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 учебной работе

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

Управление инцидентами и непрерывностью бизнеса

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **5**
Семестр: **9**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	54	54	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 9 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Старший преподаватель каф. КИБЭВС _____ А. И. Гуляев

Доцент каф. КИБЭВС _____ А. А. Конев

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ Е. М. Давыдова

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ Е. Ю. Костюченко

1. Цели и задачи дисциплины

1.1. Цели дисциплины

дать основы управления инцидентами информационное безопасности, а также формирование знаний процессах и системах управления инцидентами информационной безопасности и непрерывностью бизенса.

1.2. Задачи дисциплины

– дать основы:

– - нормативного обеспечений управления инцидентами информационной безопасности и непрерывностью бизнеса;

– - планирования, подготовки, использования, анализа и улучшения процесса управления инцидентами информационной безопасности;

– - документации системы управления инцидентами информационной безопасности;

– - реагирования на инциденты информационной безопасности;

– - функционала инструментальных средств управления событиями информационной безопасности;

– - циклической модели улучшения процессов.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление инцидентами и непрерывностью бизнеса» (Б1.В.05.01) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Базы данных и экспертные системы, Управление средствами защиты информации.

Последующими дисциплинами являются: Управление информационной безопасностью.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;

– ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;

– ПСК-5.5 способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;

– ПСК-5.1 способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;

В результате изучения дисциплины обучающийся должен:

– **знать** принципы построения системы управления информационной безопасности объекта в части систем управления инцидентами информационной безопасности и непрерывности бизнеса, современные подходы к управлению инцидентами информационной безопасности и непрерывности бизнеса объекта и направления их развития, основные международные и российские стандарты, регламентирующие управление инцидентами информационной безопасности и непрерывности бизнеса, принципы разработки процессов управления инцидентами информационной безопасности и непрерывности бизнеса, принципы создания основных документов, регламентирующих вопросы управления инцидентами информационной безопасности и непрерывности бизнеса

– **уметь** анализировать текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления инцидентами информационной безопасностью и непрерывностью бизнеса. Определять цели и задачи, решаемые разрабатываемыми процессами управления инцидентами информационной безопасности и непрерывности бизнеса .Применять процессный подход к управлению инцидентами информационной безопасности и и непрерывности бизнеса. Используя современные методы и средства, разрабатывать процессы управления инцидентами информационной безопасности и и непрерывности бизне-

са учитывающие особенности функционирования предприятий и решаемых ими задач, и оценивать их эффективность. Разрабатывать документальное обеспечение для процессов управления инцидентами информационной безопасности и и непрерывности бизнеса, включая различные политики и применять его на практике.

– **владеть** терминологией и процессным подходом построения систем управления инцидентами информационной безопасности и систем управления непрерывностью бизнеса. Навыками построения как отдельных процессов управления инцидентами управления инцидентами информационной безопасности и и непрерывности бизнеса, так и систем процессов в целом.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Лабораторные работы	36	36
Самостоятельная работа (всего)	54	54
Оформление отчетов по лабораторным работам	36	36
Проработка лекционного материала	18	18
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр					
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса	4	0	4	8	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5
2 Управление инцидентами информационной безопасности	8	32	40	80	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5
3 Управление непрерывностью бизнеса организации	6	4	10	20	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
9 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-20, ПК-27, ПСК-5.1, ПСК-5.5
	Итого	4	
2 Управление инцидентами информационной безопасности	Событие и инцидент информационной безопасности.Цели и задачи управления информационной безопасностью. Система управления инцидентами информационной безопасности. Этапв процесса управления инцидентами информационной безопасности. Обнаружение событий информационной безопасности и инцидентов информационной безопасности и опопвещение 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.	8	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5
	Итого	8	
3 Управление непрерывностью бизнеса организации	Определение непрерывности бизнеса и управление ей. Систему управления непрерывностью бизнеса. Жизненный цикл управления непрерывностью бизнеса. Документация и записи в области непрерывности бизнеса. Готовность информационных и телекоммуникационных технологий к обеспечению непрерывности бизнеса.Средства управления непрерывностью бизнеса.	6	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5
	Итого	6	
Итого за семестр		18	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин		
	1	2	3
Предшествующие дисциплины			
1 Базы данных и экспертные системы		+	+
2 Управление средствами защиты информации		+	
Последующие дисциплины			
1 Управление информационной безопасностью		+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	Конспект самоподготовки, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Тест
ПК-27	+	+	+	Конспект самоподготовки, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Тест
ПСК-5.5	+	+	+	Конспект самоподготовки, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Тест
ПСК-5.1	+	+	+	Конспект самоподготовки, Собеседование, Отчет по лабораторной работе, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
2 Управление	Развертывание SIEM системы. Определе-	16	ПК-20, ПК-27,

инцидентами информационной безопасности	ние источников получения информации о событиях информационной безопасности. Разбор необходимости нормализации событий. Создание правил корреляции событий. Создание инцидентов на основе событий информационной безопасности.		ПСК-5.1, ПСК-5.5
	Развертывание IRP системы. Передача инцидентов из SIEM системы. Получение фидов из сторонних источников. Обработка инцидентов информационной безопасности. Отработка жизненного цикла инцидента информационной безопасности.	16	
	Итого	32	
3 Управление непрерывностью бизнеса организации	Разработка стратегии и политики управления непрерывностью бизнеса.	4	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5
	Итого	4	
Итого за семестр		36	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
9 семестр				
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса	Проработка лекционного материала	4	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Собеседование, Тест
	Итого	4		
2 Управление инцидентами информационной безопасности	Проработка лекционного материала	8	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Собеседование, Тест
	Оформление отчетов по лабораторным работам	32		
	Итого	40		
3 Управление непрерывностью бизнеса организации	Проработка лекционного материала	6	ПК-20, ПК-27, ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Отчет по лабораторной работе, Собеседование, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	10		
Итого за семестр		54		

Итого	54		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	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
9 семестр				
Конспект самоподготовки	5	5	5	15
Опрос на занятиях	2	3	5	10
Отчет по лабораторной работе	10	10	10	30
Собеседование	5	5	5	15
Тест	10	10	10	30
Итого максимум за период	32	33	35	100
Нарастающим итогом	32	65	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	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	Ниже 60 баллов	F (неудовлетворительно)

зачтено)		

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. ГОСТ Р ИСО/МЭК 27001-2006 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Информационная технология МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Требования [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200058325 (дата обращения: 30.08.2021).

12.2. Дополнительная литература

1. СТО БР БФБО-1.5-2018 СТАНДАРТ БАНКА РОССИИ БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ О ФОРМАХ И СРОКАХ ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ С УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНАПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ, СВЯЗАННЫХ С НАРУШЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ [Электронный ресурс]: — Режим доступа: https://cbr.ru/statichtml/file/59420/st-15-18.pdf (дата обращения: 30.08.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационных технологий [Электронный ресурс]: Учебное пособие / А. И. Исакова - 2016. 206 с. — Режим доступа: https://edu.tusur.ru/publications/6484 (дата обращения: 30.08.2021).
2. Безопасность сетей ЭВМ. Часть 1 [Электронный ресурс]: Лабораторный практикум / А. К. Новохрестов, А. И. Гуляев - 2017. 92 с. — Режим доступа: https://edu.tusur.ru/publications/7225 (дата обращения: 30.08.2021).
3. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] — Режим доступа: https://disk.fb.tusur.ru/bsevm/practice.pdf (дата обращения: 30.08.2021).
4. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] — Режим доступа: https://disk.fb.tusur.ru/bsevm/independent_work.pdf (дата обращения: 30.08.2021).

12.3.2. 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.

12.4. Профессиональные базы данных и информационные справочные системы

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

12.5. Периодические издания

1. Информация и безопасность [Электронный ресурс]: научный журнал. - Воронеж :

ВГТУ . - Журнал выходит с 1998 г. — Режим доступа: https://elibrary.ru/title_about.asp?id=8748 (дата обращения: 30.08.2021).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. 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 количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория информатики, технологий и методов программирования

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard 78" с ПО ActivInspire;
- Проектор ViewSonic PJD5154 DLP;
- Компьютеры: DEPO Neos 235/ A8-7650K/ DDR3 4G/ 1Tb / мышь/ клавиатура/ монитор (10 шт.);
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Моноблок: Asus V222GAK-BA021D: Intel J5005/ DDR4 4G/ 500Gb/ WiFi / мышь/ клавиатура (30шт.);
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Аппаратные средства аутентификации пользователя «eToken Pro»;
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x, ПАК Аккорд;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;
- межсетевые экраны: ИКС Lite, Positive Technologies Application Firewall Education, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- системы обнаружения компьютерных атак: Snort, Suricata, СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;

- точки доступа: D-link dwl3600ap;
- системы защиты от утечки данных: Контур информационной безопасности SearchInform;
- средства мониторинга состояния автоматизированных систем: система мониторинга Zabbix;
- средства сканирования защищенности компьютерных сетей: сканер безопасности Xspider Education, система анализа защищенности сети MaxPatrol Education.

Устройства чтения смарт-карт и радиометок: Адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
– Microsoft Windows 10

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:
- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры: AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb/ мышь/ клавиатура/ монитор (15шт.);
- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
– Microsoft Windows 10

13.1.3. 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, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:
- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. 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 зрениями** 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.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Каковы основные цели следования модели Деминга при построениипроцесса управления инцидентами информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

Какова роль процесса управления инцидентами информационной безопасности в рамках системы управления информационной безопасности ?

Какова взаимосвязь между процессами управления рисками информационной безопасности и управления инцидентами информационной безопасности?

Дайте определение непрерывности бизнеса, управлению непрерывностью бизнеса, программы управления непрерывностью бизнеса и плана обеспечения непрерывности бизнеса.

Почему деятельность по управлению непрерывностью бизнеса так важна для современных организаций?

14.1.2. Темы опросов на занятиях

Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Каковы основные цели следования модели Деминга при построениипроцесса управления инцидентами информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

Какова роль процесса управления инцидентами информационной безопасности в рамках системы управления информационной безопасности ?

Какова взаимосвязь между процессами управления рисками информационной безопасности и управления инцидентами информационной безопасности?

Дайте определение непрерывности бизнеса, управлению непрерывностью бизнеса, программы управления непрерывностью бизнеса и плана обеспечения непрерывности бизнеса.

Почему деятельность по управлению непрерывностью бизнеса так важна для современных организаций?

14.1.3. Вопросы на собеседование

Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Каковы основные цели следования модели Деминга при построениипроцесса управления инцидентами информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК

ТО 18044?

Какова роль процесса управления инцидентами информационной безопасности в рамках системы управления информационной безопасности ?

Какова взаимосвязь между процессами управления рисками информационной безопасности и управления инцидентами информационной безопасности?

Дайте определение непрерывности бизнеса, управлению непрерывностью бизнеса, программы управления непрерывностью бизнеса и плана обеспечения непрерывности бизнеса.

Почему деятельность по управлению непрерывностью бизнеса так важна для современных организаций?

14.1.4. Вопросы на самоподготовку

Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Каковы основные цели следования модели Деминга при построениипроцесса управления инцидентами информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

Какова роль процесса управления инцидентами информационной безопасности в рамках системы управления информационной безопасности ?

Какова взаимосвязь между процессами управления рисками информационной безопасности и управления инцидентами информационной безопасности?

Дайте определение непрерывности бизнеса, управлению непрерывностью бизнеса, программы управления непрерывностью бизнеса и плана обеспечения непрерывности бизнеса.

Почему деятельность по управлению непрерывностью бизнеса так важна для современных организаций?

14.1.5. Темы лабораторных работ

Развертывание SIEM системы. Определение источников получения информации о событиях информационной безопасности. Разбор необходимости нормализации событий. Создание правил корреляции событий. Создание инцидентов на основе событий информационной безопасности.

Развертывание IRP системы. Передача инцидентов из SIEM системы. Получение фидов из сторонних источников. Обработка инцидентов информационной безопасности. Отработка жизненного цикла инцидента информационной безопасности.

Разработка стратегии и политики управления непрерывностью бизнеса.

14.1.6. Зачёт

Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

Каковы основные цели следования модели Деминга при построениипроцесса управления инцидентами информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

Какова роль процесса управления инцидентами информационной безопасности в рамках системы управления информационной безопасности ?

Какова взаимосвязь между процессами управления рисками информационной безопасности и управления инцидентами информационной безопасности?

Дайте определение непрерывности бизнеса, управлению непрерывностью бизнеса, программы управления непрерывностью бизнеса и плана обеспечения непрерывности бизнеса.

Почему деятельность по управлению непрерывностью бизнеса так важна для современных организаций?

14.2. 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 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории	Виды дополнительных оценочных	Формы контроля и оценки

обучающихся	материалов	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 исходя из состояния обучающегося на момент проверки

14.3. 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.