В. Основы информационной безопасности : учебное пособие / Е. В. Вострецова ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2019. – 207 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=697636> (дата обращения: 18.04.2024).
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/530927> (дата обращения: 18.04.2024).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.