МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

_____

«___»_____ 2024г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Реагирование на инциденты информационной безопасности
направление подготовки:	09.03.01 Информатика и вычислительная техника
направленность (профиль):	Информационная безопасность компьютерных систем и сетей
форма обучения:	Очная

Рабочая программа рассмотрена на заседании кафедры математики и прикладных информационных технологий

Протокол №____от_____2024г.

1. Цели и задачи освоения дисциплины

1. Цель освоения дисциплины: овладение теоретическими знаниями и практическими умениями, развитие навыков практических действий по реагированию на инциденты информационной безопасности.

Задачи освоения дисциплины:

- изучение нормативных правовых и организационных основ менеджмента инцидентов информационной безопасности;
- изучение методов обнаружения, оповещения об инцидентах информационной безопасности и их оценки;
- приобретение умений реагирования на инциденты информационной безопасности;
- приобретение навыков извлечения уроков из инцидентов информационной безопасности, введения превентивных защитных мер и улучшения общего подхода к менеджменту инцидентов информационной безопасности;
- развитие исследовательских и аналитических навыков, интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

- знание теоретических основ информационных и сетевых технологий и информационной безопасности;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины является логическим продолжением содержания дисциплины «Основы информационной безопасности» и может служить основой для прохождения учебной и производственной практик, подготовки к выполнению выпускной квалификационной работы и профессиональной деятельности.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
ПКС-1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать (З1) теоретические основы менеджмента инцидентов информационной безопасности
		Уметь (У1) планировать восстановление сетевой инфокоммуникационной системы после инцидентов ИБ; документировать ошибки в работе сетевых устройств и программного обеспечения, приводящие к инцидентам ИБ
		Владеть (В1) практическими навыками реагирования на инциденты ИБ; введения превентивных защитных мер
ПКС-3. Способен проводить оценку уровня безопасности компьютерных систем и	ПКС-3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые	Знать (З2) теоретические основы реагирования на инциденты информационной безопасности

сетей, а также проводить тестирование программного обеспечения на защищенность.	случаи, управляет процессом тестирования программного обеспечения.	Уметь (У2) планировать и организовывать мероприятия по обнаружению и оповещению инцидентов ИБ
		Владеть (В2) практическими навыками оценки инцидентов ИБ и извлечения уроков из них

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	4/7	16	-	30	62	-	Зачет

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Контроль, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.					
1	1	Правовые и организационные основы менеджмента инцидентов информационной безопасности	3	-	5	11	-	19	ПКС-1.1 ПКС-3.1	Задания на лабораторную работу
2	2	Планирование и подготовка менеджмента инцидентов информационной безопасности	4	-	7	13	-	24		
3	3	Использование системы менеджмента инцидентов информационной безопасности	3	-	6	13	-	22		
4	4	Анализ состояния информационной безопасности	3	-	6	13	-	22		
5	5	Улучшение процессов менеджмента инцидентов информационной безопасности	3	-	6	12	-	21		
6	Зачет		-	-	-	-	-	-	ПКС-1.1 ПКС-3.1	Вопросы к зачету
Итого:			16	-	30	62	-	108	X	X

заочная форма обучения (ЗФО): не реализуется

очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Правовые и организационные основы менеджмента инцидентов информационной безопасности. Общие положения. Цели. Этапы. Преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности. Примеры инцидентов информационной безопасности и их причин. ИСО/МЭК 13335–2:1998. ИСО/МЭК ТО 15947:2002. ИСО/МЭК ТО 18043:2002. ИСО/МЭК ТО 18044–2007.

Раздел 2. Планирование и подготовка менеджмента инцидентов информационной безопасности. Общее представление о менеджменте инцидентов информационной безопасности. Политика менеджмента инцидентов информационной безопасности. Программа менеджмента инцидентов информационной безопасности. Политики менеджмента рисков и информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Техническая и другая поддержка реагирования на инциденты информационной безопасности. Обеспечение осведомленности и обучение.

Раздел 3. Использование системы менеджмента инцидентов информационной безопасности. Обзор ключевых процессов. Обнаружение и оповещение о событиях информационной безопасности. Оценка и принятие решений по событиям/инцидентам. Реагирование на инциденты.

Раздел 4. Анализ состояния информационной безопасности. Дальнейшая правовая экспертиза. Извлеченные уроки. Определение улучшений безопасности. Определение улучшений системы.

Раздел 5. Улучшение процессов менеджмента инцидентов информационной безопасности. Улучшение анализа рисков и менеджмента безопасности. Осуществление улучшений безопасности. Осуществление улучшений системы.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	3	-	-	Правовые и организационные основы менеджмента инцидентов информационной безопасности
2	2	4	-	-	Планирование и подготовка менеджмента инцидентов информационной безопасности
3	3	3	-	-	Использование системы менеджмента инцидентов информационной безопасности
4	4	3	-	-	Анализ состояния информационной безопасности
5	5	3	-	-	Улучшение процессов менеджмента инцидентов информационной безопасности
Итого:		16	-	-	-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	5	-	-	Правовые и организационные основы менеджмента

					инцидентов информационной безопасности
2	2	7	-	-	Планирование и подготовка менеджмента инцидентов информационной безопасности
3	3	6	-	-	Использование системы менеджмента инцидентов информационной безопасности
4	4	6	-	-	Анализ состояния информационной безопасности
5	5	6	-	-	Улучшение процессов менеджмента инцидентов информационной безопасности
Итого:		30	-	-	-

Практические занятия

Практические занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	11	-	-	Правовые и организационные основы менеджмента инцидентов информационной безопасности	Подготовка к лабораторным работам
2	2	13	-	-	Планирование и подготовка менеджмента инцидентов информационной безопасности	Подготовка к лабораторным работам
3	3	13	-	-	Использование системы менеджмента инцидентов информационной безопасности	Подготовка к лабораторным работам
4	4	13	-	-	Анализ состояния информационной безопасности	Подготовка к лабораторным работам
5	5	12	-	-	Улучшение процессов менеджмента инцидентов информационной безопасности	Подготовка к лабораторным работам
6	1-5	-	-	-	Зачет	Подготовка к зачету
Итого:		62	-	-		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

– ИКТ – технологии (визуализация учебного материала в PowerPoint в диалоговом режиме);
– обучение в сотрудничестве (коллективная, групповая работа);
– технология проблемного обучения.

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Лабораторная работа № 1	0-15
2	Лабораторная работа № 2	0-15
	ИТОГО за первую текущую аттестацию	**0-30**
2 текущая аттестация		
3	Лабораторная работа № 3	0-15
4	Лабораторная работа № 4	0-15
	ИТОГО за вторую текущую аттестацию	**0-30**
3 текущая аттестация		
5	Лабораторная работа № 5	0-40
	ИТОГО за третью текущую аттестацию	**0-40**
	ВСЕГО	**0-100**

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/;
- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;
- Электронно-библиотечная система «ЛАНЬ» https://e.lanbook.com;
- Образовательная платформа ЮРАЙТ www.urait.ru;
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;
- Библиотеки нефтяных вузов России:
  - Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/;
  - Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/;
  - Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
	2	3	4
.	Реагирование на инциденты информационной безопасности	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70.
		Лабораторные занятия: Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям.

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом занятии.

В начале лабораторного занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

Лабораторные занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать знания, подготовиться к научно-исследовательской деятельности. В процессе работы на лабораторных занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, изучение мультимедиалекций, расположенных в свободном доступе, решение ситуационных (профессиональных) задач, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: «Реагирование на инциденты информационной безопасности»
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС-1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать (З1) теоретические основы менеджмента инцидентов информационной безопасности	Не знает теоретические основы менеджмента инцидентов информационной безопасности	Знает на низком уровне теоретические основы менеджмента инцидентов информационной безопасности	Знает на среднем уровне теоретические основы менеджмента инцидентов информационной безопасности	Знает в совершенстве теоретические основы менеджмента инцидентов информационной безопасности
		Уметь (У1) планировать восстановление сетевой инфокоммуникационной системы после инцидентов ИБ; документировать ошибки в работе сетевых устройств и программного обеспечения, приводящие к инцидентам ИБ	Не умеет планировать восстановление сетевой инфокоммуникационной системы после инцидентов ИБ; документировать ошибки в работе сетевых устройств и программного обеспечения, приводящие к инцидентам ИБ	Умеет на низком уровне планировать восстановление сетевой инфокоммуникационной системы после инцидентов ИБ; документировать ошибки в работе сетевых устройств и программного обеспечения, приводящие к инцидентам ИБ	Умеет на среднем уровне планировать восстановление сетевой инфокоммуникационной системы после инцидентов ИБ; документировать ошибки в работе сетевых устройств и программного обеспечения, приводящие к инцидентам ИБ	Умеет в совершенстве планировать восстановление сетевой инфокоммуникационной системы после инцидентов ИБ; документировать ошибки в работе сетевых устройств и программного обеспечения, приводящие к инцидентам ИБ
		Владеть (В1) практическими навыками реагирования на инциденты ИБ; введения превентивных защитных мер	Не владеет практическими навыками реагирования на инциденты ИБ; введения превентивных защитных мер	Владеет на низком уровне практическими навыками реагирования на инциденты ИБ; введения превентивных защитных мер	Владеет на среднем уровне практическими навыками реагирования на инциденты ИБ; введения превентивных защитных мер	Владеет в совершенстве практическими навыками реагирования на инциденты ИБ; введения превентивных защитных мер

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС-3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать (З2) теоретические основы реагирования на инциденты информационной безопасности	Не знает теоретические основы реагирования на инциденты информационной безопасности	Знает на низком уровне теоретические основы реагирования на инциденты информационной безопасности	Знает на среднем уровне теоретические основы реагирования на инциденты информационной безопасности	Знает в совершенстве теоретические основы реагирования на инциденты информационной безопасности
		Уметь (У2) планировать и организовывать мероприятия по обнаружению и оповещению инцидентов ИБ	Не умеет планировать и организовывать мероприятия по обнаружению и оповещению инцидентов ИБ	Умеет на низком уровне планировать и организовывать мероприятия по обнаружению и оповещению инцидентов ИБ	Умеет на среднем уровне планировать и организовывать мероприятия по обнаружению и оповещению инцидентов ИБ	Умеет в совершенстве планировать и организовывать мероприятия по обнаружению и оповещению инцидентов ИБ
		Владеть (В2) практическими навыками оценки инцидентов ИБ и извлечения уроков из них	Не владеет практическими навыками оценки инцидентов ИБ и извлечения уроков из них	Владеет на низком уровне практическими навыками оценки инцидентов ИБ и извлечения уроков из них	Владеет на среднем уровне практическими навыками оценки инцидентов ИБ и извлечения уроков из них	Владеет в совершенстве практическими навыками оценки инцидентов ИБ и извлечения уроков из них

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: «Реагирование на инциденты информационной безопасности»
Код, направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 86 с. —	ЭР*	30	100	+
2	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739	ЭР*	30	100	+

ЭР* – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/

Лист согласования 00ДО-0000761099

Внутренний документ "Реагирование на инциденты информационной безопасности_2024_09.03.01_ИБКСб"

Ответственный: Холманских Светлана Владимировна

Серийный номер ЭП	Должность	ФИО	ИО	Виза	Комментарий
2C 3F F5 AC 0A A7 33 0C	Заведующий кафедрой, имеющий ученую степень доктора наук	Барбаков Олег Михайлович		Согласовано	
14 40 51 AA 91 B6 5C 45	Директор	Каюкова Дарья Хрисановна		Согласовано	
67 20 6F 9B 0D 3A D9 88	Специалист 1 категории		Радичко Диана Викторовна	Согласовано	