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. /	_____ / Шишурин С.А./
«12» 04 2024 г.	«12» 04 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина	**ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ**
Направление подготовки	**09.03.03 Прикладная информатика**
Направленность (профиль)	**Проектирование информационных систем**
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 вычислительных системах

2. Место дисциплины в структуре ОПОП ВО

В соответствии с учебным планом по направлению подготовки 09.03.03 Прикладная информатика, направленность (профиль) Проектирование информационных систем «Введение в информационную безопасность» относится к обязательной части Блока 1.

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

Дисциплина «Введение в информационную безопасность» является базовой для изучения дисциплины «Проектирование информационных систем».

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	ОПК-2	способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.2. понимает принципы работы в информационной среде и решает типовые задачи управления бизнес-процессами с применением цифровых технологий	принципы работы современных информационных технологий и программных средств	использовать программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	навыками решения типовых задач управления бизнес-процессами с применением цифровых технологий
2	ОПК-3	способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Применяет информационно-коммуникационные технологии с учетом основных требований информационной безопасности для решения стандартных задач в области прикладной информатики	основы информационной и библиографической культуры в области прикладной информатики	решать стандартные задачи в области прикладной информатики	навыками решения стандартных задач в области прикладной информатики с учетом основных требований информационной безопасности
			ОПК-3.2. Разрабатывает меры защиты информации на основе требований	нормы и правила обеспечения информационной безопасности в сфере	разрабатывать техническую документацию, связанную с информационной	навыками разработкимер защиты информации на основе требований

№ 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
			информационной безопасности и нормативно-правовой базы	своей профессио-нальной деятельно-сти	безопасностью в области прикладной информатики	информационной безопасности и нормативно-правовой базы

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.	36,1		36,1						
аудиторная работа:	36		36						
лекции	18		18						
лабораторные	18		18						
практические									
промежуточная аттестация	0,1		0,1						
контроль									
Самостоятельная работа	71,9		71,9						
Форма итогового контроля	Зач.		Зач.						
Курсовой проект (работа)	-		-						

Таблица 3

Структура и содержание дисциплины
«Введение в информационную 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
2 семестр								
1.	Введение в информационную безопасность: основные понятия и определения. Системный подход к обеспечению информационной безопасности	1	Л	Т	2	4	ТК	УО
2.	Техника безопасности при работе на персональных ЭВМ. Анализ периодических источников по тематике	2	ЛЗ	Т	2	4	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
	обеспечения информационной безопасности.							
3.	Роль информационного ресурса в обществе. Проблемы обеспечения информационной безопасности.	3	Л	В	2	4	ТК	УО
4.	Лабораторная работа №1.1. Средства обеспечения защиты информации в системах электронного документооборота.	4	ЛЗ	Т	2	4	ТК	УО
5	Классификация источников опасности. Характеристика угроз в зависимости от вида источника. Угрозы конфиденциальности и целостности информации.	5	Л	Т	2	4	ТК	УО
6.	Лабораторная работа №1.2. Установка и снятие паролей на текстовые документы, папки, архивы.	6	ЛЗ	Т	2	4	РК	УО, Д, Тс
7.	Понятие политики безопасности. Задачи, решаемые политикой безопасности. Основные принципы политики безопасности	7	Л	В	2	4	ТК	УО
8.	Лабораторная работа №2.1. Средства и способы анализа трафика на сетевых интерфейсах в ОС Windows. Изучение настроек Ethernet для повышения безопасности	8	ЛЗ	Т	2	4	ТК	УО
9.	Цели создания политики безопасности. Субъектно-объектная модель информационной системы	9	Л	В	2	4	ТК	УО
10.	Лабораторная работа №2.2. Назначение прав пользователей при произвольном управлении доступом в ОС Windows	10	ЛЗ	Т	2	4	ТК	УО
11.	Понятия состояния системы и потока информации. Правила разграничения доступа	11	Л	Т	2	4	ТК	УО
12.	Лабораторная работа №3.1. Реализация модели политики безопасности посредством управления доступом.	12	ЛЗ	М	2	4	РК	УО, Д, Тс
13.	Политика избирательного доступа. Матрица управления доступом. Принудительное управление доступом.	13	Л	В	2	4	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
	Добровольное управление доступом.							
14.	Лабораторная работа №3.2. Реализация модели политики безопасности на основе матрицы доступа	14	ЛЗ	М	2	4	ТК	УО
15.	Политика полномочного доступа. Метки секретности, уровень прозрачности. Текущее значение уровня безопасности.	15	Л	Т	2	4	ТК	УО
16.	Лабораторная работа №4.1. Изучение сетевых средств защиты операционной системы MS Windows. Протоколирование и аудит	16	ЛЗ	Т	2	4	ТК	УО
17.	Правовая защита. Правовая защита на международном уровне и на уровне Российской Федерации.	17	Л	Т	2	1	ТК	УО
18.	Лабораторная работа №4.2. Диагностика защищенности информации в сети средствами операционной системы	18	ЛЗ	Т	2	1	РК	УО, Д, Тс
Выходной контроль					0,1	1,9	ВыхК	З
Итого:					36,1	71,9		

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 «Введение в информационную безопасность» проводится по видам учебной работы: лекции, лабораторные занятия, текущий контроль. Реализация компетентностного подхода в рамках направления подготовки 09.03.03 Прикладная информатика, для профиля подготовки Проектирование информационных систем, 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 пакетов специализированных прикладных программ и информационных ресурсов глобальной сети Интернет в перспективных направлениях прикладной 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	2	3	4	5
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 – 6
2	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.	7 - 12
3	Системы поддержки принятия решений: учебное пособие для вузов. 2-е изд., стер. https://e.lanbook.com/book/176903	А. В. Макшанов, А. Е. Журавлев, Л. Н. Тындыкарь.	Санкт-Петербург: Лань, 2021. — 108 с. — ISBN 978-5-8114-8489-8.	13 – 18

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	2	3	4	5
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	Все разделы

в) ресурсы информационно-телекоммуникационной сети «Интернет»

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

1. Официальный сайт университета: https://www.vavilovsar.ru/;
2. 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).

3. 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).

4. 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).

5. 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).

6. 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).

г) периодические издания

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

д) информационно-справочные системы и профессиональные базы данных

«Гарант», ссылка доступа – www.garant.ru

«Консультант Плюс», ссылка доступа – www.consultant.ru

е) технические средства, используемые при осуществлении образовательного процесса:

в учебном процессе по дисциплине «Введение в информационную 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 лекций;
- 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 «СолярисТехнолоджис», 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:* **KasperskyEndpointSecurity** (антивирусное программное обеспечение). Лицензиат – ООО «СолярисТехнолоджис», г. Саратов. Сублицензионный договор № 6-1128/2023/КСП-107 от 11.12.2023 г. Срок действия договора: 01.01.2024–31.12.2024 г.	Вспомогательная

№ п/п	Наименование раздела учебной дисциплины (модуля)	Наименование программы	Тип программы
1	2	3	4
3	Все разделы дисциплины	*Вспомогательное программное обеспечение:* **Адаптация и сопровождение экземпляров систем КонсультантПлюс:** Справочная Правовая Система КонсультантПлюс Исполнитель: ООО «Принцип», г. Саратов Договор адаптации и сопровождения экземпляров систем КОНСУЛЬТАНТ ПЛЮС № 24-123/223-056 от 01.02.2024 г. Срок действия договора: 01 января – 31 декабря 2024 года.	Вспомогательная
4	Все разделы дисциплины	*Вспомогательное программное обеспечение:* **Предоставление экземпляровтекущих версий специальных информационных массивов** электронного периодического справочника «Система ГАРАНТ». Исполнитель – ООО «Сервисная Компания «Гарант-Саратов», г. Саратов. Договор об оказании информационных услуг № С-3951/223-024 от 09.01.2024 г. Срок действия договора: 01 января – 30 ноября 2024 года.	Вспомогательная

7. Материально-техническое обеспечение дисциплины

Для проведения учебных занятий по данной дисциплине используются учебные аудитории № 522, Кванториум (малая аудитория), Кванториум (большая аудитория), 113, 311, 313, 315, № 114 (Киберфизическая лаборатория)

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения: для демонстрации медиаресурсов имеются проектор, экран, компьютер или ноутбук: https://vavilovsar.ru/sveden/objects/cabinets/study_rooms.html, https://vavilovsar.ru/sveden/objects/cabinets/practice_rooms.html .

Помещения для самостоятельной работы обучающихся (№ 522, Кванториум (малая аудитория), Кванториум (большая аудитория), 113 (класс ВОИР), 311, 313, структурное поздразделение "Инжиниринговый центр" (центр агроробототехники и VR/AR технологий), структурное поздразделение "Инжиниринговый центр" (студенческое конструкторское бюро) и читальный зал библиотеки) оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета:
https://vavilovsar.ru/sveden/objects/cabinets/study_rooms.html,
https://vavilovsar.ru/sveden/objects/cabinets/practice_rooms.html .

8. Оценочные материалы

Оценочные материалы, сформированные для проведения, текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине «Введение в информационную 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 06.04.2021 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 «Введение в информационную безопасность».

10. Методические указания для обучающихся по изучению дисциплины «Введение в информационную безопасность»

Методические указания по изучению дисциплины «Введение в информационную 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).