Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 16.06.2026 08:52:07
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Бюджетное учреждение высшего образования
Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

11 июня 2026 г., протокол УМС №5

Управление корпоративной информационной безопасностью

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Менеджмента и бизнеса**

Учебный план b380305-БизИнфор-26-4.plx
38.03.05 Бизнес-информатика
Направленность (профиль): Экономика предприятий и управление бизнес- процессами

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 56
самостоятельная работа 88
часов на контроль 36

Виды контроля в семестрах:
экзамен 8
контрольная работа 8
зачет 7
курсовой проект 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	17 2/6		9 1/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	8	8	24	24
Практические	16	16	16	16	32	32
Итого ауд.	32	32	24	24	56	56
Контактная работа	32	32	24	24	56	56
Сам. работа	40	40	48	48	88	88
Часы на контроль			36	36	36	36
Итого	72	72	108	108	180	180

Программу составил(и):
к.э.н., доцент, Курамшина Алсу Винировна

Рабочая программа дисциплины
Управление корпоративной информационной безопасностью

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.05 Бизнес-информатика (приказ Минобрнауки России от 29.07.2020 г. № 838)

составлена на основании учебного плана:
38.03.05 Бизнес-информатика
Направленность (профиль): Экономика предприятий и управление бизнес-процессами
утвержденного учебно-методическим советом вуза от 11.06.2026 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Менеджмента и бизнеса

Зав. кафедрой д.э.н., доцент Ширинкина Е.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	сформировать компетенции в области корпоративной информационной безопасности для построения системы противодействия угрозам деятельности компании

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Цифровая грамотность
2.1.3	Информационные технологии в бизнесе
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Управление инновационными проектами
2.2.2	Управление бизнес-проектами в ИТ-сфере
2.2.3	Реинжиниринг бизнес-процессов
2.2.4	Управление производственными системами

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-7.1: Способен использовать цифровые технологии и инструменты работы с информацией с целью удовлетворения личных, образовательных и профессиональных потребностей

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	-Основные понятия и определения в области информационной безопасности (ИБ);
3.1.2	- Нормативно-правовую базу РФ в сфере ИБ;
3.1.3	- Типологию и характеристики угроз ИБ;
3.1.4	- Принципы и модели управления рисками ИБ;
3.1.5	- Архитектуру и компоненты системы защиты информации (СЗИ);
3.1.6	- Процессы и процедуры ИБ в организации
3.2	**Уметь:**
3.2.1	Анализировать ИТ-инфраструктуру организации на предмет уязвимостей:
3.2.2	Оценивать риски ИБ
3.2.3	Участвовать в разрабатке и внедрении политики и регламенты ИБ:
3.2.4	Подбирать технические средства защиты под конкретные угрозы и бюджет;
3.2.5	Учитывать требования регуляторов и стандартов.
3.2.6	Организовывать мониторинг и реагирование на инциденты:

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Примечание**
	Раздел 1. Основы корпоративной ИБ					
1.1	Основы корпоративной ИБ /Лек/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
1.2	Основы корпоративной ИБ /Пр/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	

1.3	Основы корпоративной ИБ /Ср/	7	10	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
	Раздел 2. Стандарты и фреймворки ИБ					
2.1	Стандарты и фреймворки ИБ /Лек/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
2.2	Стандарты и фреймворки ИБ /Пр/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
2.3	Стандарты и фреймворки ИБ /Ср/	7	10	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
	Раздел 3. Управление рисками ИБ					
3.1	Управление рисками ИБ /Лек/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
3.2	Управление рисками ИБ /Ср/	7	10	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
3.3	Управление рисками ИБ /Пр/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
	Раздел 4. Организация службы ИБ					
4.1	Организация службы ИБ /Лек/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
4.2	Организация службы ИБ /Ср/	7	10	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
4.3	Организация службы ИБ /Пр/	7	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
4.4	Управление корпоративной информационной безопасностью /КП/	7	0	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	требования и темы курсового проекта
4.5	Управление корпоративной информационной безопасностью /Зачёт/	7	0	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	теоретические вопросы, практическое задание

	Раздел 5. Технические средства защиты					
5.1	Технические средства защиты /Лек/	8	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
5.2	Технические средства защиты /Пр/	8	6	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
5.3	Технические средства защиты /Ср/	8	18	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
	Раздел 6. Управление инцидентами ИБ					
6.1	Управление инцидентами ИБ /Лек/	8	2	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2	
6.2	Управление инцидентами ИБ /Пр/	8	4	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
6.3	Управление инцидентами ИБ /Ср/	8	14	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
	Раздел 7. Аудит и непрерывность бизнеса					
7.1	Аудит и непрерывность бизнеса /Лек/	8	2	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
7.2	Аудит и непрерывность бизнеса /Пр/	8	6	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
7.3	Аудит и непрерывность бизнеса /Ср/	8	16	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	
	Раздел 8. Управление корпоративной информационной безопасностью					
8.1	Управление корпоративной информационной безопасностью /Контр.раб./	8	0	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	задания для контрольной работы
8.2	Управление корпоративной информационной безопасностью /Экзамен/	8	36	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3	теоретические вопросы, практическое задание

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации
Представлены отдельным документом
5.2. Оценочные материалы для диагностического тестирования
Представлены отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Астапчук В. А., Терещенко П. В.	Корпоративные информационные системы: требования при проектировании: учебник для вузов	Москва: Юрайт, 2026, электронный ресурс	1
Л1.2	Зенков А. В.	Информационная безопасность и защита информации: учебник для вузов	Москва: Юрайт, 2026, электронный ресурс	1
Л1.3	Суворова Г. М.	Информационная безопасность: учебник для вузов	Москва: Юрайт, 2026, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие для вузов	Санкт-Петербург: Лань, 2025, электронный ресурс	1
Л2.2	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2026, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Богач М. А., Дроздова А. А., Мойсеенкова М. А.	Цифровая грамотность: учебно-методическое пособие	Сургут: Издательский центр СурГУ, 2023, электронный ресурс	1
Л3.2	Осин А. В., Хализев К. А.	Технологии обеспечения информационной безопасности больших данных в компьютерных сетях. Информационная безопасность в системах обработки данных на примере Hadoop и Spark: учебно-методическое пособие по выполнению лабораторных работ для магистров, направление подготовки 10.04.01 «информационная безопасность», профиль «интеллектуальные технологии безопасности компьютерных систем»	Москва: МТУСИ, 2025, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Административно-управленческий портал (полнотекстовые базы) http://www.aup.ru/
Э2	Журнал «Вопросы экономики» www.vopreco.ru
Э3	Статьи по управленческой экономике http://cyberleninka.ru/

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет прикладных программ Microsoft Office

6.3.2 Перечень информационных справочных систем

6.3.2.1	Информационно-правовой портал Гарант.ру http://www.garant.ru
6.3.2.2	Справочно-правовая система Консультант Плюс http://www.consultant.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (лабораторных занятий), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации оснащена: комплект специализированной учебной мебели, маркерная (меловая) доска, комплект переносного мультимедийного оборудования - компьютер, проектор, проекционный экран, компьютеры с возможностью выхода в Интернет и доступом в электронную информационно-образовательную среду. Обеспечен доступ к сети Интернет и в электронную информационную среду организации.