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

Методы и средства защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
1	Лекции	20	20	40	часов
2	Лабораторные работы	36	36	72	часов
3	Всего аудиторных занятий	56	56	112	часов
4	Самостоятельная работа	52	52	104	часов
5	Всего (без экзамена)	108	108	216	часов
6	Общая трудоемкость	108	108	216	часов
		3.0	3.0	6.0	З.Е.

Зачёт: 7 семестр
Зачёт с оценкой: 8 семестр

Томск

Согласована на портале № 50115

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) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. КИБЭВС _____ А. Ю. Якимук

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 № 50115

1. Цели и задачи дисциплины

1.1. Цели дисциплины

формирование у студентов представлений о методах и средствах, применяющихся для обеспечения информационной безопасности.

1.2. Задачи дисциплины

- изучить методы и средства защиты информации в ОС и корпоративных сетях;
- средства криптографической защиты информации;
- принципы управления средствами защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства защиты информации» (Б1.Б.04.04) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Методы и средства защиты информации.

Последующими дисциплинами являются: Защищенный электронный документооборот, Управление информационной безопасностью, Методы и средства защиты информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПСК-2 способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа;

В результате изучения дисциплины обучающийся должен:

- **знать** основные методы и средства защиты информации, используемые для обеспечения безопасности в операционной системе и компьютерных сетях.
- **уметь** устанавливать и настраивать средства защиты информации в операционных системах; анализировать защищенность корпоративных сетей; эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах
- **владеть** навыками работы как с штатными, так и с сторонними средствами защиты информации в операционной системе и корпоративных сетях.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		7 семестр	8 семестр
Аудиторные занятия (всего)	112	56	56
Лекции	40	20	20
Лабораторные работы	72	36	36
Самостоятельная работа (всего)	104	52	52
Выполнение индивидуальных заданий	16	8	8
Оформление отчетов по лабораторным работам	60	30	30
Проработка лекционного материала	28	14	14
Всего (без экзамена)	216	108	108
Общая трудоемкость, ч	216	108	108
Зачетные Единицы	6.0	3.0	3.0

Согласована на портале № 50115

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
7 семестр					
1 Основные понятия и положения защиты информации	2	0	2	4	ПСК-2
2 Основы защиты информации в операционной системе	6	20	26	52	ПСК-2
3 Основы криптографической защиты информации	6	8	12	26	ПСК-2
4 Основы защиты информации в компьютерных сетях	6	8	12	26	ПСК-2
Итого за семестр	20	36	52	108	
8 семестр					
5 Средства защиты информации в операционной системе	6	12	16	34	ПСК-2
6 Средства криптографической защиты информации	6	8	12	26	ПСК-2
7 Средства защиты информации в корпоративных сетях	6	8	14	28	ПСК-2
8 Управление средствами защиты информации	2	8	10	20	ПСК-2
Итого за семестр	20	36	52	108	
Итого	40	72	104	216	

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
7 семестр			
1 Основные понятия и положения защиты информации	Предмет защиты информации. Объект защиты информации. Понятие угрозы безопасности. Классификация угроз информационной безопасности. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации.	2	ПСК-2
	Итого	2	
2 Основы защиты	Назначение и функции ОС и ее подси-	6	ПСК-2

Согласована на портале № 50115

информации в операционной системе	стем. Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС. Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.		
	Итого	6	
3 Основы криптографической защиты информации	Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования. Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля.	6	ПСК-2
	Итого	6	
4 Основы защиты информации в компьютерных сетях	Основные понятия и терминология. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность. Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях	6	ПСК-2
	Итого	6	
Итого за семестр		20	
8 семестр			
5 Средства защиты информации в операционной системе	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Классификация субъектов и объектов доступа. Права доступа. Методы разграничения доступа. Разграничение доступа к файловым объектам. Наследование разрешений. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения.	6	ПСК-2
	Итого	6	
6 Средства криптографической защиты информации	Криптографические протоколы: общие понятия. Управление секретными ключами. Распределение секретных ключей. Понятие электронной подписи. Управление открытыми ключами. Основные	6	ПСК-2

Согласована на портале № 50115

	компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа.		
	Итого	6	
7 Средства защиты информации в корпоративных сетях	Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет. Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети. Уязвимости и защита базовых протоколов и служб:Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности. Классы сканеров безопасности и особенности применения. Защита от вирусов. Защита электронного документооборота.	6	ПСК-2
	Итого	6	
8 Управление средствами защиты информации	Принципы построения средств защиты информации; основные механизмы защиты; аппаратные средства; конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати. Управление серверами администрирования; управление группами администрирования; управление клиентскими компьютерами; работа с отчетами, статистикой.	2	ПСК-2
	Итого	2	
Итого за семестр		20	
Итого		40	

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	4	5	6	7	8
Предшествующие дисциплины								
1 Информатика		+						
2 Организационное и правовое обеспечение информационной	+							+

Согласована на портале № 50115

безопасности								
3 Основы информационной безопасности	+	+	+	+	+	+	+	+
4 Методы и средства защиты информации	+	+	+	+	+	+	+	+
Последующие дисциплины								
1 Защищенный электронный документооборот	+	+	+	+		+	+	
2 Управление информационной безопасностью								+
3 Методы и средства защиты информации	+	+	+	+	+	+	+	+

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.	
ПСК-2	+	+	+	Конспект самоподготовки, Отчет по лабораторной работе, Зачёт, Тест, Зачёт с оценкой

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
2 Основы защиты информации в операционной системе	Администрирование учетных записей в ОС Windows	4	ПСК-2
	Дискреционный механизм разграничения доступа к файловым объектам	4	
	Разграничение доступа к запуску программного обеспечения	4	
	Аудит событий безопасности операционной системы	4	
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	4	
	Итого	20	
3 Основы криптографической защиты информации	Криптографическая защита объектов файловой системы в ОС Windows	4	ПСК-2
	Применение шифрования и электронной	4	

Согласована на портале № 50115

	подписи в электронном документообороте		
	Итого	8	
4 Основы защиты информации в компьютерных сетях	Одноранговые сети	4	ПСК-2
	Настройка домена на примере Active Directory	4	
	Итого	8	
Итого за семестр		36	
8 семестр			
5 Средства защиты информации в операционной системе	Многофакторная аутентификация с помощью физического объекта	4	ПСК-2
	Разграничение доступа к устройствам	4	
	Мандатный механизм разграничения доступа к файловым объектам	4	
	Итого	12	
6 Средства криптографической защиты информации	Применение криптопровайдеров на автоматизированном рабочем месте	4	ПСК-2
	Применение средств криптографической защиты информации на автоматизированном рабочем месте	4	
	Итого	8	
7 Средства защиты информации в корпоративных сетях	Межсетевые экраны	4	ПСК-2
	Виртуальные защищенные сети	4	
	Итого	8	
8 Управление средствами защиты информации	Применение средств защиты информации для контроля целостности ОС	4	ПСК-2
	Централизованная защита от вирусов в локальной сети	4	
	Итого	8	
Итого за семестр		36	
Итого		72	

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
7 семестр				
1 Основные понятия и положения защиты информации	Проработка лекционного материала	2	ПСК-2	Зачёт, Тест
	Итого	2		

Согласована на портале № 50115

2 Основы защиты информации в операционной системе	Проработка лекционного материала	4	ПСК-2	Зачёт, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	14		
	Выполнение индивидуальных заданий	8		
	Итого	26		
3 Основы криптографической защиты информации	Проработка лекционного материала	4	ПСК-2	Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Итого	12		
4 Основы защиты информации в компьютерных сетях	Проработка лекционного материала	4	ПСК-2	Зачёт, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Итого	12		
Итого за семестр		52		
8 семестр				
5 Средства защиты информации в операционной системе	Проработка лекционного материала	4	ПСК-2	Зачёт с оценкой, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	12		
	Итого	16		
6 Средства криптографической защиты информации	Проработка лекционного материала	4	ПСК-2	Зачёт с оценкой, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Выполнение индивидуальных заданий	4		
	Итого	12		
7 Средства защиты информации в корпоративных сетях	Проработка лекционного материала	4	ПСК-2	Зачёт с оценкой, Конспект самоподготовки, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	6		
	Выполнение индивидуальных заданий	4		
	Итого	14		
8 Управление средствами защиты информации	Проработка лекционного материала	2	ПСК-2	Зачёт с оценкой, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Итого	10		

Согласована на портале № 50115

Итого за семестр	52		
Итого	104		

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
7 семестр				
Зачёт			30	30
Конспект самоподготовки			10	10
Отчет по лабораторной работе	15	15	15	45
Тест			15	15
Итого максимум за период	15	15	70	100
Нарастающим итогом	15	30	100	100
8 семестр				
Зачёт с оценкой			30	30
Конспект самоподготовки			10	10
Отчет по лабораторной работе	15	15	15	45
Тест			15	15
Итого максимум за период	15	15	70	100
Нарастающим итогом	15	30	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.

Согласована на портале № 50115

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

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

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Осипян В. О. Криптография в задачах и упражнениях. - М. : Гелиос АРВ , 2004. - 143[1] с. (наличие в библиотеке ТУСУР - 50 экз.)

2. Основы информационной безопасности : Учебное пособие для вузов. - М. : Горячая линия-Телеком , 2006. - 544 с. (наличие в библиотеке ТУСУР - 81 экз.)

3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] [Электронный ресурс] [Электронный ресурс]: учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 338 с. — Режим доступа: https://e.lanbook.com/book/63235 (дата обращения: 03.03.2021).

4. Построение защищенных корпоративных сетей [Электронный ресурс] [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 250 с. [Электронный ресурс] - Режим доступа: — Режим доступа: https://e.lanbook.com/book/66472 (дата обращения: 03.03.2021).

12.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с (наличие в библиотеке ТУСУР - 30 экз.)

2. Компьютерные сети и службы удаленного доступа [Электронный ресурс] [Электронный ресурс]: справочник / О. Ибе. — Электрон. дан. — Москва : ДМК Пресс, 2007. — 336 с. [Электронный ресурс] - Режим доступа: — Режим доступа: https://e.lanbook.com/book/1169 (дата обращения: 03.03.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Методы и средства защиты информации [Электронный ресурс]: методические рекомендации для лабораторных и самостоятельных работ / Якимук А.Ю., Новохрестов А.К., Конев А.А. - 359 с. [Электронный ресурс] - Режим доступа: — Режим доступа: https://disk.fb.tusur.ru/miszi/laboratory_work.pdf (дата обращения: 03.03.2021).

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

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

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Согласована на портале № 50115

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. http://www.elibrary.ru - научная электронная библиотека;
2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
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: 03.03.2021).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

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

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

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:

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (14 шт.);
- Обучающий стенд локальные компьютерные сети Microtik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- 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:

- 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;

Согласована на портале № 50115

- 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.

Стенды для изучения средств криптографической защиты информации в банковском деле, 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 криптографической защиты информации: программно-аппаратный комплекс шифрования «ФПСУ-IP», программно-аппаратный комплекс шифрования «ФПСУ-IP/Клиент»;

- Комплект специализированной учебной мебели;

- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– Microsoft Windows 10
– Межсетевой экран ИКС Lite

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

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

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;

- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;

- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;

- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;

- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;

- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;

- OpenOffice;

- Kaspersky Endpoint Security 10 для Windows;

- 7-Zip;

- Google Chrome.

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

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

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

Согласована на портале № 50115

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. Какая файловая система должна быть на диске, к ресурсам которого необходимо присвоить категорию конфиденциальности в Secret Net?

exFAT

UDF

NTFS

FAT32

2. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?

Идентификатор продукта

Идентификатор производителя

Страна изготовитель

Серийный номер

3. Под каким уровнем конфиденциальности необходимо войти в систему администратору, чтобы Secret Net позволила ему изменять параметры операционной системы?

Высший (строго конфиденциально)

Средний (конфиденциально)

Низший (не конфиденциально)

Администратору можно проводить настройки под любым уровнем

4. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?

Домен

Логин

Согласована на портале № 50115

Пин-код

Пароль

5. Какая из моделей разграничения доступа не применяется в Secret Net?

Дискреционная модель

Мандатная модель

Ролевая модель

Применяются все перечисленные модели

6. Каким образом предоставить полный доступ для любой клавиатуры, подключенной к системе с установленным запретом доступа к usb-портам в DeviceLock?

Внести клавиатуру в белый список как Unique Device

Внести клавиатуру в белый список как Device Model

Отключить управление доступом к USB HID в настройках безопасности программы

Любой из перечисленных вариантов

7. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?

Монитор IP-безопасности

Системный монитор

Анализ и настройка безопасности

Редактор объектов групповой политики

8. Какое действие не фиксируется при аудите системных событий?

Запуск элементов системы безопасности

Отключение элементов системы безопасности

Присвоение привилегий пользователю

Изменение системного времени

9. Какие права предоставляются пользователю при мандатном разграничении доступа в случае, если уровень конфиденциальности файла ниже уровня сеанса пользователя?

Запись

Смена владельца

Чтение

Согласована на портале № 50115

Изменение разрешений

10. Какой группы настроек нет в шаблоне безопасности?

Файловая система

Системные службы

Политика паролей

Политики учетных записей

11. Что из нижеперечисленного является группой настроек в шаблоне безопасности?

Отладка программ

Создание файла подкачки

Локальные политики

Архивация файлов и каталогов

12. Какого типа результатов анализа параметров безопасности операционной системы не существует?

Элемент определен в базе и в системе, значения совпадают

Элемент определен в базе и в системе, значения не совпадают

Элемент отсутствует в базе и в системе

Элемент не анализировался

13. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?

Файл

Каталог

Учетная запись

Ключ реестра

14. В результате какого действия программа, запрещенная правилом хеша, будет запущена?

Программу перенесли в другую папку

Программу переименовали

Программу изменили или заменили на другую версию

Программу разрешили правилом сертификата

Согласована на портале № 50115

15. С помощью какого правила в политике ограниченного использования программ можно запретить запуск любых приложений от одного производителя?

Правилом пути

Правилом хеша

Правилом сертификата

Правилом зон интернета

16. Принцип работы какого разрешения характеризуется возможностью создавать файлы, но невозможностью их изменять или удалять?

Чтение

Чтение и выполнение

Запись

Список содержимого папки

17. Отсутствие настройки по какому параметру может привести к бесполезности параметра «Требовать неповторяемости паролей»?

Максимальный срок действия пароля

Минимальная длина пароля

Минимальный срок действия пароля

Пароль должен отвечать требованиям сложности

18. Чем обусловлено требование неповторяемости паролей?

Пароль не должен повторять логин пользователя

У всех пользователей должны быть разные пароли

Пароль должен отличаться от нескольких предыдущих

В пароле не должно быть одинаковых сегментов

19. Какая из перечисленных возможностей доступна администратору eToken?

Инициализация eToken

Присвоение имени eToken

Задать новый PIN-код eToken, если пользователь забыл его

Просмотр содержимого eToken

20. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблоки-

Согласована на портале № 50115

рованы?

Аудит успеха

Аудит разрешений

Аудит запрета

Аудит отказа

14.1.2. Зачёт

Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.

Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?

В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?

Охарактеризуйте дискреционную модель управления доступом.

Раскройте понятие наследования разрешений.

Как создать политику ограниченного использования программ?

В чем основное преимущество правила хеша перед правилом пути?

Приведите три примера использования приоритета правил.

Какие типы объектов могут подвергаться фиксации при аудите доступа к объектам? Какие при этом фиксируются данные?

Каким образом происходит настройка аудита доступа к объектам?

Каким образом при помощи встроенных средств операционной системы Windows XP можно осуществлять контроль целостности настроек, связанных с информационной безопасностью?

Что такое «Шаблон безопасности»?

Для чего предназначена оснастка «Анализ и настройка безопасности»?

Опишите алгоритм работы шифрованной файловой системы Windows.

Что такое TPM?

Для чего нужна электронная подпись?

Для чего предназначены секретный и открытый ключи шифрования?

Что такое одноранговая сеть?

Каковы достоинства и недостатки одноранговых сетей?

Что такое удаленный доступ?

Что такое домен?

Сколько компьютеров может находиться в домене?

Что понимается под групповой политикой?

В чем различие между локальными политиками безопасности и групповыми политиками домена?

Какова структура объекта групповой политики, в какой последовательности применяются разделы объекта групповой политики?

Каково назначение административных шаблонов в групповой политике, как создать новый административный шаблон?

Для кого чего можно применять режимы планирования и ведения журналов?

Для чего нужен журнал паролей?

Что содержится в контейнере Конфигурация программ?

Что содержится в контейнере Конфигурация Windows?

14.1.3. Вопросы на самоподготовку

Виртуальные машины

Управление ресурсами в ОС Windows

Управление системными службами и процессами в ОС Windows

Криптографическая защита объектов файловой системы в ОС Ubuntu

Согласована на портале № 50115

Высокоуровневые сетевые службы

14.1.4. Вопросы для зачёта с оценкой

Основные группы механизмов защиты операционных систем; основные функции этих механизмов.

Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.

Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.

Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.

Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.

Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.

Задачи механизмов управления доступом.

Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.

Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.

Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.

Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.

Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.

Белый список устройств и способы его применения.

Аудит в операционных системах. Задачи аудита.

События, подвергаемые аудиту в ОС Windows.

Состав шаблона безопасности в ОС Windows.

Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows.

Какие протоколы поддерживает IIS?

Что такое HTTP-сервер?

Что такое FTP-сервер?

Что такое VPN?

Какие существуют уровни протоколов защищенного канала?

По какому параметру обычно классифицируют VPN?

Чем отличаются виртуальные машины для сервера и клиента?

Какие типы ключей есть в OpenVPN?

Что такое файловый контейнер?

Чем отличается скрытый том от обычного?

Для чего необходима очистка диска при шифровании системного диска?

Что такое криптопровайдер?

14.1.5. Темы лабораторных работ

Криптографическая защита объектов файловой системы в ОС Windows

Администрирование учетных записей в ОС Windows

Дискреционный механизм разграничения доступа к файловым объектам

Разграничение доступа к запуску программного обеспечения

Аудит событий безопасности операционной системы

Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты

Применение шифрования и электронной подписи в электронном документообороте

Многофакторная аутентификация с помощью физического объекта

Разграничение доступа к устройствам

Мандатный механизм разграничения доступа к файловым объектам

Применение криптопровайдеров на автоматизированном рабочем месте

Согласована на портале № 50115

Одноранговые сети
Настройка домена на примере Active Directory
Межсетевые экраны
Виртуальные защищенные сети
Применение средств криптографической защиты информации на автоматизированном рабочем месте
Применение средств защиты информации для контроля целостности ОС
Централизованная защита от вирусов в локальной сети

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:

Согласована на портале № 50115

– 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 № 50115