Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____Хагуров Т.А.
«___» ___05___ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.25 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки/специальность_02.03.02 **Фундаментальная информатика и информационные технологии**
(код и наименование направления подготовки/специальности)

Направленность (профиль) / специализация__Математическое и программное обеспечение компьютерных технологий
(наименование направленности (профиля) специализации)

Программа подготовки _академический бакалавриат_____
(академическая /прикладная)

Форма обучения ___очная_____
(очная, очно-заочная, заочная)

Квалификация выпускника ____бакалавр_____
(бакалавр, магистр, специалист)

Краснодар 2021

Рабочая программа дисциплины «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии.

Программу составил(а):

Жуков Сергей Александрович, доцент, к. ф.-м. н., доцент __ __
Ф.И.О. ,должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» утверждена на заседании кафедры Вычислительных Технологий
протокол №6 от «20 » мая 2021 г.

Заведующий кафедрой (разработчика) Вишняков Ю. М.
фамилия, инициал подпись

Утверждена на заседании учебно-методической комиссии факультета
Компьютерных Технологий и Прикладной Математики
протокол № 1 от «20» мая 2021 г

Председатель УМК факультета Коваленко А.В.
фамилия, инициалы подпись

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий
ФБГОУ ВО «Кубанский государственный университет»,
кандидат физико-математических наук.

Схаляхо Ч.А., доцент КВВУ им.С.М.Штеменко, к.ф.-м.н., доцент

1. Цели и задачи освоения дисциплины

1.1 Цель освоения дисциплины

Целью преподавания и изучения дисциплины «Информационная безопасность» является формирование у студентов способности оценивать угрозы информационной безопасности и разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств по ее защите, а также разрабатывать методы реализации и тестирования таких систем.

1.2 Задачи дисциплины

Студент должен знать основные понятия, методы, алгоритмы и технологии защиты информации; уметь применять теории и методы по обеспечению информационной безопасности; владеть технологиями реализации систем такой защиты.

1.2 Место дисциплины (модуля) в образовательной программе

Дисциплина «Информационная безопасность» относится к вариативной части блока Б1 Дисциплины (модули).

Для изучения дисциплины необходимо знание дисциплин “Дискретная математика”, “Алгебра”, “Основы программирования”, “Теория алгоритмов и вычислительных процессов”, “Операционные системы”, “Компьютерные сети”. Знания, получаемые при изучении основ защиты информации, используются при изучении таких дисциплин профессионального цикла учебного плана бакалавра как “Программирование в компьютерных сетях”, “Криптографические протоколы”, а также при работе над выпускной работой.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **профессиональных компетенций:**

№ п.п.	Индекс компе-тенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающие должны		
			знать	уметь	владеть
1	ОПК-5	способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии, международные и профессиональные стандарты в области информационной безопасности	использовать углубленные теоретические и практические знания в области информационной безопасности	навыками использования технологий обеспечивающих создание безопасных программных решений
2	ПК-1	способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии, международные и профессиональные стандарты в области информационной безопасности	использовать углубленные теоретические и практические знания в области информационной безопасности	навыками использования технологий обеспечивающих создание безопасных программных решений

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 6 зач.ед. (216 часов), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)	
		5	6
Аудиторные занятия (всего)	125	72,2	52,3
В том числе:			
Занятия лекционного типа	50	34	16
Лабораторные занятия	66	34	32
КСР	8	4	4
ИКР	0,5	0,2	0,3

Самостоятельная работа (всего)	55,8	35,8	20
В том числе:			
Проработка учебного (теоретического) материала	56	36	20
Промежуточная аттестации		зачет	экзамен
Контроль	35,7		35,7
Общая трудоемкость час зач. ед.	216 6	108 3	108 3

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в _5_ семестре *(очная форма).*

№	Наименование разделов	Количество часов					
		Всего	Аудиторная работа				Внеаудиторная работа
			Л	КСР	ИКР	ЛР	СРС
1	2	3	4	5	6	7	8
1	Содержание понятия безопасность и его структура.	10	4				6
2	Проектирование алгоритмов поддержки информационной безопасности.	22				16	6
3	Стандарты информационной безопасности.	10	2			2	6
4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.	16	6	2		2	6
5	Модели управления доступом к информации.	38	18	2	0,2	12	5,8
6	Модели поддержания целостности информации	12	4			2	6
	Итого по дисциплине:	108	34	4	0,2	34	35,8

Разделы дисциплины, изучаемые в _6_ семестре *(очная форма).*

№	Наименование разделов	Количество часов						
		Всего	Аудиторная работа				Внеаудиторная работа	
			Л	КСР	ИКР	ЛР	КОНТРОЛЬ	СРС
1	2	3	4	5	6	7	8	9
7	Аудит вычислительной системы и архивация	10	2			4		2
8	Анализ уязвимости системы. DLP-системы	12	2			4		2
9	Системы обнаружения вторжений	10	2			4		2
10	Поддержка информационной безопасности в вычислительных сетях	10	2			4		2
11	Зловредное программное обеспечение	10	2			2		2
12	Основы криптографии	16	2	2		6		2
13	Криптография с секретным ключом	14	2			4		4
14	Криптография с открытым ключом	62	2	2	0,3	4	35,7	4
	Итого по дисциплине:	108	16	4	0,3	32	35,7	20

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Содержание понятия безопасность и его структура	Виды безопасности и связи между ними. Анализ угроз информационной безопасности. Правовая поддержка организации информационной безопасности. Смысл компьютерной безопасности,	ЛР

		ее основные требования. Основные понятия актуализации компьютерной безопасности.	
2	Проектирование алгоритмов поддержки информационной безопасности	Организация вычислений на графе. Кодирующие и декодирующие преобразования. Алгоритмы защиты данных, основанные на комбинаторике и теории чисел.	ЛР
3	Стандарты информационной безопасности	Критерии безопасности компьютерных систем (Оранжевая книга). ISO/IEC 17799:2002 “Управление информационной безопасностью”. ISO 15408 “Общие критерии безопасности информационных технологий” “CommonCriteria” (ОК). Российские стандарты в области информационной безопасности.	ЛР
4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации	Подходы к идентификации и аутентификации. Понятие полномочий и ролей, их виды. Реализация сценария идентификации- аутентификации-авторизации в операционных системах Windows и Unix.	ЛР
5	Модели управления доступом к информации	Монитор безопасности. Основные политики доступа. Модель HRU. Модель Белла-ЛаПадулы. Модель МакЛина. Модель Take-Grant. Модель Китайская стена.	ЛР
6	Модели поддержания целостности информации	Ролевые модели доступа. Модель Биба. Модель Кларка-Вильсона.	ЛР
7	Аудит вычислительной системы и архивация	Смысл аудита и ресурсы, необходимые для его осуществления. Способы и инструментарий для аудита в операционных системах Windows и Unix. Выполнение backup-а системы, архивация данных.	ЛР
8	Анализ уязвимости системы. DLP-системы	Классификация уязвимостей. Пример уязвимости и ее использование. Методология гипотетического дефекта. Обзор DLP-систем	ЛР
9	Системы обнаружения вторжений	Обзор моделей обнаружения вторжений. Архитектура IDS-системы. Средства детекции вторжений в операционных системах.	ЛР
10	Поддержка информационной безопасности в вычислительных сетях	Анализ стека протоколов ISOOSI с точки зрения информационной безопасности. Межсетевой экран. Технология сетей VPN. Протоколы защиты информации различных уровней. Протокол Kerberos. Инфраструктура управления открытыми ключами.	ЛР
11	Зловредное программное обеспечение	Анализ различных видов вирусов. Жизненный цикл вирусов. Признаки заражения вирусом. Методы и средства антивирусной защиты.	ЛР
12	Основы криптографии	Основные схемы шифрования. Основные факты об арифметике вычетов. Алгоритмы Евклида и Рабина.	ЛР
13	Криптография с секретным ключом	Алгоритмы шифрования методами замены, перестановки, гаммирования. Алгоритмы DES,	ЛР

		AES. Управление ключами.	
14	Криптография с открытым ключом	Система Диффи-Хелмана. Шифр Эль-Гамаля. Алгоритм RSA. Электронная цифровая подпись. Инфраструктура открытых ключей.	ЛР

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ
1−9	2	Проектирование алгоритмов поддержки информационной безопасности.
10	3	Стандарты информационной безопасности.
11	4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.
12−18	5	Модели управления доступом к информации.
19	6	Модели поддержания целостности к информации
20−21	7	Аудит вычислительной системы и архивация.
22-23	8	Анализ уязвимости системы. DLP-системы
24−25	9	Системы обнаружения вторжений
26−27	10	Поддержка информационной безопасности в вычислительных сетях
28	11	Зловредное программное обеспечение
29-31	12	Основы криптографии
32-33	13	Криптография с секретным ключом
34-36	14	Криптография с открытым ключом

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.3.5 Самостоятельное изучение разделов дисциплины

Раздел 1. Законодательные акты: О безопасности, Доктрина информационной безопасности РФ, Об охране интеллектуальной собственности, О персональных данных, Об информации, информационных технологиях и о защите информации, О государственной тайне, О международном обмене информацией.

Раздел 2. Учебники и пособия по проектированию структур данных и алгоритмов их обработки. Руководства, учебники и пособия по языку VisualC++ и работе в среде VisualStudio 2012 и выше.

Раздел 3. Международные и российские стандарты РФ по информационной безопасности: закон РФ "О техническом регулировании", "Критерии оценки

доверенных компьютерных систем" (Department of Defense TrustedComputer System Evaliation Criteria, TCSEC − Оранжевая книга), ISO/IEC 15408:1999 "Критерии оценки

безопасности информационных технологий" (Evaluationcriteria for IT security − ОК), ГОСТ Р 50739, ГОСТ Р 50922-96, ГОСТ Р 51188-98, ГОСТ Р 50739-95.

Раздел 4. Руководства и учебники поадминистрированию в операционных системах Windows, Unix, Linux.

Раздел 5. Учебники и пособия из рекомендованного списка литературы.

Раздел 6. Руководства и учебники поадминистрированию в операционных системах Windows, Unix, Linux, учебные ресурсы в internet.

Раздел 7. Учебники и пособия из рекомендованного списка литературы.

Раздел 8. Учебники и пособия из рекомендованного списка литературы, а также обучающие материалы от производителей антивирусного ПО.

3. Образовательные технологии

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
5, 6	Л	Компьютерные презентации и обсуждение	72
	ЛР	Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	72
Итого:			144

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств для итоговой аттестации (экзамена в 6 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;

- ответа на экзамене

4.2.1 Перечень вопросов к зачету

1. Классификация информационных угроз.
2. Основные качества защищенной информации в ИС.
3. В чем смысл политики безопасности.
4. Что такое несанкционированный доступ (НСД) и их виды.
5. Что такое уязвимость, атака, структура атаки и возможные виды атак.
6. Виды моделей доступа к данным, их характеристика.
7. Назначение стандартов информационной безопасности. Структура стандартов.
8. Что такое сниффинг, спуффинги hijacking.
9. Что такое DOS-атака, DDOS-атака ,SYN-атака.
10. Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
11. Какого вида данные обязаны находиться в открытом доступе.

12. Назовите уровни секретности данных, которые регламентирует закон РФ “О государственной тайне”.

4.2.2 Критерии оценивания к зачету

Оценка “зачтено” - практические задания выполнены в срок в объеме не менее 80%. Студент демонстрирует правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при аргументации ответов на вопросы при защите лабораторных.

Оценка «не зачтено» -практические задания не выполнены либо предоставлены не в срок в объеме менее 60%, Студент демонстрируетналичие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа.

Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,
– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4.2.3 Перечень вопросов к экзамену

1. Классификация информационных угроз.
2. Основные качества защищенной информации в ИС.
3. В чем смысл политики безопасности.
4. Что такое несанкционированный доступ (НСД) и их виды.
5. Что такое уязвимость, атака, структура атаки и возможные виды атак.
6. Виды моделей доступа к данным, их характеристика.
7. Назначение стандартов информационной безопасности. Структура стандартов.
8. Что такое сниффинг, спуффинги hijacking.
9. Что такое DOS-атака, DDOS-атака ,SYN-атака.

10. Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.

11. Какого вида данные обязаны находиться в открытом доступе.
    Назовите уровни секретности данных, которые регламентирует закон РФ
    “О государственной тайне”.
12. Механизм идентификации, аутентификации и авторизации в ОС Unix.
13. Механизм идентификации, аутентификации и авторизации в ОС Windows.
14. Биометрические методы аутентификации
15. Механизм одноразовых паролей
16. Протокол аутентификации Kerberos
17. Основные положения дискреционной модели полномочий HRU
18. Основные положения мандатной модели полномочий Белла-ЛаПадулы
19. Модель полномочий Мак-Лина.
20. Классификация зловредного программного обеспечения.
21. Особенности полиморфного вируса и руткита.
22. Основные положения VPN-сети.
23. Назначение методов социальной инженерии и их формы.
24. Назначение и формы аудита в ОС Windows.
25. Назначение и механизм сетевого экрана.
26. Характеристика средств информационной безопасности в рамках стека протоколов ISO OSI.
27. Структураугрозинформационнойбезопасности.
28. Содержание основных понятий ИБ: «защищенность данных», «уязвимость», «атака», «злоумышленник» и др. Их отражение в стандартах ИБ.

4.2.4 Образцы билетов

Билет №1

1. Правила NRU и NWD . Области использования этих правил.
2. Характеристика схемы симметричного шифрования. Достоинства и недостатки этой схемы.
3. Сколько времени необходимо на расшифровку ключа алгоритма DES на компьютере с быстродействием 1000 млрд. операций в секунду если один ключ расшифровывается за 10 операций.

Билет№2

1. Основные компоненты модели Take-Grant. Понятие графа доступов и его пример.
2. Протокол аутентификации Kerberos.
3. Постройте матрицу управления доступом для медицинского учреждения, в котором врачи могут читать писать истории болезней и предписания по лечению, а медицинские сестры могут читать и писать предписания по лечению, но ничего не должны знать об истории болезней.

4.2.5 Критерии оценивания к экзамену

Оценка «отлично»: точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «хорошо»: при ответе на один вопрос даны точные формулировки

алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями; при ответе на второй вопрос имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «удовлетворительно»: при ответе на оба вопроса имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «неудовлетворительно»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература

1. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК, 2017. − 434 с.

5.2 Дополнительная литература

2. М. Ховард, Д. Лебланк Защищенный код. М.: ИД Русская редакция, 2004.− 704 с.
3. Проскурин В. Г. Защита программ и данных. М.: ИДАкадемия, 2012.− 208 с.
4. T. Howlett Open source security tools. Practical applications for security. Prantice Hall, 2004.− 600 p.
5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие.− М.: ИД Форум – Инфра, 2013.− 416 с.
6. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. М.:Горячая линия – Телеком, 2000.− 452 с.
7. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2008.− 256 с.
8. Девянин П. Н. Модели безопасности компьютерных систем. Учебное пособие.− М.: Академия, 2005.− 144 с

6. Перечень необходимого программного обеспечения

1. Microsoft Visual Studio 2012+ : Visual C++, C#
2. OracleVirtualBoxv 5.1 +
3. Python

Методические указания по выполнению лабораторных работ

Лабораторные работы выполняются, как правило, в компьютерном классе. Отдельные работы могут выполняться в аудитории при наличии у бакалавриантов портативных компьютеров.

На лабораторных занятиях осуществляется реализация алгоритмов работы с структурами, применяемыми при защите информации, осуществляется тестирование знаний студентов по вопросам информационной безопасности. По отдельным темам бакалавриантам поручается подготовить презентации и выступить с докладами на занятиях.

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Лекционная аудитория, желательно оборудованная видеопроектором и экраном.

Компьютерные классы, лаб. А301а. Классы оснащены компьютерами, объединенными в локальную сеть. Аудитории для лабораторных занятий, оборудованные досками.