МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовский государственный университет генетики, биотехнологии и инженерии имени Н.И. Вавилова»

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
И.о. заведующего кафедрой	Декан факультета
_____ / Ключиков А.В. /	_____ / Волощук Л.А./
«12» 04 2024 г.	«12» 04 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина	**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направление подготовки	**38.03.05 Бизнес-информатика**
Направленность (профиль)	**Цифровая бизнес-аналитика предприятий и организаций**
Квалификация выпускника	**Бакалавр**
Нормативный срок обучения	**4 года**
Форма обучения	**Очная**

Разработчик: доцент, Розанов А.В. _____ (подпись)

Саратов 2024

1. Цель освоения дисциплины

Целью изучения дисциплины является формирование у обучающихся навыков практического обеспечения защиты информации и безопасного использования программных средств в современных информационных системах.

2. Место дисциплины в структуре ОПОП ВО

В соответствии с учебным планом по направлению подготовки 38.03.05 Бизнес-информатика, направленность (профиль) Цифровая бизнес-аналитика предприятий и организаций, дисциплина «Информационная безопасность» относится к части Блока 1, формируемой участниками образовательных отношений.

Для изучения дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Информатика», «Алгоритмизация и программирование».

Дисциплина «Информационная безопасность» является базовой для изучения дисциплины «Базы данных в бизнес-аналитике».

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми индикаторами достижения компетенций

Изучение данной дисциплины направлено на формирование у обучающихся компетенций, представленных в табл. 1

Таблица 1

Требования к результатам освоения дисциплины

№ п/п	Код компетенции	Содержание компетенции	Индикаторы достижения компетенции	В результате изучения учебной дисциплины обучающиеся должны		
				знать	уметь	владеть
1	2	3	4	5	6	7
1	ПК-1	ПК-1 Способен работать, используя основные методы, способы и средства получения, хранения, переработки информации для управления бизнесом	ПК-1.5 Определяет способы защиты интеллектуальной собственности в процессе решения задач управления жизненным циклом ИТ-инфраструктуры предприятия, обеспечивает комплексную защиту информации	основные методы, способы и средства получения, хранения, переработки информации и способы защиты интеллектуальной собственности	использовать основные методы, способы и средства получения, хранения, переработки информации для управления бизнесом	навыками комплексной защиты информации и интеллектуальной собственности в процессе решения задач управления жизненным циклом ИТ-инфраструктуры предприятия

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов

Таблица 2

	Количество часов								
	Всего	*в т.ч. по семестрам*							
		1	2	3	4	5	6	7	8
Контактная работа – всего, в т.ч.	76,1					76,1			
аудиторная работа:	76					76			
лекции	38					38			
лабораторные	38					38			
практические									
промежуточная аттестация	0,1					0,1			
контроль									
Самостоятельная работа	31,9					31,9			
Форма итогового контроля	Зач.					Зач.			
Курсовой проект (работа)	-					-			

Таблица 3

Структура и содержание дисциплины
«Информационная безопасность»

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самостоятельная работа	Контроль знаний	
			Вид занятия	Форма проведения	Количество часов	Количество часов	Вид	Форма
1	2	3	4	5	6	7	8	9
5 семестр								
1.	Введение в информационную безопасность: основные понятия и определения. Системный подход к обеспечению информационной безопасности	1	Л	В	2	0,75	ТК	УО
2.	Техника безопасности при работе на персональных ЭВМ. Лабораторная работа	1	ЛЗ	Т	2	0,75	ВК	Тс

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самостоятельная работа	Контроль знаний	
			Вид занятия	Форма проведения	Количество часов	Количество часов	Вид	Форма
1	2	3	4	5	6	7	8	9
	№1.1. Методы ограничения доступа к информации с помощью парольной защиты							
3,	Роль информационного ресурса и информационной безопасности в обществе	2	Л	Т	2	0,75	ТК	УО
4.	Лабораторная работа №1.2. Методы ограничения доступа к информации с помощью парольной защиты	2	ЛЗ	М	2	0,75	ТК	УО
5.	Классификация источников опасности. Характеристика угроз конфиденциальности и целостности информации	3	Л	В	2	0,75	ТК	УО
6.	Лабораторная работа №2.1. Анализ интернет-трафика через сетевые интерфейсы ОС Windows	3	ЛЗ	Т	2	0,75	ТК	УО
7.	Понятие политики безопасности. Основные принципы политики безопасности. Задачи, решаемые политикой безопасности.	4	Л	В	2	0,75	ТК	УО
8.	Лабораторная работа №2.2. Анализ интернет-трафика через сетевые интерфейсы ОС Windows	4	ЛЗ	М	2	0,75	ТК	УО
9.	Цели создания политики безопасности. Субъектно-объектная модель информационной системы	5	Л	Т	2	0,75	ТК	УО
10.	Лабораторная работа №3.1. Назначение прав пользователей при произвольном управлении доступом в ОС Windows	5	ЛЗ	М	2	0,75	ТК	УО
11.	Понятия состояния системы и потока информации. Правила разграничения доступа	6	Л	Т	2	0,75	ТК	УО
12.	Лабораторная работа №3.2. Назначение прав пользователей при произвольном управлении доступом в ОС Windows	6	ЛЗ	Т	2	0,75	ТК	УО
13.	Политика избирательного доступа. Принудительное и добровольное управление доступом	7	Л	В	2	0,75	ТК	УО
14.	Лабораторная работа №4.1. Анализ защищенности информации средствами протоколирования и аудита	7	ЛЗ	Т	2	0,75	ТК	УО

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самостоятельная работа	Контроль знаний	
			Вид занятия	Форма проведения	Количество часов	Количество часов	Вид	Форма
1	2	3	4	5	6	7	8	9
15.	Политика полномочного доступа. Текущее значение уровня безопасности	8	Л	Т	2	0,75	ТК	УО
16.	Лабораторная работа №4.2. Анализ защищенности информации средствами протоколирования и аудита	8	ЛЗ	М	2	0,75	ТК	УО
17	Правовая защита информационной безопасности на международном уровне и на уровне Российской Федерации	9	Л	Т	2	0,75	ТК	УО
18.	Лабораторная работа №5.1. Анализ защищенности информационной системы встроенными средствами диагностики - WMIC	9	ЛЗ	Т	2	0,75	ТК	УО
19.	Аппаратные, программные и криптографические средства защиты. Инженерно-технические и комбинированные средства защиты информации	10	Л	В	2	0,75	ТК	УО
20.	Лабораторная работа №5.2. Анализ защищенности информационной системы встроенными средствами диагностики - WMIC	10	ЛЗ	Т	2	0,75	РК	УО, Д, Тс
21.	Классификация угроз информационным системам. Случайные угрозы. Преднамеренные угрозы. Шпионаж и диверсии	11	Л	Т	2	0,75	ТК	УО
22.	Лабораторная работа №6.1. Шифрование и дешифрование в MS Excel	11	ЛЗ	М	2	0,75	ТК	УО
23	Несанкционированный доступ к информации. Электромагнитное излучение и наводки. Несанкционированная модификация структуры	12	Л	Т	2	0,75	ТК	УО
24.	Лабораторная работа №6.2. Шифрование и дешифрование в MS Excel	12	ЛЗ	Т	2	0,75	ТК	УО
25	Задачи защиты информации от случайных угроз. Дублирование информации. Повышение надёжности компьютерных систем. Создание отказоустойчивых систем	13	Л	Т	2	0,75	ТК	УО
26.	Лабораторная работа №7.1 Основные признаки присутствия на компьютере вредоносных программ	13	ЛЗ	Т	2	0,75	ТК	УО

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самостоятельная работа	Контроль знаний	
			Вид занятия	Форма проведения	Количество часов	Количество часов	Вид	Форма
1	2	3	4	5	6	7	8	9
27	Оптимизация взаимодействия пользователей и обслуживающего персонала. Минимизация ущерба от аварий и стихийных бедствий. Блокировка ошибочных операций	14	Л	В	2	0,75	ТК	УО
28	Лабораторная работа №7.2. Основные признаки присутствия на компьютере вредоносных программ	14	ЛЗ	Т	2	0,75	РК	УО, Д, Тс
29	Защита информации от несанкционированного доступа. Идентификация и аутентификация. Защита информации от шпионажа и диверсий	15	Л	Т	2	0,75	ТК	УО
30.	Лабораторная работа №8.1. Программные средства информационной безопасности	15	ЛЗ	М	2	0,75	ТК	УО
31	Использование паролей в сетях ЭВМ. Виды паролей. Противодействие угрозам съёма паролей	16	Л	Т	2	0,75	ТК	УО
32	Лабораторная работа №8.2. Программные средства информационной безопасности	16	ЛЗ	Т	2	0,75	ТК	УО
33	Защита баз данных. Защита от несанкционированной модификации структуры баз данных	17	Л	В	2	0,75	ТК	УО
34.	Лабораторная работа №9.1 Установка и настройка параметров российских антивирусных программ Касперский, Dr. Web	17	ЛЗ	Т	2	0,75	ТК	УО
35	Криптографические методы защиты информации. Моноалфавитное и полиалфавитное шифрование	18	Л	М	2	0,75	ТК	УО
36	Лабораторная работа №9.2 Установка и настройка параметров зарубежных антивирусных программ Avast, Eset NOD32	18	ЛЗ	Т	2	0,75	ТК	УО
37	Аппаратные и программные средства защиты информации в компьютерных сетях.	19	Л	Т	2	0,75	ТК	УО
38.	Лабораторная работа №10. Правовая основа защиты информации в компьютерных сетях	19	ЛЗ	Т	2	0,75	РК	УО, Д, Тс

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самостоятельная работа	Контроль знаний	
			Вид занятия	Форма проведения	Количество часов	Количество часов	Вид	Форма
1	2	3	4	5	6	7	8	9
Выходной контроль					0,1	3,4	ВыхК	З
Итого:					76,1	31,9		

Примечание:
Условные обозначения:
Виды контактной работы: Л – лекция, ЛЗ – лабораторное занятие.
Формы проведения занятий: В – лекция-визуализация, Т – лекция/занятие, проводимое в традиционной форме, М - моделирование.
Виды контроля: ВК – входной контроль, ТК – текущий контроль, РК – рубежный контроль, УО – устный опрос, Д – доклад, Тс – тестирование, З – зачет.

5. Образовательные технологии

Организация занятий по дисциплине «Информационная безопасность» проводится по видам учебной работы: лекции, лабораторные занятия, текущий и рубежный контроль. Реализация компетентностного подхода в рамках направления подготовки 38.03.05 Бизнес-информатика, для профиля подготовки Цифровая бизнес аналитика предприятий и организаций, предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой для формирования и развития профессиональных навыков обучающихся.

Лекционные занятия проводится в поточной аудитории с применением мультимедийного проектора в виде учебной презентации. Основные моменты лекционных занятий конспектируются. Отдельные темы предлагаются для самостоятельного изучения с обязательным составлением конспекта.

Целью лабораторных занятий является выработка практических навыков применения информационных технологий при решении различных задач с использованием специализированных пакетов прикладных программ и информационных ресурсов глобальной сети Интернет в перспективных направлениях бизнес-информатики.

Для достижения этих целей используются как традиционные формы работы – выполнение лабораторных работ и т.п., так и интерактивные методы – групповая работа, анализ проблемных ситуаций, моделирование.

Групповая работа при анализе конкретных ситуаций развивает способности проведения анализа и диагностики исследуемых процессов.

Метод анализа проблемной ситуации в наибольшей степени соответствует задачам высшего образования. Он более, чем другие методы, способствует развитию у обучающихся изобретательности, умения решать проблемы с учетом конкретных условий и при наличии фактической информации. С помощью метода анализа проблемной ситуации у обучающихся развиваются такие квалификационные качества, как умение четко формулировать и высказывать свою позицию, умение коммуницировать, дискутировать, воспринимать и оценивать новую или нестандартную информацию.

Моделирование представляет собой современные метод повышения творческой активности обучаемых, позволяя рассматривать и анализировать не только стандартные условия функционирования процессов, но и недоступные для обычной практики предельные или даже катастрофические ситуации.

Лабораторные занятия проводятся в специальных аудиториях - компьютерных классах, оборудованных высокопроизводительными персональными компьютерами с широкополосным доступом к информационным ресурсам локальной Intranet-сети университета и общемировой компьютерной сети Интернет.

Самостоятельная работа охватывает проработку обучающимися отдельных вопросов теоретического курса, анализ конкретных ситуаций и подготовку их презентаций.

Самостоятельная работа осуществляется в индивидуальном и групповом формате. Самостоятельная работа выполняется обучающимися на основе учебно-методических материалов дисциплины (приложение 2). Самостоятельно изучаемые вопросы курса включаются в экзаменационные вопросы.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература (библиотека Вавиловского университета):

№ п/п	Наименование, ссылка для электронного доступа или количество экземпляров в библиотеке	Автор(ы)	Место издания, издательство, год	Используется при изучении разделов (из п.4 табл. 3)
1	Системы искусственного интеллекта: учебное пособие https://e.lanbook.com/book/427532	Ю. А. Степанов, А. В. Вылегжанина, Л. Н. Бурмин.	Кемерово: Кем ГУ, 2024. — 102 с. — ISBN 978-5-8353-3166-6.	1 – 12

2	Программирование на C++ в примерах и задачах https://pdfroom.com/books/programmirovanie-na-c-v-primerax-i-zadacax/qXgenBQY26P/download	А.Н. Васильев	Москва: Изд-во «Э», 2020.-368 с.- ISBN 978-5-699-87445-3	13 – 24
3	Обработка данных средствами электронных таблиц: учебно-методическое пособие. https://e.lanbook.com/book/172096	Н.В. Петракова	Брянск: Брянский ГАУ, 2020. — 60 с. — ISBN 978-5-8353-3166-6.	24 – 38

б) дополнительная литература (ЭБС)

№ п/п	Наименование, ссылка для электронного доступа или количество экземпляров в библиотеке	Автор(ы)	Место издания, издательство, год	Используется при изучении разделов (из п.4 табл. 3)
1	Программирование на Python: учебно-методическое пособие https://e.lanbook.com/book/420758	О.А. Сергеева	Кемерово: КемГУ, 2024	Все разделы
2	Теория информации: учебник для вузов. https://e.lanbook.com/book/126940	И.Ю. Попов, И.В. Блинова	Санкт-Петербург: Лань, 2021. – 444 с.ISBN 978-5-8114-4204-1	Основы защиты информации

в) ресурсы информационно-телекоммуникационной сети «Интернет»

Для освоения дисциплины рекомендуются следующие сайты информационно-коммуникационной сети «Интернет»:

- Официальный сайт университета: www.vavilovsar.ru;
- форум по профессиональным приемам работы в Microsoft Excel, ссылка доступа – https://forum.msexcel.ru;
- математическая интернет-школа, ссылка доступа – http://gendocs.ru;

- подробные авторские руководства по продуктам MathWorks, ссылка доступа – http://matlab.exponenta.ru
- интернет-решения для бизнеса, ссылка доступа – http://www.rusweb.org;
- бизнес-школа ЛИНК, ссылка доступа –http://www.schoollink.org

г) периодические издания

образовательный математический портал, ссылка доступа – http: // www.exponenta.ru

д) информационные справочные системы и профессиональные базы данных:

Для пользования стандартами и нормативными документами рекомендуется применять информационные справочные системы и профессиональные базы данных, доступ к которым организован библиотекой университета через локальную вычислительную сеть.

Для пользования электронными изданиями рекомендуется использовать следующие информационные справочные системы и профессиональные базы данных:

1. Научная библиотека университета https://www.vavilovsar.ru/biblioteka

Базы данных содержат сведения о всех видах литературы, поступающей в фонд библиотеки. Более 1400 полнотекстовых документов (учебники, учебные пособия и т.п.) (доступ: с любого компьютера, подключенного к сети Internet).

2. Электронная библиотечная система «Лань» https://e.lanbook.com

Электронная библиотека издательства «Лань» – ресурс, включающий в себя как электронные версии книг издательства «Лань», так и коллекции полнотекстовых файлов других российских издательств (доступ: после регистрации с компьютера университета с любого компьютера, подключенного к сети Internet).

3. ЭБС IPR SMART http://iprbookshop.ru

ЭБС обеспечивает возможность работы с постоянно пополняемой базой лицензионных изданий (более 40000) по широкому спектру дисциплин – учебные, научные издания и периодика, представленные более 600 федеральными, региональными и вузовскими издательствами, научно-исследовательскими институтами и ведущими авторскими коллективами (доступ: после регистрации с компьютера университета с любого компьютера, подключенного к сети Internet).

4. ЭБС Znanium https://znanium.ru

Фонд ЭБС Znanium постоянно пополняется электронными версиями изданий, публикуемых Научно-издательским центром ИНФРА-М, коллекциями книг и журналов других российских издательств, а также произведениями отдельных авторов (доступ: с любого компьютера, подключенного к сети Internet; свободная регистрация).

5. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

Российский информационный портал в области науки, медицины, технологии и образования. На платформе аккумулируются полные тексты и рефераты научных статей и публикаций (доступ: с любого компьютера, подключенного к сети Internet; свободная регистрация).

е) информационные технологии, используемые при осуществлении образовательного процесса:

в учебном процессе по дисциплине «Информационная безопасность» используются следующие технические средства информационных технологий:

- высокопроизводительные персональные компьютеры, с помощью которых осуществляется доступ к информационным ресурсам сети Интернет, выполняются расчеты и моделирование и оформляются результаты самостоятельной работы;
- видеопроекторы и экраны для демонстрации слайдов и видеофрагментов мультимедийных презентаций;
- средства телекоммуникаций: электронная почта, мессенджеры, социальные сети и т.п.

- **программное обеспечение:**

№ п/п	Наименование раздела учебной дисциплины (модуля)	Наименование программы	Тип программы
1	2	3	4
1	Все разделы дисциплины	*Вспомогательное программное обеспечение:* **«Р7-Офис»** Предоставление неисключительных прав на программное обеспечение «Р7-Офис». Лицензиат – ООО «Солярис Технолоджис», г. Саратов. Договор № ЦЗ-1К-033 от 21.12.2022 г. Срок действия договора: с 01.01.2023 г. Лицензия на 3 года с правом последующего бессрочного использования, для образовательных учреждений.	Вспомогательная
2	Все разделы дисциплины	*Вспомогательное программное обеспечение:*	Вспомогательная

		Kaspersky Endpoint Security (антивирусное программное обеспечение). Лицензиат – ООО «Солярис Технолоджис», г. Саратов. Сублицензионный договор № 6-1128/2023/КСП-107 от 11.12.2023 г. Срок действия договора: 01.01.2024–31.12.2024 г.	

7. Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа используется помещение № 402, оборудованное меловыми и маркерными досками, мультимедийным проектором, экраном, аудиосистемой, средствами частичного затемнения дневного света.

Для выполнения лабораторных работ имеются лаборатории №№ 520, 522 с современными аппаратно-программными комплексами и предустановленным лицензионным программным обеспечением, указанным выше. Компьютеры подключены к сети «Интернет» и обеспечивают свободный доступ в электронную информационно-образовательную среду университета.

8. Оценочные материалы

Оценочные материалы, сформированные для проведения, текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине «Информационная безопасность» разработаны на основании следующих документов:

- Федерального закона Российской Федерации от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);
- приказа Министерства науки и высшего образования РФ от 6 апреля 2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

Оценочные материалы представлены в приложении 1 к рабочей программе дисциплины и включают в себя:

- перечень компетенций с указание этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы

формирования компетенций в процессе освоения образовательной программы;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

9. Учебно-методическое обеспечение самостоятельной работы

Перечень учебно-методического обеспечения самостоятельной работы представлен в приложении 2 к рабочей программе по дисциплине «Информационная безопасность».

10. Методические указания для обучающихся по изучению дисциплины «Информационная безопасность»

Методические указания по изучению дисциплины «Информационная безопасность» включают в себя:

1. Краткий курс лекций (Приложение 3)
2. Методические указания по выполнению лабораторных работ (Приложение 4)

Рассмотрено и утверждено на заседании кафедры «Цифровое управление процессами в АПК»
«_12_» _апреля_2024_года (протокол № 10а).