МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

«13» 04 2017 г.

Рабочая программа дисциплины
Защита в операционных системах

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2017

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита в операционных системах» являются овладение знаниями, умениями и навыками, позволяющими настраивать подсистемы защиты операционных систем в соответствии с требованиями безопасности, обеспечивать безопасное сетевое взаимодействие компьютерных систем и вести разработки программных модулей, реализующих функции защиты операционных систем.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к базовой части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Основы информационной безопасности», «Системы управления базами данных», «Операционные системы» и «Сети и системы передачи данных».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин: «Основы построения защищенных баз данных», «Защита программ и данных», «Программно-аппаратные средства обеспечения информационной безопасности».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

- способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);
- способностью участвовать в разработке проектной и технической документации (ПК-6);
- способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7).

В рамках указанных компетенций обучающийся должен

- Знать:

– защитные механизмы и средства обеспечения безопасности операционных систем;

- Уметь:

– формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;

• Владеть:

– навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Лабораторные занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
1	Подсистемы безопасности ОС	7	1-9	54	18	18	18	Контрольная работа 9-й неделе
2	Средства обеспечения безопасности ОС	7	10-18	54	18	18	18	
	Промежуточная аттестация							Зачет
	ИТОГО			**108**	**36**	**36**	**36**	–

Подсистемы безопасности ОС. Угрозы безопасности ОС. Подсистемы безопасности автоматизированных систем на базе СВТ и механизмы защиты. Подсистема идентификации, аутентификации и управления доступом. Подсистема аудита. Подсистема целостности. Криптографическая подсистема.

Средства обеспечения безопасности ОС. Домены безопасности. Механизмы безопасности Linux. Защита сетевого взаимодействия. Внешние средства защиты ОС Windows. Расширения безопасности ОС Windows. Защищенные хранилища и RAID-массивы.

План лабораторных занятий

На лабораторных занятиях студенты осваивают навыки настройки подсистем безопасности ОС Windows и Linux и дополнительных сертифицируемых средств путем экспериментального воздействия на настройку защитных механизмов и отслеживания их реакции на эти воздействия.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1	Подсистемы безопасности ОС. Угрозы безопасности ОС.	№1
2-3	Подсистемы безопасности ОС. Подсистемы безопасности автоматизированных систем на базе СВТ и механизмы защиты.	№2
4-6	Подсистемы безопасности ОС. Подсистема идентификации, аутентификации и управления доступом. Подсистема аудита.	№3
7-8	Подсистемы безопасности ОС. Подсистема целостности.	№4
9	Подсистемы безопасности ОС. Криптографическая подсистема.	№5
10-12	Средства обеспечения безопасности ОС. Домены безопасности.	№6
13-14	Средства обеспечения безопасности ОС. Защита сетевого взаимодействия.	№7
15	Средства обеспечения безопасности ОС. Механизмы безопасности Linux.	№8
16	Средства обеспечения безопасности ОС. Расширения безопасности ОС Windows.	№9
17	Средства обеспечения безопасности ОС. Внешние средства защиты ОС Windows.	№10
18	Средства обеспечения безопасности ОС. Защищенные хранилища и RAID-массивы.	№11

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе образовательных технологий аналогичных творческой мастерской. На лабораторных занятиях, проводимых методом творческой мастерской студентам предоставляется возможность в очерченных рамках тематики и указанной цели самостоятельно добиваться сочетания настройки политик безопасности и настроек средств защиты информации, обеспечивающие баланс производительности, доступности и безопасности. Задание студентам строится таким образом, что сначала он выполняет указанные действия и наблюдает результат, а за тем должен самостоятельно спланировать свои действия для достижения указанного результата. При этом данные действия в полной мере не отрабатывались ранее. Приветствуется вариативность достижения результата.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья и инвалидов, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты как правило доделывают лабораторные работы, которые начали на аудиторных занятиях и готовят обязательный отчет, где либо описывают наблюдаемые результаты, либо порядок действий, приводящий к заданной цели.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачет). Фонд оценочных средств дисциплины приведён в приложении 1.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	10	5	0	5	0	40	40	100

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 10 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий в течение одного семестра – от 0 до 5 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Контроль результатов самостоятельной работы, которая состоит в доведении до заключительной стадии и оформлении исследований, начатых на аудиторных занятиях. Оформленные работы в электронном виде сдаются преподавателю для дальнейшей проверки.

Выполнение заданий в рамках самостоятельной работы в течении семестра – от 0 до 5 баллов.

0 баллов – работа не сдана

1 балл – работа содержит грубые ошибки, требуемый уровень защищенности не достигнут, оформление не соответствует предъявляемым требованиям.

2 балла – работа содержит грубые ошибки, полученный уровень защищенности не вполне достаточен, присутствуют ошибки в объекте воздействия, оформление соответствует предъявляемым требованиям.

3 балла – работа содержит ошибки, критически не влияющие на получение результата, требуемый уровень защищенности достигнут, оформление не соответствует предъявляемым требованиям.

4 балла – работа содержит незначительные ошибки, требуемый уровень защищенности достигнут, оформление соответствует предъявляемым требованиям.

5 баллов – работа не содержит ошибок, требуемый уровень защищенности достигнут, оформление соответствует предъявляемым требованиям.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа должна быть аккуратно оформлена по стандарту оформления реферата и экспертного заключения. В ней должны присутствовать описательная, исследовательская и заключительная часть, а также обоснованные выводы.

Контрольная работа оценивается – от 0 до 40 баллов, а именно

работа на «отлично» оценивается от 35 до 40 баллов;

работа на «хорошо» оценивается от 30 до 34 баллов;

работа на «удовлетворительно» оценивается от 20 до 29 баллов;

работа на «неудовлетворительно» оценивается от 0 до 19 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой устный зачет.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 35 до 40 баллов;

ответ на «хорошо» оценивается от 30 до 34 баллов;

ответ на «удовлетворительно» оценивается от 20 до 29 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 19 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за седьмой семестр по дисциплине «Защита в операционных системах» составляет 100 баллов.

Таблица 2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Защита в операционных системах» в оценку (зачет)

50 баллов и более	«зачтено»
меньше 50 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Хорев, П. Б. Программно-аппаратная защита информации [Электронный ресурс] : Учебное пособие / П. Б. Хорев. - 2, испр. и доп. - Москва : Издательство "ФОРУМ" ; Москва : ООО "Научно-издательский центр ИНФРА-М", 2015. - 352 с. - ISBN 978-5-00091-004-7 : Б. ц. URL: http://znanium.com/go.php?id=489084 (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

2) Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : Учебное пособие / Владимир Федорович Шаньгин. - Москва : Издательский Дом "ФОРУМ" ; Москва : ООО "Научно-издательский центр ИНФРА-М", 2013. - 592 с. - ISBN 978-5-8199-0411-4 : Б. ц. URL: http://znanium.com/go.php?id=402686 (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

б) дополнительная литература:

1) Таненбаум, Э. С. Современные операционные системы [Текст] = Modern Operating Systems / Э. С. Таненбаум ; пер. на рус. яз. А. Леонтьева. - 2-е изд. - Москва ; Санкт-Петербург [и др.] : Питер, 2007. - 1037, [3] с. : рис. - (Классика Computer Science). - Библиогр.: с. 998-1020. - Алф. указ.: с. 1021-1037. - ISBN 978-5-318-00299-1 (в пер.). - ISBN 0-13-031358-0 (анг.).

2) Олифер, В. Г. Сетевые операционные системы [Текст] : учеб. для вузов / В. Г. Олифер, Н. А. Олифер. - 2-е изд. - Москва ; Санкт-Петербург [и др.] : Питер, 2009. - 668, [4] с. : ил. - (Учебник для вузов). - Алф. указ.: с. 652-668. - ISBN 978-5-91180-528-9.

в) Интернет-ресурсы:

1) Управление Windows 7 с помощью групповой политики [Электронный ресурс]. URL: http://www.oszone.net/11240/Group_Policy (дата обращения 02.01.2017) Загл. с экрана. Яз. рус.

2) Защита в Linux [Электронный ресурс]. URL: http://www.astra-linux.com/vvedenie.html (дата обращения 26.09.2016) Загл. с экрана. Яз. рус.

3) Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI [Электронный ресурс]. URL: http://www.osp.ru/winitpro/2007/02/4102619/ (дата обращения 02.01.2017) Загл. с экрана. Яз. рус.

г) программное обеспечение:

1) Лицензионное программное обеспечение: ОС Windows, ОС Windows Server, Программно-аппаратный комплекс «Аккорд 2000/NT», Программно-аппаратный комплекс «Соболь», Антивирусная программа «Антивирус Касперского».

2) Свободно распространяемое программное обеспечение: КриптоПро CS 3 в режиме демо, Secret Net 5 в режиме демо, Virtual Box.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходимы аудитория, оборудованная компьютером с установленным любым программным обеспечением, позволяющим читать следующие форматы файлов данных: pdf, doc, docx, ppt, pptx и подключаемый к нему проектор.

Для проведения лабораторных занятий необходимы аудитории, оборудованные компьютерами класса не ниже Pentium IV, с установленным любым программным обеспечением ОС Windows, Virtual Box, КриптоПро CSP, Secret Net, желательно носители eToken или ruToken по количеству рабочих мест.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Авторы

Доцент кафедры теоретических основ компьютерной безопасности и криптографии, к.ю.н., доцент _____ А.В. Гортинский

Старший преподаватель кафедры теоретических основ компьютерной безопасности и криптографии _____ И.Ю. Юрин

Программа разработана в 2012 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «25» мая 2012 года, протокол № 18).

Программа актуализирована в 2017 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «09» января 2017 года, протокол № 10).

Заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, профессор, к.ф.-м.н. _____ В.Н. Салий

Декан факультета компьютерных наук и информационных технологий, к.ф.-м.н., доцент _____ А.Г. Федорова