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
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление компьютерными инцидентами

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **2**
Семестр: **3**
Учебный план набора 2021 года

Распределение рабочего времени

№	Виды учебной деятельности	3 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: 3 семестр

Томск

Согласована на портале № 49296

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) 10.04.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. КИБЭВС _____ А. К. Новохрестов

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Согласована на портале № 49296

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины является овладение студентами основными принципами управления инцидентами информационной безопасности.

1.2. Задачи дисциплины

– Получение студентами знаний о принципах определения событий информационной безопасности (ИБ) как инцидентов ИБ.

– Получение студентами умений и навыков по оценке и реагированию на идентифицированные инциденты ИБ.

– Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление компьютерными инцидентами» (Б1.В.6) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Технологии обеспечения информационной безопасности.

Последующими дисциплинами являются: Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-12 способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

– ПК-13 способностью организовать управление информационной безопасностью;

– ПК-14 способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

В результате изучения дисциплины обучающийся должен:

– **знать** Принципы определения событий информационной безопасности (ИБ) как инцидентов ИБ. Основные методы контроля обеспечения информационной безопасности в организации.

– **уметь** Оценивать риски и реагировать на идентифицированные инциденты ИБ.

– **владеть** Навыками настройки и эксплуатации SIEM-систем.

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
		3 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

Согласована на портале № 49296

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
3 семестр					
1 Основы управления инцидентами ИБ	6	4	10	20	ПК-12, ПК-13
2 Процесс управления инцидентами ИБ	6	12	18	36	ПК-12, ПК-13, ПК-14
3 SIEM-системы	6	20	26	52	ПК-14
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
3 семестр			
1 Основы управления инцидентами ИБ	Событие информационной безопасности. Инцидент информационной безопасности. Структурный подход к менеджменту инцидентов ИБ. Этапы менеджмента инцидентов ИБ. Менеджмент и анализ рисков ИБ. Инциденты информационной безопасности и их причины.	6	ПК-12, ПК-13
	Итого	6	
2 Процесс управления инцидентами ИБ	Планирование и подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ. Структура менеджмента инцидентов ИБ. Политика менеджмента инцидентов информационной безопасности. Программа менеджмента инцидентов информационной безопасности. Политики менеджмента рисков и информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ. Обнаружение и оповещение о событиях ИБ. Оценка и принятие решений по событиям/инцидентам. Реагирование на инциденты. Анализ инцидентов ИБ и процесса менеджмента инцидентов ИБ. Улучшение анализа рисков и менеджмента ИБ.	6	ПК-12, ПК-13, ПК-14

Согласована на портале № 49296

	Итого	6	
3 SIEM-системы	Техническая и другая поддержка реагирования на инциденты информационной безопасности. Электронные базы данных событий/инцидентов ИБ и технические средства для быстрого пополнения и обновления базы данных. SIEM-системы: IBM QRadar, MaxPatrol SIEM, ArcSight, Splunk и другие. Технологические тренды развития SIEM-систем.	6	ПК-14
	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 Технологии обеспечения информационной безопасности	+		
Последующие дисциплины			
1 Преддипломная практика	+	+	+

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-12	+	+	+	Отчет по лабораторной работе, Опрос на занятиях, Зачёт, Тест
ПК-13	+	+	+	Отчет по лабораторной работе, Опрос на занятиях, Зачёт, Тест
ПК-14	+	+	+	Отчет по лабораторной работе, Опрос на занятиях, Зачёт, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Согласована на портале № 49296

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
3 семестр			
1 Основы управления инцидентами ИБ	Анализ рисков ИБ	4	ПК-13
	Итого	4	
2 Процесс управления инцидентами ИБ	Подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ	4	ПК-13
	Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ	4	
	Обнаружение и оповещение о событиях ИБ. Отчеты о событиях и инцидентах информационной безопасности	4	
	Итого	12	
3 SIEM-системы	Установка и настройка MaxPatrol SIEM. Подготовка к работе.	4	ПК-14
	Управление компьютерами в MaxPatrol SIEM.	4	
	Сбор событий в MaxPatrol SIEM	4	
	Работа с инцидентами в MaxPatrol SIEM	4	
	Работа с отчетами и мониторинг в MaxPatrol SIEM	4	
	Итого	20	
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
3 семестр				
1 Основы управления инцидентами ИБ	Проработка лекционного материала	6	ПК-12, ПК-13	Зачёт, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	10		
2 Процесс управления инцидентами ИБ	Проработка лекционного материала	6	ПК-12, ПК-13, ПК-14	Зачёт, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	12		

Согласована на портале № 49296

	Итого	18		
3 SIEM-системы	Проработка лекционного материала	6	ПК-14	Зачёт, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	20		
	Итого	26		
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
3 семестр				
Зачёт			28	28
Опрос на занятиях	4	6	6	16
Отчет по лабораторной работе	4	12	20	36
Тест			20	20
Итого максимум за период	8	18	74	100
Нарастающим итогом	8	26	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)

Согласована на портале № 49296

	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью». Выпуск 1 [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. – М.: Горячая линия- Телеком, 2012. – 244 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5178 (дата обращения: 30.08.2020).

12.2. Дополнительная литература

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200068822 (дата обращения: 30.08.2020).
2. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — Режим доступа: https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-450371 (дата обращения: 30.08.2020).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Информационные технологии в управлении [Электронный ресурс]: Методические указания по выполнению лабораторных и самостоятельных работ / И. Г. Афанасьева - 2018. 75 с. — Режим доступа: https://edu.tusur.ru/publications/7868 (дата обращения: 30.08.2020).

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. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю
2. Дополнительно рекомендуется использовать информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

Согласована на портале № 49296

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

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:

- MaxPatrol Education
- Microsoft Windows 10
- VirtualBox
- Visio

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы),

Согласована на портале № 49296

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

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?

Согласована на портале № 49296

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?
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

Согласована на портале № 49296

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 %

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

ББС-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

Согласована на портале № 49296

Степень влияния на защищенность информации и рабочего места группы пользователей

Субъективная оценка экспертами корректности функционирования средства защиты информации

14.1.2. Темы опросов на занятиях

Событие информационной безопасности. Инцидент информационной безопасности. Структурный подход к менеджменту инцидентов ИБ. Этапы менеджмента инцидентов ИБ. Менеджмент и анализ рисков ИБ. Инциденты информационной безопасности и их причины.

Планирование и подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ. Структура менеджмента инцидентов ИБ. Политика менеджмента инцидентов информационной безопасности. Программа менеджмента инцидентов информационной безопасности. Политики менеджмента рисков и информационной безопасности. Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ. Обнаружение и оповещение о событиях ИБ. Оценка и принятие решений по событиям/инцидентам. Реагирование на инциденты. Анализ инцидентов ИБ и процесса менеджмента инцидентов ИБ. Улучшение анализа рисков и менеджмента ИБ.

Техническая и другая поддержка реагирования на инциденты информационной безопасности. Электронные базы данных событий/инцидентов ИБ и технические средства для быстрого пополнения и обновления базы данных. SIEM-системы: IBM QRadar, MaxPatrol SIEM, ArcSight, Splunk и другие. Технологические тренды развития SIEM-систем.

14.1.3. 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.

Согласована на портале № 49296

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.

14.1.4. Темы лабораторных работ

Анализ рисков ИБ

Подготовка к менеджменту инцидентов ИБ. Политика обработки сообщений о событиях и инцидентах ИБ

Создание группы реагирования на инциденты информационной безопасности. Использование системы менеджмента инцидентов ИБ

Обнаружение и оповещение о событиях ИБ. Отчеты о событиях и инцидентах информационной безопасности

Установка и настройка MaxPatrol SIEM. Подготовка к работе.

Управление компьютерами в MaxPatrol SIEM.

Сбор событий в MaxPatrol SIEM

Работа с инцидентами в MaxPatrol SIEM

Работа с отчетами и мониторинг в MaxPatrol SIEM

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;

Согласована на портале № 49296

– 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 № 49296