

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Соловьев Дмитрий Александрович

Должность: ректор ФГБОУ ВО Саратовский университет

Дата подписания: 14.03.2025 15:13:47


Уникальный программный ключ:

528682d78e671e5f7601f72f735a12

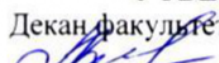


МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовский государственный университет генетики, биотехнологии и инженерии имени Н.И. Вавилова»

СОГЛАСОВАНО

И.о. заведующего кафедрой
 / Ключиков А.В. /
« 12 » 04 2024 г.

УТВЕРЖДАЮ

Декан факультета
 / Волощук Л.А. /
« 12 » 04 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина	УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИТ- ПРЕДПРИЯТИЯ
Направление подготовки	38.04.05 Бизнес-информатика
Направленность (профиль)	Управление бизнес анализом
Квалификация выпускника	Магистр
Нормативный срок обучения	2 года
Форма обучения	Очная

Разработчик: доцент, Розанов А.В.


(подпись)

Саратов 2024

1. Цель освоения дисциплины

Целью изучения дисциплины является формирование у обучающихся навыков управления безопасностью ИТ-предприятия, обеспечения защиты информации и безопасного использования программных средств в современных информационных и телекоммуникационных системах

2. Место дисциплины в структуре ОПОП ВО

В соответствии с учебным планом по направлению подготовки 38.04.05 Бизнес-информатика, направленность (профиль) Управление бизнес анализом, дисциплина «Управление безопасностью ИТ-предприятия» относится к части Блока 1, формируемой участниками образовательных отношений.

Для изучения дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Искусственный интеллект в бизнес среде» и «Наука о данных для бизнеса».

Дисциплина «Управление безопасностью ИТ-предприятия» является базовой для изучения дисциплины: «Управление рисками»

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-2	способен собирать информацию, выбирать рациональные ИС и ИКТ-решения для управления бизнесом, разрабатывать стратегию развития архитектуры предприятия	ПК-2.2. выбирает рациональные ИС и ИКТ-решения для управления бизнесом	рациональные информационные системы (ИС) и информационно-коммуникационные (ИКТ) решения для безопасного управления бизнесом	собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности	навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности 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
Контактная работа – всего, в т.ч.	32,1			32,1	
<i>аудиторная работа:</i>	32			32	
лекции	16			16	
лабораторные	16			16	
Лабораторные					
<i>промежуточная аттестация</i>	0,1			0,1	
<i>контроль</i>					
Самостоятельная работа	75,9			75,9	
Форма итогового контроля	Зач.			Зач.	
Курсовой проект (работа)	-			-	

Таблица 3

Структура и содержание дисциплины «Управление безопасностью IT-предприятия»

№ 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
3 семестр								
1.	Управление безопасностью IT-предприятия: основные понятия и определения. Системный подход к обеспечению информационной безопасности	1	Л	В	2	4	ТК	УО
2.	Техника безопасности при работе на персональных ЭВМ. Лабораторная работа №1. Средства обеспечения защиты информации в системах электронного документооборота.	2	ЛЗ	Т	2	4	ВК	Тс

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самосто- ятель- ная ра- бота	Контроль знаний	
			Вид занятия	Форма про- ведения	Количество часов		Количество часов	Вид
1	2	3	4	5	6	7	8	9
3.	Классификация источников опасности. Характеристика угроз конфиденциальности и целостности информации	3	Л	Т	2	4	ТК	УО
4.	Лабораторная работа №2. Средства и способы анализа трафика на сетевых интерфейсах в ОС Windows. Изучение настроек Ethernet для повышения безопасности	4	ЛЗ	М	2	4	ТК	УО
5.	Понятие политики безопасности. Задачи, решаемые политикой безопасности. Основные принципы политики безопасности	5	Л	В	2	4	ТК	УО
6.	Лабораторная работа №3. Реализация модели политики безопасности посредством управления доступом. Управление доступом в ОС Windows	6	ЛЗ	Т	2	6	РК	УО, Д, Тс
7.	Политика избирательного доступа. Принудительное и добровольное управление доступом	7	Л	Т	2	4	ТК	УО
8.	Лабораторная работа №4. Изучение сетевых средств защиты операционной системы MS Windows. Протоколирование и аудит	8	ЛЗ	Т	2	4	ТК	УО
9.	Правовая защита на международном уровне и на уровне Российской Федерации. Законы Российской Федерации в области информационной безопасности. Организационная защита.	9	Л	Т	2	4	ТК	УО
10.	Лабораторная работа №5. Анализ защищенности. Защита от потери и отказов программно-аппаратных средств. Изучение встроенных средств диагностики - WMIC.	10	ЛЗ	Т	2	4	ТК	УО
11.	Классификация угроз информационным системам. Случайные угрозы. Преднамеренные угрозы. Шпионаж и диверсии.	11	Л	В	2	6	РК	УО, Д, Тс
12.	Лабораторная работа №6. Шифрование и дешифрование средствами табличного процессора MS Excel.	12	ЛЗ	Т	2	4	ТК	Тс
13.	Криптографические методы защиты информации. Методы моноалфавитной подстановки. Полиалфавитная подстановка	13	Л	Т	2	6	РК	УО
14.	Лабораторная работа №7. Использование межсетевых экранов (брандмауэров) и файрволов для защиты информации в сетях	14	ЛЗ	Т	2	4	ТК	УО
15.	Программные средства защиты информации в компьютерных сетях. Аппаратные средства обеспечения кибербезопасности	15	Л	Т	2	4	ТК	УО

№ п/п	Тема занятия. Содержание	Неделя семестра	Контактная работа			Самосто- ятель- ная ра- бота	Контроль знаний	
			Вид занятия	Форма про- ведения	Количество часов		Количество часов	Вид
1	2	3	4	5	6	7	8	9
16.	Лабораторная работа №8. Установка и настройка параметров антивирусных программ Касперский, Dr. Web, Avast, Eset NOD32	16	ЛЗ	Т	2	6	ПК	УО, Д, Тс,
Выходной контроль					0,1	5,9	ВыхК	3
Итого:					32,1	75,9		

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 «Управление безопасностью IT-предприятия» проводится по видам учебной работы: лекции, Лабораторные занятия, текущий контроль. Реализация компетентного подхода в рамках направления подготовки 38.04.05 Бизнес-информатика, для профиля подготовки Управление бизнес анализом, 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 проводятся 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 лабораторных 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 современный 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 вопросы выходного контроля.

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 – 5

№ 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
2	Программирование на C++ в примерах и задачах https://pdfroom.com/books/programming-na-c-v-primerax-i-zadacax/qXgenBQY26P/download	А.Н. Васильев	Москва: Изд-во «Э», 2020.-368 с.- ISBN 978-5-699-87445-3	6 – 12
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.	13 – 16

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 «Управление безопасностью IT-предприятия» 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 видеоснимков 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
2	Все разделы дисциплины	<i>Вспомогательное программное обеспечение:</i> «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
№ п/п	Наименование раздела учебной дисциплины (модуля)	Наименование программы	Тип программы
1	2	3	4

3	Все разделы дисциплины	<p><i>Вспомогательное программное обеспечение:</i></p> <p>Kaspersky Endpoint Security (антивирусное программное обеспечение).</p> <p>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.</p>	Вспомогательная
4	Все разделы дисциплины	<p><i>Вспомогательное программное обеспечение:</i></p> <p>Адаптация и сопровождение экземпляров систем КонсультантПлюс: Справочная Правовая Система КонсультантПлюс Исполнитель: ООО «Принцип», г. Саратов</p> <p>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.</p>	Вспомогательная
5	Все разделы дисциплины	<p><i>Вспомогательное программное обеспечение:</i></p> <p>Предоставление экземпляров текущих версий специальных информационных массивов электронного периодического справочника «Система ГАРАНТ».</p> <p>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.</p>	Вспомогательная

7. Материально-техническое обеспечение дисциплины

Для проведения занятий лекционного типа используется помещение №422, оборудованное меловыми и маркерными досками, мультимедийным проектором, экраном, аудиосистемой, средствами частичного затемнения дневного света.

Для выполнения лабораторных работ имеются лаборатории №№ 134, 134а 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 «Управление безопасностью IT-предприятия», 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 указанием 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 «Управление безопасностью IT-предприятия».

10. Методические указания для обучающихся по изучению дисциплины «Управление безопасностью IT-предприятия»

Методические указания по изучению дисциплины «Управление безопасностью IT-предприятия» 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).