

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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин



22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.08 Информационная безопасность и защита информации

1. Код и наименование направления подготовки/специальности:
38.04.05 Бизнес-информатика
2. Профиль подготовки / специализация / магистерская программа:
Информационная бизнес-аналитика
3. Квалификация (степень) выпускника: магистр
4. Форма обучения: очная
5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем
6. Составители программы: Сафронов Виталий Владимирович,
доцент кафедры кибербезопасности информационных систем
7. Рекомендована: НМС факультета ПММ, протокол № 5 от 22.03.2024

отметки о продлении вносятся вручную)

8. Учебный год: 2024/2025

Семестр(ы): 1

9. Цели и задачи учебной дисциплины:

Целью освоения учебной дисциплины являются формирование целостного представления об информационной безопасности, получение теоретических и практических знаний, позволяющих организовывать работы по созданию и внедрению профессионально-ориентированных информационных систем с учетом необходимости реализации информационной безопасности, используя возможности современных интеллектуальных информационных технологий

Задачи учебной дисциплины:

- изучение основ технологий обеспечения информационной безопасности;
- изучение методологий проектирования и реализации системы защиты информации, с учетом угроз, характерных для современных информационных систем;
- получение знаний, необходимых для управления электронным предприятием и подразделениями электронного бизнеса, включая управление информационной безопасностью.

10. Место учебной дисциплины в структуре ОПОП: часть, формируемая участниками образовательных отношений, блока Б1 учебного плана.

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	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-4	Способен управлять разработкой профессионально-ориентированных информационных систем с учетом возможностей современных интеллектуальных информационных технологий	ПК-4.3	Организует работы по созданию и внедрению профессионально-ориентированных информационных систем с учетом возможностей современных интеллектуальных информационных технологий	Знать: – <i>законодательную базу информационной безопасности;</i> – <i>модели политики безопасности;</i> – <i>наиболее известные симметричные и асимметричные криптосистемы;</i> – <i>наиболее известные модели политики безопасности.</i> Уметь: – <i>реализовывать алгоритмы шифрования, кодирования;</i> – <i>определять и решать задачи по управлению информационной безопасностью;</i> – <i>подбирать модель политики безопасности для экономических информационных систем, включая электронный бизнес;</i> – <i>организовывать работы по созданию и внедрению ЭИС с учетом возможностей современных интеллектуальных информационных технологий.</i> Владеть: – <i>навыками построения модели информационной безопасности;</i> – <i>навыками криптографического закрытия данных и работы с ключами.</i>
ПК-6	Способен управлять электронным предприятием и подразделениями электронного бизнеса	ПК-6.2	Владеет навыками управления электронным предприятием и подразделениями электронного бизнеса	

12. Объем дисциплины в зачетных единицах/час (в соответствии с учебным планом) — 3/108.

Форма промежуточной аттестации (зачет/экзамен) зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			1 семестр	2 семестр
Аудиторные занятия				
в том числе:	лекции	32	32	
	практические			
	лабораторные	16	16	
Самостоятельная работа		60	60	
в том числе: курсовая работа (проект)				
Форма промежуточной аттестации (зачет – 0 час. / экзамен – 0 час.)				
Контроль				
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			Онлайн-курс «Информационная безопасность и защита информации» (ИБиЗД) (3/0, маг., эк.) 1) ». – https://edu.vsu.ru/course/view.php?id=27146
1.1	Вопросы обеспечения информационной безопасности в ЭИС.	Предметная область информационной безопасности. Исторические сведения и этапы развития проблем и технологий обеспечения информационной безопасности. Термины и определения Проблема ИБ: предпосылки возникновения. Задачи разработчиков информационных систем. Понятие «защищенная система». Свойства ЗС. Виды защиты данных. Угрозы ИБ. Функции непосредственной защиты информации. Экономические информационные системы. Применяемые методы и средства защиты. Методы идентификации и аутентификации.	
1.2	Криптография и криптоанализ	Типы криптографических схем. Симметричные алгоритмы. Асимметричные алгоритмы. Хэширование. Криптоанализ. ЭЦП. Применение в электронном бизнесе.	
1.3	Построение систем защиты.	Принципы построения и требования к системам защиты. Состав систем обеспечения безопасности данных. Изъяны защиты. Классификации. Причины возникновения. Политика безопасности. Модели безопасности. Стандарты информационной безопасности	
2. Практические занятия (не предусмотрены)			
3. Лабораторные занятия			
3.1	Лабораторная работа №1 Тема: разработка системы разграничения доступа	Изучение выбранной (по вариантам) предметной области, разработка модели ИБ ИС и реализация алгоритмов закрытия данных для различных уровней доступа.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Вопросы обеспечения информационной безопасности в ЭИС.	10		4	20	38
2	Криптография и криптоанализ	10		4	20	35
3	Построение систем защиты.	12		8	20	35
	Итого:	32		16	60	108

14. Методические указания для обучающихся по освоению дисциплины

Работа с конспектами лекций, выполнение практических заданий, выполнение лабораторных заданий, заданий текущей и промежуточной аттестаций.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины (список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Нестеров С. А., Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров, М., Юрайт, 2016, 321с
2	Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. [Электронный ресурс].

б) дополнительная литература:

№ п/п	Источник
34	Кетков, Ю.Л. Введение в языки программирования С и С++ : курс / Ю.Л. Кетков. – М. : Интернет-Университет Информационных Технологий, 2008. – 252 с. – URL: https://biblioclub.lib.vsu.ru/index.php?page=book&id=234040 (16.09.2016).
4	Шилдт Г. С++. Базовый курс / Г. Шилдт. – М. : Вильямс, 2015. – 624 с.
5	Столлов Е.Л. Генераторы случайных чисел в системах компьютерной безопасности[Электронный ресурс]. - Казань, 2014. - Режим доступа: http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf
6	Воронков Б. Н. Технология двойного "затемнения" в электронных платежных системах. Алгоритмы, программа, моделирование / Б. Воронков, Ю. Крыжановская, Ю. Фельдшерова Saarbrücken : LAP LAMBERT Academic Publishing, 2014 99 с. : ил. ISBN 978-3-659-55591-6

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
7	www.lib.vsu.ru – ЗНБ ВГУ
8	https://e.lanbook.com/ – Электронно-библиотечная система "Лань"

* Вначале указываются ЭБС, с которыми у ВГУ имеются договоры, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы
(учебно-методические рекомендации, пособия, задачки, методические указания по выполнению лабораторных и контрольных работ)

№ п/п	Источник
1	Криптографические методы защиты информации [Электронный ресурс] : учебно-методическое пособие : [для студ. фак. прикладной математики, информатики и механики очной и очно-заоч. форм обучения, для направлений и специальностей: 01.03.02 - Прикладная математика и информатика, 02.03.02 - Фундаментальная информатика и информационные технологии, 01.04.02 - Прикладная математика и информатика, 10.05.01 - Компьютерная безопасность] / Воронеж. гос. ун-т ; сост.: Б.Н. Воронков, Ю.А. Крыжановская. — Электрон. текстовые дан. — Воронеж: Издательский дом ВГУ, 2018
2	Программные методы защиты информации : Метод. указания к спецкурсу "Теорет. основы защиты информации" : Для студ. 4 к. д/о и 5 к.в/о фак. ПММ / ВГУ. Каф. техн. кибернетики и автомат. регулирования; Сост. Ю.А.Крыжановская Ч.1 Воронеж, 2002 36 с. : ил.. табл. 7.15
3	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс] : учебное пособие для спо / Никифоров С. Н. 2-е изд., стер. Санкт-Петербург : Лань, 2022 160 с. ISBN 978-5-507-44449-6

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

При реализации дисциплины используются модульно-рейтинговая и личностно-ориентированные технологии обучения (ориентированные на индивидуальность студента, компьютерные и коммуникационные технологии). В рамках дисциплины предусмотрены следующие виды лекций: информационная, лекция-визуализация, лекция с применением обратной связи.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория должна быть оборудована учебной мебелью, компьютером, мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), допускается переносное оборудование.

Лабораторные занятия должны проводиться в специализированной аудитории, оснащенной учебной мебелью и персональными компьютерами с доступом в сеть Интернет (компьютерные классы, студии), мультимедийным оборудованием (мультимедийный проектор, экран, средства звуковоспроизведения). Число рабочих мест в аудитории должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере.

Для самостоятельной работы необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет.

Программное обеспечение (см. файл МТО):

- ОС Windows 8 (10)
- Интернет-браузер (Google Chrome, Mozilla Firefox)
- Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО)
- Adobe Reader (свободное и/или бесплатное ПО)

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- вопросы

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Вопросы обеспечения информационной безопасности в ЭИС.	ПК-4, ПК-6	ПК-4.3, ПК-6.2	КИМы для проведения текущей аттестации Задания для лабораторных работ
2.	Криптография и криптоанализ	ПК-4, ПК-6	ПК-4.3, ПК-6.2	
3.	Построение систем защиты.	ПК-4, ПК-6	ПК-4.3, ПК-6.2	
Промежуточная аттестация форма контроля – зачет				КИМы для проведения итоговой аттестации

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного ответа на вопросы; выполнения лабораторных работ.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования. Промежуточная аттестация по итогам освоения дисциплины проводится в форме зачета. Для получения положительной итоговой оценки необходимо выполнение лабораторной работы и верные ответы на вопросы зачета.

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью опроса и выполнения лабораторной работы.

Текущая аттестация проводится в виде защиты лабораторных работ и опросов по пройденным темам, адрес курса в электронной образовательной среде «Электронный университет ВГУ» <https://edu.vsu.ru/course/view.php?id=27146>.

Примерный список вопросов

1. Хэширование. Хэш-функции. Алгоритмы
2. Метод рассечения-разнесения.
3. Сжатие
4. Симметричные алгоритмы шифрования
5. Асимметричные алгоритмы шифрования
6. Кодирование. Отличия от шифрования. Алгоритмы (табличная кодировка, кодировочная книга)
7. Стеганография
8. ЭЦП. Подделка электронных подписей
9. Проблема защиты информации. Ее актуальность. Основные понятия информационной без-

опасности.

10. Основные виды защиты информации
11. Предпосылки кризисной ситуации с обеспечением защиты информации. Задачи разработчиков современных информационных систем в контексте безопасности.
12. Методы создания безопасных систем обработки информации.
13. Угрозы информации. Понятия и определения. Различные типы классификаций
14. Понятие «защищенная система», свойства защищенных систем.
15. Виды защиты данных
16. Типы разрушающих программных средств. Средства противодействия
17. Проблема идентификации/аутентификации. Типы аутентификации
18. Классификация информации по ее доступности.
19. Слабые места вычислительных систем.
20. Подсистемы системы защиты
21. Принципы организации систем защиты данных.
22. Требования к системам защиты
23. Угрозы безопасности
24. Методы и средства защиты данных. Классификация средств защиты.
25. Экономические информационные системы
26. Основные положения для защиты АИС, ЭИС
27. Политика безопасности. Понятия, определения. Формальные модели безопасности. Типы моделей безопасности, примеры. Этапы построения ПБ
28. Нормативно-правовое обеспечение информационной безопасности бизнеса
29. Стандарты ИБ. Примеры. Особенности. Свойства.
30. Системы разграничения доступа. Авторизация.
31. Криптология. Криптография. Криптоанализ. Задачи криптографии и криптоанализа.
32. Основные требования к защитным преобразованиям информации.
33. Защита данных в сетях
34. Изъяны защиты.
35. Источники правовой информации.
36. ИБ в банковской деятельности
37. Взаимодействие бизнеса и ИБ (парадигмы, схемы, угрозы, атаки)

Лабораторные работы

Примеры заданий

1. Реализовать вариант дискреционной политики безопасности для электронного бизнеса с несколькими способами криптографического закрытия данных
2. Реализовать вариант мандатной политики безопасности для электронного бизнеса с несколькими способами криптографического закрытия данных

20.2 Итоговый контроль успеваемости

Промежуточная аттестация по дисциплине (зачет) осуществляется с помощью следующих оценочных средств: вопросы.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Зачтено – выполнены и защищена лабораторная работа, получено больше половины верных ответов при опросах	Пороговый и выше	Зачтено
Не зачтено – не выполнена лабораторная работа, получено меньше половины верных ответов при опросах.	Ниже порогового	Не зачтено

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

ПК-4 Способен управлять разработкой профессионально--ориентированных информационных систем с учетом возможностей современных интеллектуальных информационных технологий.

ПК-6 Способен управлять электронным предприятием и подразделениями электронного бизнеса

Вопросы с вариантами ответов

1. Отметьте правильный ответ
К понятию информационной безопасности НЕ относятся:
+ природоохранные мероприятия;
– надежность работы компьютера;
– сохранность ценных данных.
2. Отметьте правильный ответ
Информационное оружие – это?
+ комплекс технических средств, методов и технологий, направленных против управленческих систем;
– нормативно-правовая база по информационной безопасности;
– комплекс индивидуального и общественного сознания.
3. Отметьте правильный ответ
К банковской тайне можно отнести:
+ информацию о банковском счете, вкладе, операциях по счету, о клиентах банка;
– информацию о сотрудниках банка;
– информацию о режиме работы банка.
4. Отметьте правильный ответ
Сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации относятся к:
+ тайне банковского счета;
– тайне операций по банковскому счету;
– тайне банковского вклада.
5. Отметьте правильный ответ
Под «маскарадом» понимается ...
+ выполнение каких-либо действий одним пользователем от имени другого пользователя;
– обработка денежных счетов при получении мелких сумм;
– монополизация какого-либо ресурса системы.

Вопросы с кратким текстовым ответом

1. Дополните:
... – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
+ персональные данные
2. Дополните
Проверка подлинности пользователя. Это
+ аутентификация
3. Вставьте пропущенное слово:
Обрабатываемые персональные данные подлежат ... либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом
+ уничтожению
4. Дополните

Подписавший не вправе утверждать, что он не подписывал документ, т.к. ключ подписи принадлежит именно ему и именно он отвечает за его безопасное хранение – свойство ...

+ неотказуемости

+ неотказуемость

5. Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

+ профессиональная тайна

Критерии и шкалы оценивания заданий ФОС:

Для оценивания выполнения заданий используется балльная шкала:

Вопросы с вариантами ответов (закрытые)

Критерий оценивания	Шкала оценок
Верный ответ	1 балл
Неверный ответ	0 баллов

Вопросы с кратким текстовым ответом

Критерий оценивания	Шкала оценок
Должен быть сформулирован ответ из указанных вариантов (один или несколько) или аналогичные по сути ответы с альтернативными терминами и определениями	2 балла
Неверный ответ	0 баллов

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).