

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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



УТВЕРЖДАЮ  
Проректор по учебной работе

Документ подписан электронной подписью

Сертификат: 1с6сfa0a-52a6-4f49-aef0-5584d3fd4820

Владелец: Троян Павел Ефимович

Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

**Безопасность операционных систем**

Уровень образования: **высшее образование - специалитет**

Направление подготовки (специальность): **38.05.01 Экономическая безопасность**

Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **3**

Семестр: **5**

Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	32	32	часов
3	Всего аудиторных занятий	50	50	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	22	22	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	3.Е

Зачет: 5 семестр

Томск 2017

## ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16 января 2017 года, рассмотрена и утверждена на заседании кафедры « \_\_\_ » \_\_\_\_\_ 20\_\_ года, протокол № \_\_\_\_\_.

Разработчики:

мнс каф. КИБЭВС

\_\_\_\_\_ А. Ю. Якимук

доцент каф. КИБЭВС

\_\_\_\_\_ А. А. Конев

Заведующий обеспечивающей каф.  
КИБЭВС

\_\_\_\_\_ А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ

\_\_\_\_\_ Е. М. Давыдова

Заведующий выпускающей каф.  
КИБЭВС

\_\_\_\_\_ А. А. Шелупанов

Эксперт:

доцент каф. КИБЭВС

\_\_\_\_\_ А. А. Конев

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью дисциплины «Безопасность операционных систем» является освоение принципов построения современных операционных систем (ОС) и принципов администрирования подсистемы защиты информации в ОС.

### 1.2. Задачи дисциплины

- Задачи изучения дисциплины – получение студентами:
- – знаний о методах несанкционированного доступа (НСД) к ресурсам ОС;
- – знаний о структуре подсистемы защиты в ОС;
- – навыков использования средств и методов защиты от НСД к ресурсам ОС.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность операционных систем» (Б1.В.ОД.17) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Информационная безопасность в локальных и распределенных вычислительных сетях.

## 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 студент должен:

- **знать** – основные виды и угрозы безопасности операционных систем; – защитные механизмы и средства обеспечения безопасности операционных систем.
- **уметь** – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.
- **владеть** – профессиональной терминологией в области 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
		5 семестр
Аудиторные занятия (всего)	50	50
Лекции	18	18
Лабораторные работы	32	32
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	22	22
Подготовка к контрольным работам	2	2
Оформление отчетов по лабораторным работам	12	12
Проработка лекционного материала	8	8
Всего (без экзамена)	72	72
Общая трудоемкость ч	72	72
Зачетные Единицы	2.0	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	Лекции	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
5 семестр					
1 Основные механизмы обеспечения безопасности ОС	2	0	2	4	ПСК-2
2 Средства и методы аутентификации в ОС	4	8	6	18	ПСК-2
3 Разграничение доступа к ресурсам ОС	6	16	6	28	ПСК-2
4 Контроль работы подсистемы защиты	4	8	6	18	ПСК-2
5 Контрольная работа и обсуждение ее результатов	2	0	2	4	ПСК-2
Итого за семестр	18	32	22	72	
Итого	18	32	22	72	

### 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
5 семестр			
1 Основные механизмы обеспечения безопасности ОС	Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.	2	ПСК-2
	Итого	2	
2 Средства и методы аутентификации в ОС	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.	4	ПСК-2
	Итого	4	
3 Разграничение доступа к ресурсам ОС	Классификация субъектов и объектов доступа. Права доступа. Методы раз-	6	ПСК-2

	граничения доступа. Разграничение доступа к файловым объектам. Наследование разрешений. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения.		
	Итого	6	
4 Контроль работы подсистемы защиты	Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.	4	ПСК-2
	Итого	4	
5 Контрольная работа и обсуждение ее результатов	Обсуждение результатов контрольной работы	2	ПСК-2
	Итого	2	
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	4	5
Предшествующие дисциплины					
1 Информатика			+	+	
2 Основы информационной безопасности	+	+	+	+	
Последующие дисциплины					
1 Информационная безопасность в локальных и распределенных вычислительных сетях	+	+	+	+	

### 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 и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Лабораторные работы	Самостоятельная работа	

ПСК-2	+	+	+	Проверка контрольных работ, Отчет по лабораторной работе, Опрос на занятиях, Зачет
-------	---	---	---	--

### 6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные лабораторные занятия	Интерактивные лекции	Всего
5 семестр			
IT-методы	4		4
IT-методы	10		10
Презентации с использованием мультимедиа с обсуждением		6	6
Итого за семестр:	14	6	20
Итого	14	6	20

### 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
5 семестр			
2 Средства и методы аутентификации в ОС	Аутентификация в операционных системах при помощи физического объекта	4	ПСК-2
	Двухфакторная аутентификация в программном обеспечении на основе технологии SSO	4	
	Итого	8	
3 Разграничение доступа к ресурсам ОС	Дискреционный механизм разграничения доступа к файловым объектам	4	ПСК-2
	Мандатный механизм разграничения доступа к файловым объектам	4	
	Разграничение доступа к устройствам	4	
	Разграничение доступа к запуску программного обеспечения	4	
	Итого	16	
4 Контроль работы подсистемы защиты	Аудит событий безопасности операционной системы	4	ПСК-2
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	4	

	Итого	8	
Итого за семестр		32	

### 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
<b>5 семестр</b>				
1 Основные механизмы обеспечения безопасности ОС	Проработка лекционного материала	2	ПСК-2	Зачет
	Итого	2		
2 Средства и методы аутентификации в ОС	Проработка лекционного материала	2	ПСК-2	Зачет, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
3 Разграничение доступа к ресурсам ОС	Проработка лекционного материала	2	ПСК-2	Зачет, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
4 Контроль работы подсистемы защиты	Проработка лекционного материала	2	ПСК-2	Зачет, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
5 Контрольная работа и обсуждение ее результатов	Подготовка к контрольным работам	2	ПСК-2	Проверка контрольных работ
	Итого	2		
Итого за семестр		22		
Итого		22		

### 10. Курсовая работа (проект)

Не предусмотрено РУП

### 11. Рейтинговая система для оценки успеваемости студентов

#### 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	Максимальный балл за период	Максимальный балл за период	Всего за семестр
-------------------------------	--------------------------------	-----------------------------	-----------------------------	------------------

	начала семестра	между 1КТ и 2КТ	между 2КТ и на конец семестра	
5 семестр				
Зачет			30	30
Опрос на занятиях	5	5	5	15
Отчет по лабораторной работе	10	15	15	40
Проверка контрольных работ			15	15
Итого максимум за пери- од	15	20	65	100
Нарастающим итогом	15	35	100	100

### 11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

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

### 11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

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

## 12. Учебно-методическое и информационное обеспечение дисциплины

### 12.1. Основная литература

1. Операционные системы : Учебное пособие / О. М. Раводин, В. О. Раводин ; Министерство образования Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 165[3] с. : ил. - Библиогр.: с. 163-165. (наличие в библиотеке ТУСУР - 26 экз.)

### 12.2. Дополнительная литература

1. Робачевский А.М. Операционная система UNIX: Учебное пособие для вузов. – СПб.:



ВНУ–Санкт-Петербург, 2002. – 514 с. (наличие в библиотеке ТУСУР - 17 экз.)

2. Гордеев А.В. Операционные системы: Учебник для вузов. – 2-е изд. – СПб.: Питер, 2004. – 415 с. (наличие в библиотеке ТУСУР - 17 экз.)

3. Олифер В.Г., Олифер Н.А. Сетевые операционные системы: Учебник для вузов. – СПб.: Питер, 2007. – 538 с. (наличие в библиотеке ТУСУР - 10 экз.)

4. Раводин О.М., Раводин В.О. Безопасность операционных систем: Учебное пособие. – 2-е изд., перераб. и доп. – Томск: В-Спектр, 2006. – 226 с. (наличие в библиотеке ТУСУР - 80 экз.)

### **12.3 Учебно-методические пособия**

#### **12.3.1. Обязательные учебно-методические пособия**

1. Конев А.А. Безопасность операционных систем: презентации по курсу лекций (часть 1) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-1-lect.pdf>

2. Конев А.А. Безопасность операционных систем: презентации по курсу лекций (часть 2) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-2-lect.pdf>

3. Конев А.А. Безопасность операционных систем: методические указания по выполнению лабораторных работ. Часть 1 [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/os-lab.pdf>

4. Конев А.А. Безопасность операционных систем: методические указания по выполнению лабораторных работ. Часть 2 [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-lab.pdf>

5. Конев А.А. Безопасность операционных систем: методические указания по выполнению практических работ [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/os-pract.pdf>

6. Конев А.А. Безопасность операционных систем: вопросы к контрольной работе (1-й семестр) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-1-kontr.pdf>

7. Конев А.А. Безопасность операционных систем: вопросы к контрольной работе (2-й семестр) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-2-kontr.pdf>

8. Конев А.А. Безопасность операционных систем: вопросы к экзамену [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-2-exam.pdf>

#### **12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья**

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение**

1. Не предусмотрено

## **13. Материально-техническое обеспечение дисциплины**

### **13.1. Общие требования к материально-техническому обеспечению дисциплины**

#### **13.1.1. Материально-техническое обеспечение для лекционных занятий**

Для проведения лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 808. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Аудиосистема – 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор Optoma – 1

шт.; Компьютер лекционный ASUS ASRock AMD E2-1800/4 ГБ – 1 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 7 SP1; Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

### **13.1.2. Материально-техническое обеспечение для лабораторных работ**

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель;– 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

### **13.1.3. Материально-техническое обеспечение для самостоятельной работы**

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

## **13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья**

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеомониторов для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

## **14. Фонд оценочных средств**

### **14.1. Основные требования к фонду оценочных средств и методические рекомендации**

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

### **14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья**

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

**Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью**

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету,	Преимущественно письменная проверка

	контрольные работы	
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 средствам для лиц с ограниченными возможностями здоровья**

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

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

УТВЕРЖДАЮ  
Проректор по учебной работе  
\_\_\_\_\_ П. Е. Троян  
«\_\_» \_\_\_\_\_ 20\_\_ г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**

**Безопасность операционных систем**

Уровень образования: **высшее образование - специалитет**

Направление подготовки (специальность): **38.05.01 Экономическая безопасность**

Направленность (профиль): **Экономико-правовое обеспечение экономической безопасности**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **3**

Семестр: **5**

Учебный план набора 2016 года

Разработчики:

- мнс каф. КИБЭВС А. Ю. Якимук
- доцент каф. КИБЭВС А. А. Конев

Зачет: 5 семестр

Томск 2017

## 1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПСК-2	способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа	Должен знать – основные виды и угрозы безопасности операционных систем; – защитные механизмы и средства обеспечения безопасности операционных систем.; Должен уметь – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.; Должен владеть – профессиональной терминологией в области информационной безопасности.;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

## 2 Реализация компетенций

### 2.1 Компетенция ПСК-2

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

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	– основные виды и угрозы безопасности операционных систем; – защитные механизмы и средства обеспечения безопасности операционных систем.	– использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.	– профессиональной терминологией в области информационной безопасности.
Виды занятий	<ul style="list-style-type: none"> <li>• Интерактивные лабораторные занятия;</li> <li>• Интерактивные лекции;</li> <li>• Лабораторные работы;</li> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>• Интерактивные лабораторные занятия;</li> <li>• Интерактивные лекции;</li> <li>• Лабораторные работы;</li> <li>• Лекции;</li> <li>• Самостоятельная работа;</li> </ul>	<ul style="list-style-type: none"> <li>• Интерактивные лабораторные занятия;</li> <li>• Лабораторные работы;</li> <li>• Самостоятельная работа;</li> </ul>
Используемые средства оценивания	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Опрос на занятиях;</li> <li>• Зачет;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Опрос на занятиях;</li> <li>• Зачет;</li> </ul>	<ul style="list-style-type: none"> <li>• Отчет по лабораторной работе;</li> <li>• Зачет;</li> </ul>

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	<ul style="list-style-type: none"> <li>• знает в полном объеме основные виды и угрозы безопасности операционных систем;</li> <li>• знает в полном объеме как оценить защитные механизмы и средства обеспечения безопасности операционных систем;</li> </ul>	<ul style="list-style-type: none"> <li>• умеет в полном объеме использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;</li> </ul>	<ul style="list-style-type: none"> <li>• в полном объеме владеет профессиональной терминологией в области информационной безопасности;</li> </ul>
Хорошо (базовый уровень)	<ul style="list-style-type: none"> <li>• знает на продвинутом уровне основные виды и угрозы безопасности операционных систем;</li> <li>• знает на продвинутом уровне как оценить защитные механизмы и средства обеспечения безопасности операционных систем;</li> </ul>	<ul style="list-style-type: none"> <li>• умеет на продвинутом уровне использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;</li> </ul>	<ul style="list-style-type: none"> <li>• на продвинутом уровне владеет профессиональной терминологией в области информационной безопасности;</li> </ul>
Удовлетворительно (пороговый уровень)	<ul style="list-style-type: none"> <li>• знает на базовом уровне основные виды и угрозы безопасности операционных систем;</li> </ul>	<ul style="list-style-type: none"> <li>• умеет на базовом уровне использовать средства операционных систем для обеспечения</li> </ul>	<ul style="list-style-type: none"> <li>• на базовом уровне владеет профессиональной терминологией в области информацион-</li> </ul>

	<ul style="list-style-type: none"> <li>• знает на базовом уровне как оценить защитные механизмы и средства обеспечения безопасности операционных систем;</li> </ul>	<p>эффективного и безопасного функционирования автоматизированных систем;</p>	<p>ной безопасности;</p>
--	---	---	--------------------------

### 3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

#### 3.1 Зачёт

- Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.
- Методы биометрической аутентификации.
- Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.
- Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки. Применение физического объекта в технологии SSO.
- Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.
- Основные группы механизмов защиты операционных систем; основные функции этих механизмов.

#### 3.2 Темы контрольных работ

- Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.
- Основные группы механизмов защиты операционных систем; основные функции этих механизмов.

#### 3.3 Темы опросов на занятиях

- Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.
- Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.
- 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.
- Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.

#### 3.4 Темы лабораторных работ

- Аутентификация в операционных системах при помощи физического объекта
- Двухфакторная аутентификация в программном обеспечении на основе технологии SSO
- Дискреционный механизм разграничения доступа к файловым объектам
- Мандатный механизм разграничения доступа к файловым объектам
- Разграничение доступа к устройствам
- Разграничение доступа к запуску программного обеспечения
- Аудит событий безопасности операционной системы
- Анализ, настройка и контроль целостности параметров безопасности подсистемы защи-

ты

## 4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, согласно п. 12 рабочей программы.

### 4.1. Основная литература

1. Операционные системы : Учебное пособие / О. М. Раводин, В. О. Раводин ; Министерство образования Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 165[3] с. : ил. - Библиогр.: с. 163-165. (наличие в библиотеке ТУСУР - 26 экз.)

### 4.2. Дополнительная литература

1. Робачевский А.М. Операционная система UNIX: Учебное пособие для вузов. – СПб.: ВHV–Санкт-Петербург, 2002. – 514 с. (наличие в библиотеке ТУСУР - 17 экз.)

2. Гордеев А.В. Операционные системы: Учебник для вузов. – 2-е изд. – СПб.: Питер, 2004. – 415 с. (наличие в библиотеке ТУСУР - 17 экз.)

3. Олифер В.Г., Олифер Н.А. Сетевые операционные системы: Учебник для вузов. – СПб.: Питер, 2007. – 538 с. (наличие в библиотеке ТУСУР - 10 экз.)

4. Раводин О.М., Раводин В.О. Безопасность операционных систем: Учебное пособие. – 2-е изд., перераб. и доп. – Томск: В-Спектр, 2006. – 226 с. (наличие в библиотеке ТУСУР - 80 экз.)

### 4.3. Обязательные учебно-методические пособия

1. Конев А.А. Безопасность операционных систем: презентации по курсу лекций (часть 1) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-1-lect.pdf>

2. Конев А.А. Безопасность операционных систем: презентации по курсу лекций (часть 2) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-2-lect.pdf>

3. Конев А.А. Безопасность операционных систем: методические указания по выполнению лабораторных работ. Часть 1 [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/os-lab.pdf>

4. Конев А.А. Безопасность операционных систем: методические указания по выполнению лабораторных работ. Часть 2 [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-lab.pdf>

5. Конев А.А. Безопасность операционных систем: методические указания по выполнению практических работ [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/os-pract.pdf>

6. Конев А.А. Безопасность операционных систем: вопросы к контрольной работе (1-й семестр) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-1-kontr.pdf>

7. Конев А.А. Безопасность операционных систем: вопросы к контрольной работе (2-й семестр) [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-2-kontr.pdf>

8. Конев А.А. Безопасность операционных систем: вопросы к экзамену [Электронный ресурс]. - <http://kibevs.tusur.ru/sites/default/files/upload/manuals/bos-2-exam.pdf>

### 4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрено