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
_____П.В. Сенченко
«30» _____06_____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **заочная**
Факультет: **Заочный и вечерний факультет (ЗиВФ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **5, 6**
Семестр: **10, 11**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	10 семестр	11 семестр	Всего	Единицы
Лекционные занятия	4	4	8	часов
Практические занятия	4		4	часов
Лабораторные занятия	8	4	12	часов
Самостоятельная работа	128	17	145	часов
Контрольные работы		2	2	часов
Подготовка и сдача экзамена		9	9	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	36	180	часов
			5	з.е.

Формы промежуточной аттестация	Семестр	Количество
Экзамен	11	
Контрольные работы	11	1

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 30.06.2021
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 78246

1. Общие положения

1.1. Цели дисциплины

1. Овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

1.2. Задачи дисциплины

1. Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.
2. Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.
3. Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специальности (special hard skills - SHS).
Индекс дисциплины: Б1.О.03.23.
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		
ОПК-4. Способен разрабатывать и принимать экономически и финансово обоснованные организационно-управленческие решения, планировать и организовывать профессиональную деятельность, осуществлять контроль и учет ее результатов	ОПК-4.1. Знает принципы формирования политики информационной безопасности в организациях кредитно-финансовой сферы и систему организационных мер, направленных на обеспечение экономической безопасности в организации	Знает принципы формирования политики информационной безопасности в организациях кредитно-финансовой сферы и систему организационных мер, направленных на обеспечение экономической безопасности в организации
	ОПК-4.2. Умеет осуществлять расчет аналитических показателей, необходимых для решения поставленной экономической задачи	Умеет осуществлять расчет аналитических показателей, необходимых для решения поставленной экономической задачи
	ОПК-4.3. Владеет методами количественной оценки экономических показателей деятельности предприятия с целью принятия обоснованных экономических решений	Владеет методами количественной оценки экономических показателей деятельности предприятия с целью принятия обоснованных экономических решений

Согласована на портале № 78246

ОПК-5. Способен осуществлять профессиональную деятельность в соответствии с нормами профессиональной этики, нормами права, нормативными правовыми актами в сфере экономики, исключающими противоправное поведение	ОПК-5.1. Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области экономической безопасности	Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности
	ОПК-5.2. Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности
	ОПК-5.3. Владеет навыками информационно-аналитического обеспечения предупреждения, выявления, пресечения, раскрытия и расследования экономических и налоговых преступлений	Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации
ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.1. Знает типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности	Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа
	ОПК-6.2. Умеет применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности	Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности
	ОПК-6.3. Владеет инструментами управления процессами организации, в том числе на основе норм права и с использованием ИКТ, использует как минимум один из общих или специализированных пакетов прикладных программ (MS Excel, Stata, SPSS, R и др.), предназначенных для выполнения обработки статистической информации, построения и проведения диагностики эконометрических моделей	Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа в процессе функционирования сетей электросвязи

Согласована на портале № 78246

Профессиональные компетенции		
-	-	-

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	
		10 семестр	11 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	26	16	10
Лекционные занятия	8	4	4
Практические занятия	4	4	
Лабораторные занятия	12	8	4
Контрольные работы	2		2
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	145	128	17
Подготовка к тестированию	108	104	4
Подготовка к лабораторной работе, написание отчета	33	24	9
Подготовка к контрольной работе	4		4
Подготовка и сдача экзамена	9		9
Общая трудоемкость (в часах)	180	144	36
Общая трудоемкость (в з.е.)	5	4	1

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	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр						
1 Анализ объекта защиты	1	4	8	52	65	ОПК-4, ОПК-5, ОПК-6
2 Внутренние угрозы ИБ	1	-	-	24	25	ОПК-4, ОПК-5, ОПК-6
3 Подбор и увольнение сотрудников	1	-	-	28	29	ОПК-4, ОПК-5, ОПК-6
4 Текущая работа с персоналом	1	-	-	24	25	ОПК-4, ОПК-5, ОПК-6
Итого за семестр	4	4	8	128	144	
11 семестр						
6 Управление инцидентами ИБ	1	-	-	2	5	ОПК-4, ОПК-5, ОПК-6
7 Системы менеджмента ИБ	1	-	4	11	16	ОПК-4, ОПК-5, ОПК-6

Согласована на портале № 78246

8 Свод правил по управлению ИБ	1	-	-	2	3	ОПК-4, ОПК-5, ОПК-6
9 Обеспечение защиты информации в экстренных ситуациях	1	-	-	2	3	ОПК-4, ОПК-5, ОПК-6
Итого за семестр	4	0	4	17	25	
Итого	8	4	12	145	169	

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
10 семестр			
1 Анализ объекта защиты	Анализ объектов защиты	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
2 Внутренние угрозы ИБ	Внутренние угрозы ИБ	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
3 Подбор и увольнение сотрудников	Подбор и увольнение сотрудников	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
4 Текущая работа с персоналом	Текущая работа с персоналом	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
Итого за семестр		4	
11 семестр			
6 Управление инцидентами ИБ	Управление инцидентами ИБ	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
7 Системы менеджмента ИБ	Системы менеджмента ИБ	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
8 Свод правил по управлению ИБ	Свод правил по управлению ИБ	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
9 Обеспечение защиты информации в экстренных ситуациях	Обеспечение защиты информации в экстренных ситуациях	1	ОПК-4, ОПК-5, ОПК-6
	Итого	1	
Итого за семестр		4	
Итого		8	

5.3. Контрольные работы

Виды контрольных работ и часы на контрольные работы приведены в таблице 5.3.
Таблица 5.3 – Контрольные работы

№ п.п.	Виды контрольных работ	Трудоемкость, ч	Формируемые компетенции
11 семестр			

Согласована на портале № 78246

1	Контрольная работа с автоматизированной проверкой	2	ОПК-4, ОПК-5, ОПК-6
	Итого за семестр	2	
	Итого	2	

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
10 семестр			
1 Анализ объекта защиты	Изучение Digital Secure	8	ОПК-4, ОПК-5, ОПК-6
	Итого	8	
	Итого за семестр	8	
11 семестр			
7 Системы менеджмента ИБ	Использование Digital Secure для формирования политики безопасности организации	4	ОПК-4, ОПК-5, ОПК-6
	Итого	4	
	Итого за семестр	4	
	Итого	12	

5.5. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.5.

Таблица 5.5. – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Анализ объекта защиты	Анализ объекта защиты. Формирование модели документооборота. Формирование модели угроз. Формирование модули нарушителя. Определение перечня актуальных угроз.	4	ОПК-4, ОПК-5, ОПК-6
	Итого	4	
	Итого за семестр	4	
	Итого	4	

5.6. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.7. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.7.

Таблица 5.7. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				

Согласована на портале № 78246

1 Анализ объекта защиты	Подготовка к тестированию	28	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	24	ОПК-4, ОПК-5, ОПК-6	Лабораторная работа
	Итого	52		
2 Внутренние угрозы ИБ	Подготовка к тестированию	24	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Итого	24		
3 Подбор и увольнение сотрудников	Подготовка к тестированию	28	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Итого	28		
4 Текущая работа с персоналом	Подготовка к тестированию	24	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Итого	24		
Итого за семестр		128		
11 семестр				
6 Управление инцидентами ИБ	Подготовка к тестированию	1	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Подготовка к контрольной работе	1	ОПК-4, ОПК-5, ОПК-6	Контрольная работа
	Итого	2		
7 Системы менеджмента ИБ	Подготовка к тестированию	1	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Подготовка к контрольной работе	1	ОПК-4, ОПК-5, ОПК-6	Контрольная работа
	Подготовка к лабораторной работе, написание отчета	9	ОПК-4, ОПК-5, ОПК-6	Лабораторная работа
	Итого	11		
8 Свод правил по управлению ИБ	Подготовка к тестированию	1	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Подготовка к контрольной работе	1	ОПК-4, ОПК-5, ОПК-6	Контрольная работа
	Итого	2		
9 Обеспечение защиты информации в экстренных ситуациях	Подготовка к тестированию	1	ОПК-4, ОПК-5, ОПК-6	Тестирование
	Подготовка к контрольной работе	1	ОПК-4, ОПК-5, ОПК-6	Контрольная работа
	Итого	2		
Итого за семестр		17		
	Подготовка и сдача экзамена	9		Экзамен
Итого		154		

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.8.

Согласована на портале № 78246

Таблица 5.8 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лек. зан.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-4	+	+	+	+	Контрольная работа, Лабораторная работа, Тестирование, Экзамен
ОПК-5	+	+	+	+	Контрольная работа, Лабораторная работа, Тестирование, Экзамен
ОПК-6	+	+	+	+	Контрольная работа, Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью». Выпуск 1 [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. – Электрон. дан. – М.: Горячая линия- Телеком, 2012. – 244 с. [Электронный ресурс]: — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5178.

7.2. Дополнительная литература

1. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. [Электронный ресурс]: — Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=187854.

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://protect.gost.ru/document.aspx?control=7&id=173886.

3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=177398.

4. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187871.

5. ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183954.

6. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187948.

7. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=184904.

8. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=179072.

Согласована на портале № 78246

9. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2: учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 130 с [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/5179.

10. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3 [Электронный ресурс] [Электронный ресурс]: учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 170 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/5180.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/223313.

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 практических занятий

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;

Согласована на портале № 78246

- Магнитно-маркерная доска;
- Обучающий стенд локальные компьютерные сети Microtik routerboard - 2 шт.;
- ViPNET УМК "Безопасность сетей";
- Коммутатор Mikrotik CRS125-24G-1S-IN - 6 шт.;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 - 3 шт.;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 - 2 шт.;
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 - 2 шт.;
- Маршрутизатор Cisco C881-V-K9 - 2 шт.;
- Маршрутизатор Check Point CPAP-SG1200R-NGFW - 2 шт.;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:
- абонентские 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;
- межсетевые экраны: ИКС Lite, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:
- абонентские 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 криптографической защиты информации: программно-аппаратный комплекс шифрования "ФПСУ-IP", программно-аппаратный комплекс шифрования "ФПСУ-IP/Клиент".
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:
- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Магнитно-маркерная доска;
- Обучающий стенд локальные компьютерные сети Microtik routerboard - 2 шт.;
- ViPNET УМК "Безопасность сетей";
- Коммутатор Mikrotik CRS125-24G-1S-IN - 6 шт.;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 - 3 шт.;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 - 2 шт.;
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 - 2 шт.;
- Маршрутизатор Cisco C881-V-K9 - 2 шт.;
- Маршрутизатор Check Point CPAP-SG1200R-NGFW - 2 шт.;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:
- абонентские 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;
- межсетевые экраны: ИКС Lite, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;

Согласована на портале № 78246

- точки доступа: D-link dwl3600ap.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:

- абонентские 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 криптографической защиты информации: программно-аппаратный комплекс шифрования "ФПСУ-IP", программно-аппаратный комплекс шифрования "ФПСУ-IP/Клиент".
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

8.4. 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.

8.5. 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.

Согласована на портале № 78246

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Анализ объекта защиты	ОПК-4, ОПК-5, ОПК-6	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
2 Внутренние угрозы ИБ	ОПК-4, ОПК-5, ОПК-6	Тестирование	Примерный перечень тестовых заданий
3 Подбор и увольнение сотрудников	ОПК-4, ОПК-5, ОПК-6	Тестирование	Примерный перечень тестовых заданий
4 Текущая работа с персоналом	ОПК-4, ОПК-5, ОПК-6	Тестирование	Примерный перечень тестовых заданий
6 Управление инцидентами ИБ	ОПК-4, ОПК-5, ОПК-6	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
7 Системы менеджмента ИБ	ОПК-4, ОПК-5, ОПК-6	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Свод правил по управлению ИБ	ОПК-4, ОПК-5, ОПК-6	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
9 Обеспечение защиты информации в экстренных ситуациях	ОПК-4, ОПК-5, ОПК-6	Контрольная работа	Примерный перечень вариантов (заданий) контрольных 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

Согласована на портале № 78246

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

Согласована на портале № 78246

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?
    1. Группы пользователей и права доступа
    2. Пользователи и группы
    3. Сервер и рабочая станция
    4. Риски и контрмеры
2. По каким угрозам в системе ГРИФ не оценивается ущерб?
    1. Конфиденциальности
    2. Целостности
    3. Достоверность
    4. Доступность
3. Какой категории угроз не представлено в системе ГРИФ?
    1. Физические угрозы человека
    2. Угрозы персонала
    3. Системные ошибки
    4. Физические угрозы
4. Какого типа экономического ущерба не существует?
    1. Долговременный экономический ущерб
    2. Кратковременный экономический ущерб
    3. Отсроченный экономический ущерб
    4. Немедленный экономический ущерб
5. По какой причине для класса группы авторизованных интернет-пользователей в системе ГРИФ не предлагается никаких средств защиты рабочего места?
    1. Для данной группы характерна минимальная вероятность реализации угрозы
    2. Для группы по умолчанию выбран набор средств защиты рабочего места
    3. Для группы неизвестно, откуда будет осуществляться доступ
    4. Для группы неизвестна степень влияния на систему
6. Какие данные нельзя указать при задании контрмер в системе ГРИФ?
    1. Стоимость внедрения
    2. Возможное снижение затрат на ИБ
    3. Срок внедрения контрмеры
    4. Название для отчета
7. Какие параметры нельзя включить в состав отчета по проекту в системе КОНДОР?
    1. Выполненные требования
    2. Невыполненные требования
    3. Риски
    4. Контрмеры
8. Какой информации не содержится в отчете по периоду, формируемом системой КОНДОР?
    1. Количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита
    2. Уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита
    3. Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
    4. Затраты на контрмеры в целом по системе для выбранного периода аудита
9. Чему по умолчанию равны вероятность в течение года и критичность реализации для только что созданной угрозы?
    1. 25 %
    2. 15 %
    3. 10 %
    4. 0 %
10. Какой информации не содержится в отчете по проекту, формируемом системой КОНДОР?
    1. Изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
    2. Изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

Согласована на портале № 78246

3. Текст выполненных требований по каждому разделу
4. Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

11. Какое количество мер защиты содержит в себе «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0»?
    1. 32
    2. 33
    3. 34
    4. 35
12. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР ИББС-1.2?
    1. Диаграмма Ганта
    2. Гистограмма
    3. Круговая диаграмма
    4. Срез структуры
13. Что понимается под базовым временем простоя ресурсов?
    1. Время необходимое на обработку информации после запроса
    2. Время отклика системы на запрос
    3. Время, в течение которого доступ к информации ресурса невозможен
    4. Время, в течение которого система загружает необходимые для работы службы
14. Что понимается под эффективностью средства защиты информации?
    1. Показатель быстродействия системы в условиях использования средств защиты информации
    2. Коэффициент снижения уровня риска по отношению к первоначальному уровню
    3. Степень влияния на защищенность информации и рабочего места группы пользователей
    4. Субъективная оценка экспертами корректности функционирования средства защиты информации
15. Что понимается под базовой вероятностью конфиденциальности?
    1. Вероятность огласки информации минимального уровня конфиденциальности в системе
    2. Минимальная вероятность реализации угрозы
    3. Максимальная вероятность реализации угрозы
    4. Вероятность огласки информации максимального уровня конфиденциальности в системе
16. Какой тип внутренних нарушителей наиболее подвержен социальной инженерии?
    1. Подрабатывающий
    2. Внедренный
    3. Манипулируемый
    4. Нелояльный
17. Что не входит перечень того, что для любой организации, серьезно относящейся к информационной безопасности, важно применять в структурном и плановом подходе ГОСТ Р 15 51630 ИСО/МЭК ТО 18044–2007?
    1. Обнаружение, оповещение об инцидентах информационной безопасности и их оценка
    2. Реагирование на инциденты информационной безопасности, включая активацию защитных мер для предотвращения, уменьшения последствий и (или) восстановление после негативных воздействий
    3. Предотвращение инцидентов информационной безопасности
    4. Извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к менеджменту инцидентов информационной безопасности
18. Что понимается под инцидентом информационной безопасности?
    1. Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости
    2. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной

Согласована на портале № 78246

безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности
3. Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности
4. Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов

19. Какому из перечисленных типов внутренних нарушителей характерна постановка задачи извне?
    1. Халатный
    2. Манипулируемый
    3. Подрабатывающий
    4. Обиженный
20. Что понимается под характеристиками группы пользователей?
    1. Состав группы пользователей
    2. Название группы пользователей
    3. Вид доступа группы пользователей
    4. Описание группы пользователей

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.

Согласована на портале № 78246

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. Темы лабораторных работ

1. Изучение Digital Secure
2. Использование Digital Secure для формирования политики безопасности организации

9.1.4. Примерный перечень вариантов (заданий) контрольных работ

1. Определение перечня актуальных угроз для адвокатского бюро
2. Определение перечня актуальных угроз для интернет магазина
3. Определение перечня актуальных угроз для банка
4. Определение перечня актуальных угроз для больницы
5. Определение перечня актуальных угроз для школы

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 9.4.

Согласована на портале № 78246

Таблица 9.4 – 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.

Согласована на портале № 78246

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 11 от «14» 12 2020 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
Декан ЗиВФ	И.В. Осипов	Согласовано, 126832c4-9aa6-45bd-8e71-e9e09d25d010

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	А.Ю. Якимук	Согласовано, 4ffdf265-fb78-4863-b293-f03438cb07cc

РАЗРАБОТАНО:

Старший преподаватель, каф. КИБЭВС	Н.С. Егошин	Разработано, fcf3535c-ecd4-4970-898f-6fb05597d34a

Согласована на портале № 78246