МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента науки и инноваций
_____ В. М. Рулевский
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Стандарты в области информационной безопасности

Уровень образования: **высшее образование - подготовка кадров высшей квалификации**
Направление подготовки / специальность: **10.06.01 Информационная безопасность**
Направленность (профиль) / специализация: **Методы и системы защиты информации, информационная безопасность**
Форма обучения: **заочная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **2**
Семестр: **3**
Учебный план набора 2015 года

Распределение рабочего времени

№	Виды учебной деятельности	3 семестр	Всего	Единицы
1	Лекции	4	4	часов
2	Практические занятия	4	4	часов
3	Всего аудиторных занятий	8	8	часов
4	Самостоятельная работа	60	60	часов
5	Всего (без экзамена)	68	68	часов
6	Подготовка и сдача зачета	4	4	часов
7	Общая трудоемкость	72	72	часов
			2.0	З.Е.

Зачет: 3 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 24.06.2015
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 47168

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «17» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.06.01 Информационная безопасность, утвержденного 30.07.2014 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Преподаватель каф. КИБЭВС _____ А. Ю. Якимук

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:

Заведующий аспирантурой _____ Т. Ю. Коротина

Доцент лаборатории безопасных биомедицинских технологий ЦТБ КИБЭВС _____ Д. Д. Зыков

Согласована на портале № 47168

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью освоения дисциплины является формирование компетенций, соответствующих требованиям Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.06.01- Информационная безопасность", утвержденного 30.07.2014 приказом Минобрнауки России № 874.

1.2. Задачи дисциплины

– изучение принципов оценки степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

– освоение навыков применения программно-аппаратных и технических средств защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности;

– исследование, создание новых и совершенствование существующие методы защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Стандарты в области информационной безопасности» (Б1.В.ДВ.2.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информационная безопасность, Методы и средства защиты информации.

Последующими дисциплинами являются: Методы и системы защиты информации, информационная безопасность, Подготовка к сдаче и сдача государственного экзамена.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-3 способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

– ПК-3 способность применять программно-аппаратные и технические средства защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности, исследовать, создавать новые и совершенствовать существующие методы защиты информации;

В результате изучения дисциплины обучающийся должен:

– **знать** стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

– **уметь** применять стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

– **владеть** навыками применения стандартов в области информационной безопасности при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		3 семестр
Аудиторные занятия (всего)	8	8

Согласована на портале № 47168

Лекции	4	4
Практические занятия	4	4
Самостоятельная работа (всего)	60	60
Проработка лекционного материала	40	40
Подготовка к практическим занятиям, семинарам	20	20
Всего (без экзамена)	68	68
Подготовка и сдача зачета	4	4
Общая трудоемкость, ч	72	72
Зачетные Единицы	2.0	

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	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
3 семестр					
1 Методы управления рисками на основе серии стандартов ИСО 27000 "Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности"	3	4	42	49	ОПК-3, ПК-3
2 Методы оценки безопасности информационных технологий в ИСО/МЭК 15408.	1	0	18	19	ОПК-3, ПК-3
Итого за семестр	4	4	60	68	
Итого	4	4	60	68	

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
3 семестр			
1 Методы управления рисками на основе серии стандартов ИСО 27000 "Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности"	Изучение стандартов:ГОСТ Р ИСО/МЭК 27000-2012 — "СМИБ. Общий обзор и терминология";ГОСТ Р ИСО/МЭК 27001-2006 — "СМИБ.Требования";ГОСТ Р ИСО/МЭК 27002-2012 — "СМИБ. Свод норм и правил менеджмента информационной безопасности";ГОСТ Р ИСО/МЭК 27003-2012 — "СМИБ. Руководство по реализации системы менеджмента информационной безопасности";ГОСТ Р ИСО/МЭК 27004-2011 — "СМИБ. Измерения";ГОСТ Р ИСО/МЭК 27005-2010 —	3	ОПК-3, ПК-3

Согласована на портале № 47168

	"СМИБ. Менеджмент риска информационной безопасности.";ГОСТ Р ИСО/МЭК 27006-2008 — "СМИБ.Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности";ГОСТ Р ИСО/МЭК 27007-2014 — "СМИБ. Руководства по аудиту систем менеджмента информационной безопасности";ГОСТ Р ИСО/МЭК 27011-2012 — "СМИБ. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002";ГОСТ Р ИСО/МЭК 27013-2014 — "СМИБ. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1";ГОСТ Р ИСО/МЭК 27031-2012 — "СМИБ. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса";ГОСТ Р ИСО/МЭК 27033-1-2011 — "СМИБ. Безопасность сетей. Часть 1. Обзор и концепции";ГОСТ Р ИСО/МЭК 27033-3-2014 — "СМИБ. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления";ГОСТ Р ИСО/МЭК 27034-1-2014 — "СМИБ. Безопасность приложений. Часть 1. Обзор и общие понятия";ISO/IEC 27035-1 — Информационные технологии — методы безопасности - управление инцидентами Информационной безопасности — Часть 1: Принципы управления инцидентами;ISO/IEC 27035-2 — Информационные технологии — методы безопасности — управление инцидентами Информационной безопасности - Часть 2: Инструкции, чтобы запланировать и подготовиться к реагированию на инциденты.		
	Итого	3	
2 Методы оценки безопасности информационных технологий в ИСО/МЭК 15408.	Изучение стандартов: ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности;ГОСТ Р	1	ОПК-3, ПК-3

Согласована на портале № 47168

	ИСО/МЭК 15408-3-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.		
	Итого	1	
Итого за семестр		4	

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
Предшествующие дисциплины		
1 Информационная безопасность	+	+
2 Методы и средства защиты информации	+	+
Последующие дисциплины		
1 Методы и системы защиты информации, информационная безопасность	+	+
2 Подготовка к сдаче и сдача государственного экзамена	+	+

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.	Прак. зан.	Сам. раб.	
ОПК-3	+	+	+	Зачет, Тест, Отчет по практическому занятию
ПК-3	+	+	+	Зачет, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции

Согласована на портале № 47168

3 семестр			
1 Методы управления рисками на основе серии стандартов ИСО 27000 "Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности"	Анализ рисков информационной безопасности на основе построения модели информационных потоков.	2	ОПК-3, ПК-3
	Анализ рисков на основе модели угроз и уязвимостей.	1	
	Анализ рисков на основе международного стандарта ISO 17799.	1	
	Итого	4	
Итого за семестр		4	

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
3 семестр				
1 Методы управления рисками на основе серии стандартов ИСО 27000 "Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности"	Подготовка к практическим занятиям, семинарам	20	ОПК-3, ПК-3	Зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	22		
	Итого	42		
2 Методы оценки безопасности информационных технологий в ИСО/МЭК 15408.	Проработка лекционного материала	18	ОПК-3, ПК-3	Зачет, Отчет по практическому занятию, Тест
	Итого	18		
Итого за семестр		60		
	Подготовка и сдача зачета	4		Зачет
Итого		64		

Согласована на портале № 47168

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: https://e.lanbook.com/book/5178 (дата обращения: 28.11.2018).

12.2. Дополнительная литература

1. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 [Электронный ресурс] [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: https://e.lanbook.com/book/5179 (дата обращения: 28.11.2018).
2. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3 [Электронный ресурс] [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 170 с. — Режим доступа: https://e.lanbook.com/book/5180 (дата обращения: 28.11.2018).
3. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 4 [Электронный ресурс] [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 214 с. — Режим доступа: https://e.lanbook.com/book/5181 (дата обращения: 28.11.2018).
4. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 5 [Электронный ресурс] [Электронный ресурс]: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 166 с. — Режим доступа: https://e.lanbook.com/book/5182 (дата обращения: 28.11.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А. Стандарты в области управления информационной безопасностью [Электронный ресурс]: практикум. – Томск: В-Спектр, 2018. – 111 с. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/yay/practstand.pdf (дата обращения: 28.11.2018).

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. 1. http://www.elibrary.ru - научная электронная библиотека;
2. 2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;

Согласована на портале № 47168

3. 3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
4. 4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

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: 28.11.2018).

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 практических занятий

Лаборатория "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 (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– VirtualBox

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;

Согласована на портале № 47168

- 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

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?
Группы пользователей и права доступа
Пользователи и группы
Сервер и рабочая станция
Риски и контрмеры
2. По каким угрозам в системе ГРИФ не оценивается ущерб?
Конфиденциальности
Целостности
Достоверность
Доступность
3. Какой категории угроз не представлено в системе ГРИФ?
Физические угрозы человека
Угрозы персонала
Системные ошибки
Физические угрозы
4. Какого типа экономического ущерба не существует?
Долговременный экономический ущерб
Кратковременный экономический ущерб
Отсроченный экономический ущерб
Немедленный экономический ущерб
5. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «нарушение бизнес-деятельности»?
Кратковременный экономический ущерб
Отсроченный экономический ущерб
Немедленный экономический ущерб
Долговременный экономический ущерб
6. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?

Согласована на портале № 47168

Не повлияет

Приравняет к нулю

Вызовет уменьшение

Вызовет рост

7. Какая из перечисленных выполняемых проверок не входит в перечень обязательных действий, входящих в руководство по реализации средств управления против злонамеренного кода?

Проверка любых файлов на электронном или оптическом носителе, а также файлов, полученных по сетям, на наличие злонамеренного кода перед использованием

Проверка web-страниц на наличие злонамеренного кода

Проверка обновлений средства управления против злонамеренного кода

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?

Для данной группы характерна минимальная вероятность реализации угрозы

Для группы по умолчанию выбран набор средств защиты рабочего места

Для группы неизвестно, откуда будет осуществляться доступ

Для группы неизвестна степень влияния на систему

9. Какие данные нельзя указать при задании контрмер в системе ГРИФ?

Стоимость внедрения

Возможное снижение затрат на ИБ

Срок внедрения контрмеры

Название для отчета

10. Какие параметры нельзя включить в состав отчета по проекту в системе КОНДОР?

Выполненные требования

Невыполненные требования

Риски

Контрмеры

11. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «подрыв репутации»?

Кратковременный экономический ущерб

Отсроченный экономический ущерб

Долговременный экономический ущерб

Немедленный экономический ущерб

12. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «снижение розничных продаж»?

Отсроченный экономический ущерб

Немедленный экономический ущерб

Кратковременный экономический ущерб

Долговременный экономический ущерб

13. Какой информации не содержится в отчете по периоду, формируемом системой КОНДОР?

Количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита

Уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита

Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

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?

25 %

15 %

10 %

Согласована на портале № 47168

0 %

15. Какой информации не содержится в отчете по проекту, формируемом системой КОНДОР?

Изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

Изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

Текст выполненных требований по каждому разделу

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»?

32

33

34

35

17. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР ИББС-1.2?

Диаграмма Ганта

Гистограмма

Круговая диаграмма

Срез структуры

18. Что понимается под базовым временем простоя ресурсов?

Время необходимое на обработку информации после запроса

Время отклика системы на запрос

Время, в течение которого доступ к информации ресурса невозможен

Время, в течение которого система загружает необходимые для работы службы

19. Фактором, значимым для использования уязвимости не является?

Время, затрачиваемое на идентификацию уязвимости

Техническая компетентность специалиста

Программное средство, требуемое для анализа

Знание проекта и функционирования объекта

20. Что понимается под эффективностью средства защиты информации?

Показатель быстродействия системы в условиях использования средств защиты информации

Коэффициент снижения уровня риска по отношению к первоначальному уровню

Степень влияния на защищенность информации и рабочего места группы пользователей

Субъективная оценка экспертами корректности функционирования средства защиты информации

21. Что понимается под базовой вероятностью конфиденциальности?

Вероятность огласки информации минимального уровня конфиденциальности в системе

Минимальная вероятность реализации угрозы

Максимальная вероятность реализации угрозы

Вероятность огласки информации максимального уровня конфиденциальности в системе

22. Какой тип внутренних нарушителей наиболее подвержен социальной инженерии?

Подрабатывающий

Внедренный

Манипулируемый

Нелояльный

23. К внешним чрезвычайным ситуациям не относятся?

Стихийные бедствия

Преступные действия

Техногенные аварии и сбои

Диверсии

Согласована на портале № 47168

24. Что не входит перечень того, что для любой организации, серьезно относящейся к информационной безопасности, важно применять в структурном и плановом подходе ГОСТ Р ИСО/МЭК ТО 18044–2007?

Обнаружение, оповещение об инцидентах информационной безопасности и их оценка

Реагирование на инциденты информационной безопасности, включая активацию защитных мер для предотвращения, уменьшения последствий и (или) восстановление после негативных воздействий

Предотвращение инцидентов информационной безопасности

Извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к менеджменту инцидентов информационной безопасности

25. Что понимается под инцидентом информационной безопасности?

Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости

Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности

Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности

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

26. К какому варианту неработоспособности относится болезнь сотрудника?

Полное прекращение выполнения сотрудником своих обязанностей

Опасность для жизни персонала

Прекращение выполнения сотрудником рутинных операций

Саботаж

27. К какой группе внешних чрезвычайных ситуаций относится скупка контрольного пакета акций?

Общественные

Правовые

Экономические

Стихийные бедствия

28. Какому из перечисленных типов внутренних нарушителей характерна постановка задачи извне?

Халатный

Манипулируемый

Подрабатывающий

Обиженный

29. Что понимается под характеристиками группы пользователей?

Состав группы пользователей

Название группы пользователей

Вид доступа группы пользователей

Описание группы пользователей

30. Какая статья расходов не входит в расходы на информационную безопасность?

Затраты на приобретение систем защиты информации

Затраты на управление системой защиты информации

Затраты на разработку политики безопасности

Затраты на обучение персонала

31. Что произойдет, если задать пороговое значение риска в 50% в системе КОНДОР?

Будут отображены все положения стандартов, риски для которых ниже 50%

Будут отображены все положения стандартов, риски для которых выше 50%

Согласована на портале № 47168

Будут отображены только критичные положения стандартов, которые не выполнены

Будут отображены только критичные положения стандартов, которые выполнены

14.1.2. Зачёт

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.

14.1.3. Вопросы для подготовки к практическим занятиям, семинарам

Анализ рисков информационной безопасности на основе построения модели информационных потоков.

Анализ рисков на основе модели угроз и уязвимостей.

Анализ рисков на основе международного стандарта ISO 17799.

Согласована на портале № 47168

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 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 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.

Согласована на портале № 47168