МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И ПРОТИВОДЕЙСТВИЕ АТАКАМ НА ОБЪЕКТЫ КИИ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **1**
Семестр: **2**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	2 семестр	Всего	Единицы
Лекционные занятия	28	28	часов
Лабораторные занятия	52	52	часов
в т.ч. в форме практической подготовки	36	36	часов
Самостоятельная работа	64	64	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	180	180	часов
	5	5	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	2

Томск

1. Общие положения

1.1. Цели дисциплины

1. Изучить основные принципы управления инцидентами информационной безопасности.
2. Изучить основы мониторинга инфраструктуры организации, а также формирование знаний о процессах и системах мониторинга.

1.2. Задачи дисциплины

1. Получение студентами знаний о принципах определения событий информационной безопасности (ИБ) как инцидентов ИБ.
2. Получение студентами умений и навыков по оценке и реагированию на идентифицированные инциденты ИБ.
3. Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.
4. Получение студентами умений и навыков нормативному обеспечению управления инцидентами информационной безопасности.
5. Получение студентами умений и навыков планирования, подготовки, использования, анализа и улучшения процесса управления инцидентами информационной безопасности.
6. Получение студентами умений и навыков реагирования на инциденты информационной безопасности.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль профессиональной подготовки (major).
Индекс дисциплины: Б1.В.1.4.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		

ПК-1. Способен обеспечивать анализ, проектирование, разработку, функционирование, эксплуатацию систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	ПК-1.1. Знает общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	Знает общие принципы работы систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей.
	ПК-1.2. Умеет разрабатывать необходимую техническую документацию в области проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей	Умеет разрабатывать необходимую техническую документацию для систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей
	ПК-1.3. Владеет навыками проектирования элементов систем информационной безопасности объектов критической информационной инфраструктуры	Владеет навыками проектирования элементов систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей

ПК-3. Способен разрабатывать организационно-распорядительные документы, регламентирующие функционирование систем информационной безопасности объектов критической информационной инфраструктуры	ПК-3.1. Знает содержание и порядок деятельности персонала по эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры	Знает содержание и порядок деятельности персонала по эксплуатации систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей
	ПК-3.2. Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры	Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей
	ПК-3.3. Умеет разрабатывать технические задания на создание систем информационной безопасности объектов критической информационной инфраструктуры с учетом действующих нормативных и методических документов	Умеет разрабатывать технические задания на создание систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей
	ПК-3.4. Владеет инструментами проведения и фиксации результатов проверки функционирования систем информационной безопасности объектов критической информационной инфраструктуры	Владеет инструментами проведения и фиксации результатов проверки функционирования систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей
	ПК-3.5. Умеет осуществлять планирование и организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.	Умеет осуществлять планирование и организацию работы персонала систем выявления инцидентов и противодействия атакам на объекты критической информационной инфраструктуры и ее частей

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	80	80
Лекционные занятия	28	28
Лабораторные занятия	52	52
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	64	64
Написание конспекта самоподготовки	10	10
Подготовка к тестированию	12	12
Подготовка к устному опросу / собеседованию	10	10
Подготовка к лабораторной работе, написание отчета	32	32
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	180	180
Общая трудоемкость (в з.е.)	5	5

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр					
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса	4	-	6	10	ПК-1, ПК-3
2 Управление инцидентами информационной безопасности	12	24	24	60	ПК-1, ПК-3
3 Процесс управления инцидентами информационной безопасности	6	20	15	41	ПК-1, ПК-3
4 SIEM-системы	6	8	19	33	ПК-1, ПК-3
Итого за семестр	28	52	64	144	
Итого	28	52	64	144	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
2 семестр			

1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса	Обзор международных и российских стандартов, регламентирующих управление инцидентами информационной безопасности и непрерывностью бизнеса	4	ПК-1, ПК-3
	Итого	4	
2 Управление инцидентами информационной безопасности	Событие и инцидент информационной безопасности. Цели и задачи управления информационной безопасностью. Система управления инцидентами информационной безопасности. Этапы процесса управления инцидентами информационной безопасности. Обнаружение событий информационной безопасности и инцидентов информационной безопасности и оповещение о них. Обработка событий информационной безопасности и инцидентов информационной безопасности. Реагирование на инциденты информационной безопасности. Документация системы управления инцидентами информационной безопасности. Группа реагирования на инциденты информационной безопасности. Обеспечение осведомленности и обучение в области инцидентов информационной безопасности. Сохранение доказательств на инциденты информационной безопасности. Средства управления событиями информационной безопасности.	12	ПК-1, ПК-3
	Итого	12	

3 Процесс управления инцидентами информационной безопасности	Планирование и подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ. Структура менеджмента инцидентов ИБ. Политика менеджмента инцидентов информационной безопасности. Программа менеджмента инцидентов информационной безопасности. Политики менеджмента рисков и информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ. Обнаружение и оповещение о событиях ИБ. Оценка и принятие решений по событиям/инцидентам. Реагирование на инциденты. Анализ инцидентов ИБ и процесса менеджмента инцидентов ИБ. Улучшение анализа рисков и менеджмента ИБ.	6	ПК-1, ПК-3
	Итого	6	
4 SIEM-системы	Техническая и другая поддержка реагирования на инциденты информационной безопасности. Электронные базы данных событий/инцидентов ИБ и технические средства для быстрого пополнения и обновления базы данных. SIEM-системы: IBM QRadar, MaxPatrol SIEM, ArcSight, Splunk и другие. Технологические тренды развития SIEM-систем.	6	ПК-1, ПК-3
	Итого	6	
Итого за семестр		28	
Итого		28	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
2 семестр			
2 Управление инцидентами информационной безопасности	Выявление инцидентов информационной безопасности	8	ПК-1, ПК-3
	Защита баз данных предприятия	8	ПК-1, ПК-3
	Защита контроллера домена предприятия	8	ПК-1, ПК-3
	Итого	24	

3 Процесс управления инцидентами информационной безопасности	Защита данных файлового сервера	8	ПК-1, ПК-3
	Защита данных сегмента АСУ ТП	8	ПК-1, ПК-3
	Защита научно-технической информации предприятия	4	ПК-1, ПК-3
	Итого	20	
4 SIEM-системы	Защита корпоративного портала от внутреннего нарушителя	8	ПК-1, ПК-3
	Итого	8	
Итого за семестр		52	
Итого		52	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
2 семестр				
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса	Написание конспекта самоподготовки	2	ПК-1, ПК-3	Конспект самоподготовки
	Подготовка к тестированию	2	ПК-1, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	2	ПК-1, ПК-3	Устный опрос / собеседование
	Итого	6		
2 Управление инцидентами информационной безопасности	Написание конспекта самоподготовки	4	ПК-1, ПК-3	Конспект самоподготовки
	Подготовка к тестированию	4	ПК-1, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	4	ПК-1, ПК-3	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	12	ПК-1, ПК-3	Лабораторная работа
	Итого	24		

3 Процесс управления инцидентами информационной безопасности	Написание конспекта самоподготовки	2	ПК-1, ПК-3	Конспект самоподготовки
	Подготовка к тестированию	3	ПК-1, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	2	ПК-1, ПК-3	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	8	ПК-1, ПК-3	Лабораторная работа
	Итого	15		
4 SIEM-системы	Написание конспекта самоподготовки	2	ПК-1, ПК-3	Конспект самоподготовки
	Подготовка к тестированию	3	ПК-1, ПК-3	Тестирование
	Подготовка к устному опросу / собеседованию	2	ПК-1, ПК-3	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	12	ПК-1, ПК-3	Лабораторная работа
	Итого	19		
Итого за семестр		64		
	Подготовка и сдача экзамена	36		Экзамен
Итого		100		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ПК-1	+	+	+	Конспект самоподготовки, Устный опрос / собеседование, Лабораторная работа, Тестирование, Экзамен
ПК-3	+	+	+	Конспект самоподготовки, Устный опрос / собеседование, Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
2 семестр				
Конспект самоподготовки	0	0	5	5
Устный опрос / собеседование	0	0	5	5
Лабораторная работа	15	20	20	55
Тестирование	0	0	5	5
Экзамен				30
Итого максимум за период	15	20	35	100
Нарастающим итогом	15	35	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. ГОСТ Р ИСО/МЭК 27001-2021 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Информационная технология МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Требования [Электронный ресурс] [Электронный ресурс]: — Режим доступа: https://docs.cntd.ru/document/1200181890.

2. Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. — Новосибирск : НГТУ, 2018. — 122 с. — ISBN 978-5-7782-3603-5. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/118277.

7.2. Дополнительная литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : СКФУ, 2017. — 86 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/155146.

2. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200068822 .

3. Абденов, А. Ж. Методика оценки риска для информационных систем на основе экспертных оценок : учебное пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель. — Новосибирск : НГТУ, 2014. — 71 с. — ISBN 978-5-7782-2588-6. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/118246.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Конев, А. А. Выявление инцидентов и противодействие атакам на объекты критической информационной инфраструктуры: учебно-методическое пособие [Электронный ресурс] / А. А. Конев, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 174 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10002.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля

и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса	ПК-1, ПК-3	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Управление инцидентами информационной безопасности	ПК-1, ПК-3	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Процесс управления инцидентами информационной безопасности	ПК-1, ПК-3	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

4 SIEM-системы	ПК-1, ПК-3	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции

2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?
   a) Группы пользователей и права доступа
   b) Пользователи и группы
   c) Сервер и рабочая станция
   d) Риски и контрмеры

2. По каким угрозам в системе ГРИФ не оценивается ущерб?
   a) Конфиденциальности
   b) Целостности
   c) Достоверность
   d) Доступность

3. Какой категории угроз не представлено в системе ГРИФ?
   a) Физические угрозы человека
   b) Угрозы персонала
   c) Системные ошибки
   d) Физические угрозы

4. Какого типа экономического ущерба не существует?
   a) Долговременный экономический ущерб
   b) Кратковременный экономический ущерб
   c) Отсроченный экономический ущерб
   d) Немедленный экономический ущерб

5. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «нарушение бизнес-деятельности»?
   a) Кратковременный экономический ущерб
   b) Отсроченный экономический ущерб
   c) Немедленный экономический ущерб
   d) Долговременный экономический ущерб

6. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?
   a) Не повлияет
   b) Приравняет к нулю
   c) Вызовет уменьшение
   d) Вызовет рост

7. Какая из перечисленных выполняемых проверок не входит в перечень обязательных действий, входящих в руководство по реализации средств управления против злонамеренного кода?
   a) Проверка любых файлов на электронном или оптическом носителе, а также файлов, полученных по сетям, на наличие злонамеренного кода перед использованием
   b) Проверка web-страниц на наличие злонамеренного кода
   c) Проверка обновлений средства управления против злонамеренного кода
   d) Проверка приложений к электронным письмам и загрузок на наличие злонамеренного кода перед использованием

8. По какой причине для класса группы авторизованных интернет-пользователей в системе ГРИФ не предлагается никаких средств защиты рабочего места?
   a) Для данной группы характерна минимальная вероятность реализации угрозы
   b) Для группы по умолчанию выбран набор средств защиты рабочего места
   c) Для группы неизвестно, откуда будет осуществляться доступ
   d) Для группы неизвестна степень влияния на систему

9. Какие данные нельзя указать при задании контрмер в системе ГРИФ?
   a) Стоимость внедрения
   b) Возможное снижение затрат на ИБ
   c) Срок внедрения контрмеры
   d) Название для отчета

10. Какие параметры нельзя включить в состав отчета по проекту в системе КОНДОР?
    a) Выполненные требования
    b) Невыполненные требования
    c) Риски
    d) Контрмеры

11. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «подрыв репутации»?
    a) Кратковременный экономический ущерб
    b) Отсроченный экономический ущерб
    c) Долговременный экономический ущерб
    d) Немедленный экономический ущерб

12. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «снижение розничных продаж»?
    a) Отсроченный экономический ущерб
    b) Немедленный экономический ущерб
    c) Кратковременный экономический ущерб
    d) Долговременный экономический ущерб

13. Какой информации не содержится в отчете по периоду, формируемом системой КОНДОР?
    a) Количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита
    b) Уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита
    c) Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого

раздела в выбранных периодах аудита
d) Затраты на контрмеры в целом по системе для выбранного периода аудита

14. Чему по умолчанию равны вероятность в течение года и критичность реализации для только что созданной угрозы?
a) 25 %
b) 15 %
9 %
c) 0 %

15. Какой информации не содержится в отчете по проекту, формируемом системой КОНДОР?
a) Изменения количества выполненных требований в целом по системе, по всем разделам или
b) для каждого раздела в выбранных периодах аудита
c) Изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в
d) выбранных периодах аудита
e) Текст выполненных требований по каждому разделу
f) Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

16. Какое количество мер защиты содержит в себе «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0»?
a) 32
b) 33
c) 34
d) 35

17. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР
ББС-1.2?
a) Диаграмма Ганта
b) Гистограмма
c) Круговая диаграмма
d) Срез структуры

18. Что понимается под базовым временем простоя ресурсов?
a) Время необходимое на обработку информации после запроса
b) Время отклика системы на запрос
c) Время, в течение которого доступ к информации ресурса невозможен
d) Время, в течение которого система загружает необходимые для работы службы

19. Фактором, значимым для использования уязвимости не является?
a) Время, затрачиваемое на идентификацию уязвимости
b) Техническая компетентность специалиста
c) Программное средство, требуемое для анализа
d) Знание проекта и функционирования объекта

20. Что понимается под эффективностью средства защиты информации?
a) Показатель быстродействия системы в условиях использования средств защиты информации
b) Коэффициент снижения уровня риска по отношению к первоначальному уровню
c) Степень влияния на защищенность информации и рабочего места группы пользователей
d) Субъективная оценка экспертами корректности функционирования средства защиты информации

9.1.2. Перечень экзаменационных вопросов

1. Цель и этапы анализа объектов защиты.
2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
3. Идентификация и классификация объектов защиты.
4. Типизация информационных систем. Данные об информационной системе, необходимые для построения модели документооборота.
5. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.
6. Подходы к построению модели нарушителя.
7. Классификация нарушителей (ФСТЭК).
8. Классификация угроз безопасности персональных данных (ФСТЭК).
9. Методика определения актуальных угроз (ФСТЭК).
10. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.
11. Угрозы, источником которых является персонал организации.
12. Методы «социальной инженерии» и способы защиты от них.
13. Обязанности сотрудников Службы безопасности при приёме сотрудников на работу.
14. Нормативная документация, обязательная к ознакомлению и подписанию при приёме на работу.
15. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.
16. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.
17. Упрощённая модель классификации субъектов.
18. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.
19. Основные положения регламента контроля использования технических средств обработки и передачи информации.
20. Основные положения инструкции по организации парольной защиты.
21. Основные положения документов, регламентирующих использование средств аутентификации и носителей ключевой информации.
22. Основные положения инструкции по организации антивирусной защиты.
23. Основные положения инструкции по работе с электронной почтой.
24. Типы чрезвычайных ситуаций. Структура аварийного плана. Причины изменения аварийного плана.
25. Классификация объектов при составлении аварийного плана.
26. Требования к различным классам объектов и их резервированию.
27. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.
28. Приведите примеры источников информации об инцидентах информационной безопасности.
29. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.
30. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

9.1.3. Примерный перечень тем для конспектов самоподготовки

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?
2. Каковы основные цели следования модели Деминга при построении процесса управления инцидентами информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?
3. Какова роль процесса управления инцидентами информационной безопасности в рамках системы управления информационной безопасности ?

4. Какова взаимосвязь между процессами управления рисками информационной безопасности и управления инцидентами информационной безопасности?
5. Дайте определение непрерывности бизнеса, управлению непрерывностью бизнеса, программы управления непрерывностью бизнеса и плана обеспечения непрерывности бизнеса.
6. Почему деятельность по управлению непрерывностью бизнеса так важна для современных организаций?

9.1.4. Примерный перечень вопросов для устного опроса / собеседования

1. Событие информационной безопасности.
2. Инцидент информационной безопасности.
3. Структурный подход к менеджменту инцидентов ИБ.
4. Этапы менеджмента инцидентов ИБ. Менеджмент и анализ рисков ИБ.
5. Инциденты информационной безопасности и их причины.
6. Планирование и подготовка к менеджменту инцидентов ИБ.
7. Политика обработки сообщений о событиях и инцидентах ИБ.
8. Структура менеджмента инцидентов ИБ.
9. Политика менеджмента инцидентов информационной безопасности.
10. Программа менеджмента инцидентов информационной безопасности.
11. Политики менеджмента рисков и информационной безопасности.
12. Создание группы реагирования на инциденты информационной безопасности.
13. Использование системы менеджмента инцидентов ИБ.
14. Обнаружение и оповещение о событиях ИБ.
15. Оценка и принятие решений по событиям/инцидентам.
16. Реагирование на инциденты.
17. Анализ инцидентов ИБ и процесса менеджмента инцидентов ИБ.
18. Улучшение анализа рисков и менеджмента ИБ.

9.1.5. Темы лабораторных работ

1. Выявление инцидентов информационной безопасности
2. Защита баз данных предприятия
3. Защита контроллера домена предприятия
4. Защита данных файлового сервера
5. Защита данных сегмента АСУ ТП
6. Защита научно-технической информации предприятия
7. Защита корпоративного портала от внутреннего нарушителя

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.
Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «25» 1 2022 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc
Доцент, каф. КИБЭВС	А.К. Новохрестов	Разработано, 1df3f1b6-c21f-4a1c-b6d5-0010ff8a4977