Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

«Б.1.1.29 Безопасность операционных систем»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль "Безопасность автоматизированных систем"

форма обучения – очная
курс – 3
семестр – 5
зачетных единиц – 6
часов в неделю – 5
всего часов – 180,
в том числе:
лекции – 32
коллоквиумы – 16
практические занятия – 32
самостоятельная работа – 100
экзамен – 5 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: теоретическая и практическая подготовка специалистов в области эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности и привитие навыков в использовании методов обеспечения защиты информации в ОС.

Задачи изучения дисциплины:

- изучение назначения и функций ОС;
- приобретение навыков управления ресурсами и задачами в ОС;
- освоение администрирования ОС;
- изучение требований к защите ОС;
- изучение методов и средств разграничения доступа в ОС;
- изучение аудита в ОС;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность планирования политики безопасности ОС;
- приобретение навыков эффективной и безопасной эксплуатации ОС автоматизированных систем;
- формирование специальных теоретических и практических знаний, обеспечивающих возможность проектировании средств защиты информации и средств контроля защищенности автоматизированных систем;
- приобретение навыков эффективного применения информационно-технологических ресурсов ОС с учетом требований информационной безопасности;
- приобретение навыков эффективного применения средств защиты информационно-технологических ресурсов ОС;
- формирование специальных теоретических и практических знаний, позволяющих администрировать подсистему информационной безопасности автоматизированной системы;
- формирование специальных теоретических и практических знаний, позволяющих обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность операционных систем» относится к числу базовой части дисциплин.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» - знать формы и способы представления данных в персональном компьютере, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; уметь

применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска и т.п.), пользоваться сетевыми средствами и внешними носителями информации для обмена данными; владеть навыками обеспечения безопасности информации с помощью типовых программных средств, навыками поиска и обмена информацией в глобальной сети Интернет;

«Технологии и методы программирования» - знать общие принципы построения и использования современных языков программирования высокого уровня, язык программирования высокого уровня (объектно-ориентированное программирование); уметь работать с интегрированной средой разработки программного обеспечения, использовать динамически подключаемые библиотеки; владеть навыками разработки, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» - знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

Дисциплина «Безопасность операционных систем» является предшествующей для изучения следующих базовых дисциплин: «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Организация ЭВМ и вычислительных систем».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3).

Студент должен знать:

- операционные системы персональных ЭВМ;
- принципы построения и функционирования, примеры реализаций современных операционных систем;
- функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;

- критерии оценки эффективности и надежности средств защиты ОС;
- принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- архитектуру системы безопасности ОС Windows XP/7/2008 R2;
- используемые в Windows XP/7/2008 R2 протоколы аутентификации, их достоинства и недостатки;
- управление учетными записями пользователей и групп в целях обеспечения безопасности;
- уязвимости ОС Windows XP/7/2008 R2 и методы их устранения;
- проблемы и особенности применения файловой системы с шифрованием (EFS), способы повышения уровня безопасности при использовании EFS;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- принципы формирования политики информационной безопасности в автоматизированных системах.

Студент должен уметь:

- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
- оценивать эффективность и надежность защиты операционных систем;
- планировать политику безопасности операционных систем;
- пользоваться нормативными документами по защите информации;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

- разрабатывать частные политики информационной безопасности автоматизированных систем;
- формулировать и настраивать политику безопасности распространенных операционных систем;
- разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации;

Студент должен владеть:

- навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;
- навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;
- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) операционных систем с учетом требований по обеспечению информационной безопасности;
- навыками эффективного применения средств разграничения доступа к ресурсам ОС (объектам Active Directory и файловой системы, сетевым ресурсам);
- навыками использования механизма групповых политик для централизованной настройки безопасных конфигурации рабочих станций и серверов;
- навыками применения дополнительных инструментов и утилит для управления системой безопасности ОС Windows XP/7/2008 R2;
- навыками организации централизованного сбора и анализа журналов регистрации для последующего разбора инцидентов;
- навыками построения системы управления обновлениями ОС Windows XP/7/2008 R2 и программного обеспечения на их основе;
- навыками использования рекомендаций ФСТЭК, ФСБ, Microsoft, NIST и других организаций по настройке средств безопасности Windows XP/7/2008 R2;
- профессиональной терминологией в области информационной безопасности;
- навыками работы с нормативными правовыми актами;
- навыками организации и обеспечения режима секретности;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- навыками безопасного использования технических средств в профессиональной деятельности.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	2	3	4	5	6	7	8	9	10
5 семестр									
1	1	1	Назначение и функции операционных систем	26	4	2	-	6	14
1	3	2	Управление задачами и ресурсами в ОС	40/2	4	2	-	6/2	28
1	5	3	Автоматизация решения задач администрирования в ОС с использованием языков сценариев	26/4	6/2	2/2	-	4	14
2	9	4	Требования к защите ОС	28/4	8/2	4/2	-	6	10
2	12	5	Разграничение доступа в ОС	28/4	6/2	4/2	-	6	12
2	15	6	Аудит ОС	32/4	4/2	2	-	4/2	22
Всего				**180/18**	**32/8**	**16/6**	**-**	**32/4**	**100**

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	Тема 1. Назначение и функции операционных систем Введение. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Понятие операционной системы (ОС), назначение, история развития, состав и функции ОС. Основные понятия операционных систем: задача, приложение, процесс, ресурс, файл, каталог.	1, 2, 3, 32
1	2	2	Системное и прикладное программное обеспечение. Функции системного и прикладного программного обеспечения. ОС Windows. История развития, основные возможности и особенности.	1, 2, 3, 32
2	2	3	Тема 2. Управление задачами и ресурсами в ОС Понятия задачи, процесса и потока. Планирование и диспетчеризация процессов и потоков: стратегии планирования, дисциплины диспетчеризации.	3, 5, 6, 7, 8, 32

2	**2**	**4**	Процессы ядра ОС. Процессы уровня приложений. Понятие устройства. Драйверы устройств, классификация драйверов, управление драйверами.	3, 5, 6, 7, 8, 32
3	**2**	**5**	Тема 3. Автоматизация решения задач администрирования в ОС с использованием языков сценариев Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.	5, 6, 7, 8, 32
3	**2**	**6**	Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС.	5, 6, 7, 8, 32
3	**2**	**7**	Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода. Отладка сценариев.	5, 6, 7, 8, 32
4	**2**	**8**	Тема 4. Требования к защите ОС Классификация угроз безопасности ОС. Наиболее распространенные угрозы.	5, 6, 7, 8, 9, 32
4	**2**	**9**	Понятие защищенной ОС. Подходы к организации защиты.	5, 6, 7, 8, 9, 32
4	**2**	**10**	Этапы построения защиты. Административные меры защиты.	5, 6, 7, 8, 9, 32
4	**2**	**11**	Политики безопасности в ОС Windows.	5, 6, 7, 8, 9, 32
5	**2**	**12**	Тема 5. Разграничение доступа в ОС Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.	6, 7, 8, 9, 32
5	**2**	**13**	Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.	6, 7, 8, 9, 32
5	**2**	**14**	Понятия идентификации, аутентификации и учета. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.	6, 7, 8, 9, 32
6	**2**	**15**	Тема 6. Аудит ОС Необходимость аудита. Требования к подсистеме аудита. Централизованный аудит.	7, 8, 9, 32
6	**2**	**16**	Штатный аудит в ОС Windows. Реализации аудита в современных ОС. Создание настраиваемых представлений. Настройка аудита в домене Active Directory.	7, 8, 9, 32

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	**2**	**1**	POSIX-совместимые операционные системы.	1, 2, 3, 5, 10, 11, 32

			Особенности архитектуры. История развития. Пользователи. Процессы.	
2	**2**	**2**	Память, виртуальное адресное пространство. Методы распределения памяти. Защита памяти.	1, 2, 12, 15, 32
3	**2**	**3**	Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.	2, 3, 5, 14, 16, 32
4	**2**	**4**	Виртуальные машины. Изоляция процессов и пользователей.	11, 12, 13, 17, 19, 32
4	**2**	**5**	Стандарты безопасности ОС.	12, 16, 17, 20, 32
5	**2**	**6**	Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.	11, 12, 13, 17, 19, 32
5	**2**	**7**	Примеры реализации идентификации, аутентификации и учета в современных ОС.	13, 14, 18, 32
6	**2**	**8**	Особенности настройки аудита в домене Active Directory	11, 12, 20, 21, 22, 32

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	6	**1**	Моделирование стратегий планирования центрального процессора ЭВМ	1, 2, 3, 5, 6, 7, 8, 32
2	6	**2**	Моделирование стратегий загрузки оперативного запоминающего устройства ЭВМ	1, 2, 3, 5, 6, 7, 8, 32
3	4	**3**	Моделирование работы центральных устройств ЭВМ	1, 2, 3, 5, 6, 7, 8, 32
4	6	**4**	Разработка системы идентификации/ аутентификации на основе паролей	1, 2, 3, 5, 6, 7, 8, 32
5	6	**5**	Разработка системы генерации пароля и шифрования сообщений	1, 2, 3, 5, 6, 7, 8, 32
6	4	**6**	Настройка подсистемы аудита ОС Windows	1, 2, 3, 5, 6, 7, 8, 32

8. Перечень лабораторных работ

Лабораторные работы учебным планом не предусмотрены.

9. Задания для самостоятельной работы студентов

№ Темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	**2**	**3**	**4**
1	14	Средства обнаружения уязвимостей в ОС Windows XP/Vista/7/Linux.	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 29, 30, 31, 32
2	10	Организация разграничения доступа в ОС Windows XP/Vista/7/Linux.	

2	18	Анализ типовых архитектур защищенных ОС	
3	14	Средства организации аудита сторонних разработчиков для ОС Windows XP/Vista/7/Linux.	
4	10	Антивирусные средства для ОС Windows XP/Vista/7/Linux.	
5	12	Средства аутентификации сторонних разработчиков для ОС Windows XP/Vista/7/Linux.	
6	22	Организация аудита стандартными средствами в ОС Windows XP/Vista/7/Linux.	

Виды, график контроля СРС, (по решению кафедры УМКС/УМКН).

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
5 семестр			
1-4	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), экзамен
5,6	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Экзамен

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [32].

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

12. Курсовой проект

Курсовой проект учебным планом не предусмотрен.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Изучение дисциплины направлено на формирование следующих компетенций: ПК-1, ПК-2, ПК-3.

Карта компетенции ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	Б.1.1.29 «Безопасность операционных систем»	Знает: - операционные системы персональных ЭВМ; - принципы построения и функционирования, примеры реализаций современных операционных систем; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	Лекции Коллоквиумы Самостоятельная работа Семинары	Тестирование
		Умеет: - использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - формулировать и настраивать политику безопасности распространенных операционных систем;	Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - навыками работы с современными операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; - навыками установки и настройки современных операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) операционных систем с учетом требований по обеспечению информационной безопасности;	Лекции Коллоквиумы Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

Карта компетенции ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	Б.1.1.29 «Безопасность операционных систем»	Знает: - операционные системы персональных ЭВМ; - принципы построения и функционирования, примеры реализаций современных операционных систем; - функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;	Лекции Коллоквиумы Самостоятельная работа Семинары	Тестирование
		Умеет: - использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - оценивать эффективность и надежность защиты операционных систем; - планировать политику безопасности операционных систем;	Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - навыками работы с современными операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; - навыками установки и настройки современных операционных систем семейств Windows и Unix с учетом требований по обеспечению	Лекции Коллоквиумы Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

		информационной безопасности; - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) операционных систем с учетом требований по обеспечению информационной безопасности;		

Карта компетенции ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	Б.1.1.29 «Безопасность операционных систем»	Знает: - место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - терминологию, основные руководящие и регламенти-рующие документы в области ЭВМ, комплексов и систем; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области; - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; - автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - принципы формирования политики информационной безопасности в	Лекции Коллоквиумы Самостоятельная работа Практические занятия	Тестирование

		автоматизированных системах;		
		Умеет: - пользоваться нормативными документами по защите информации; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - планировать политику безопасности информационных систем; - разрабатывать частные политики информационной безопасности автоматизированных систем; - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; -разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;	Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - профессиональной терминологией в области информационной безопасности; - навыками работы с нормативными правовыми актами; - навыками организации и обеспечения режима секретности; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками безопасного использования технических средств в профессиональной деятельности.	Лекции Коллоквиумы Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

Формирование профессиональных компетенций по дисциплине производится на практических и лекционных занятиях (75%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче экзамена (15%).

При выставлении экзаменационных оценок преподаватель руководствуется следующим:

- оценки «отлично» заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную

литературу и знакомый с дополнительной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на высоком уровне освоения. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины и их значение для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

- оценки «хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе, продемонстрировавший умения и навыки в рамках формируемых компетенций на хорошем уровне освоения, способный к самостоятельному пополнению знания в ходе дальнейшей учебной работы и профессиональной деятельности;

- оценки «удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, освоившийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «удовлетворительно» выставляется студенту, допустившему неточность в ответе на экзамене;

- оценка «неудовлетворительно» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившего принципиальные ошибки в выполнении предусмотренных программой заданий, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Вопросы для зачета

Зачет учебным планом не предусмотрен.

Вопросы для экзамена

1. Классификация угроз информационной безопасности
2. Контроль доступа: матрица доступа, списки управления доступом и перечни возможностей
3. Модель матрицы доступов Харрисона-Руззо-Ульмана
4. Модель Белла-ЛаПадулла
5. Модель Биба
6. Базовая модель ролевого разграничения доступа
7. Архитектура операционной системы Windows

8. Структура процессов и потоков в ОС Windows, режимы выполнения кода.
9. Архитектура подсистемы безопасности LSA Windows
10. Компоненты LSA, процесс входа локального пользователя в ОС Windows
11. Аутентификация в ОС Windows: типы и сетевые протоколы
12. Форматы хешей Windows и хранилища паролей в ОС Windows
13. Особенности взлома хешей LM и NTLM, утилиты для взлома.
14. Принцип работы системы безопасности LSA и монитора ссылок безопасности в ОС Windows.
15. Идентификаторы безопасности SID. Типы учетных записей в ОС Windows
16. Маркеры доступа процессов и потоков в ОС Windows
17. Учетные записи служб ОС Windows. Ограниченный маркер доступа
18. Права на вход и привилегии пользователей в ОС Windows.
19. Дескрипторы безопасности и списки контроля доступа в ОС Windows
20. Авторизация в ОС Windows. Алгоритм оценки прав доступа
21. Наследование разрешений в ОС Windows, оценка записей контроля доступа с наследованием
22. Уровни целостности в ОС Windows. Мандатные политики.
23. Принципы работы механизма UAC. Фильтрованный маркер доступа. Опция requestedExecutionLevel в манифесте. Виртуализация операций записи для устаревших приложений.
24. Кэш регистрационных данных ОС Windows. Способы получения паролей из кэша
25. Способы сброса пароля учетной записи Windows
26. Анонимная регистрация пользователей (нулевой сеанс) в ОС Windows.
27. Методы аутентификации, поддерживаемые ОС Windows. Уязвимость протокола WDigest
28. Обзор протокола Kerberos. Структура билета Kerberos в ОС Windows
29. Политики аудита безопасности в ОС Windows (включение аудита в системе, требования к аудиту).
30. Просмотр событий безопасности в ОС Windows (журналы аудита, коды событий, настраиваемые представления)
31. Назначение и компоненты локальных и групповых политик безопасности в ОС Windows
32. Политики защиты паролей в GPO.
33. Политики административных шаблонов в ОС Windows
34. Модель изолированной программной среды
35. Политики ограниченного использования программ SRP в ОС Windows
36. Политики AppLocker в ОС Windows
37. Контролируемый доступ к папкам в ОС Windows
38. Шифрованная файловая система EFS
39. Технология BitLocker в ОС Windows
40. Основные компоненты Active Directory. Понятие домена, дерева, леса. Типы групп.

Тестовые задания по дисциплине

Для проведения тестирования используются тестовые материалы, разработанные в среде АСТ-Тест.

Примеры тестовых заданий:

1. Все данные о пользователях UNIX хранит в файле /etc/passwd в текстовом виде. Каждому пользователю соответствует одна строка, поля которой разделяются двоеточиями, например:
   Alex:x:1100:1200:alexander:/home/alex:/bin/bash
   Напишите GID

2. Все данные о пользователях UNIX хранит в файле /etc/passwd в текстовом виде. Каждому пользователю соответствует одна строка, поля которой разделяются двоеточиями, например:
   Alex:x:1100:1200:alexander:/home/alex:/bin/bash
   Напишите UID

3. Кто из пользователей является суперпользователем:
   1) root:x:1100:1200:root:/home/root:/bin/bash
   2) root:x:0:0:root:root:/bin/bash
   3) root:x:0:1000:root:/home/root:/bin/bash
   4) root:x:1100:1200:root:/home/root:/bin/bash

4. Класс защищенности автоматизированной системы – это:
   1) Определенная совокупность требований по защите информации, предъявляемых к автоматизированной системе.
   2) определенное требование по защите информации, предъявляемых к персоналу автоматизированной системы
   3) определенная совокупность требований по обработки информации, предъявляемых к автоматизированной системе
   4) совокупность требований по обработки информации, предъявляемых к персоналу автоматизированной системе

5. Все данные о пользователях UNIX хранит в файле /etc/passwd в текстовом виде. Каждому пользователю соответствует одна строка, поля которой разделяются двоеточиями, например:
   Alex:x:1000:2000:alexander:/home/alex:/bin/bash
   Напишите login

6. Все данные о пользователях UNIX хранит в файле /etc/passwd в текстовом виде. Каждому пользователю соответствует одна строка, поля которой разделяются двоеточиями, например:
   Alex:1234:1000:2000:alexander:/home/alex:/bin/bash
   Напишите password

7. Что такое уязвимость нулевого дня:

1) Термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки .

2) Разработчик не хочет исправлять данную уязвимость

3) Термин означает, что разработчик изначально заложил в программу уязвимость, чтобы в дальнейшем использовать ее в своих целях

4) Уязвимость, когда дата ОС переводится в нулевое значение.

8. Идентификация – это:

1) процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.

2) предоставление личных данных пользователем

3) процедура, в результате которой субъект получает определенные права в системе

4) метод хранения логина и пароля

9. Аутентификация – это:

1) проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;

2) подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;

3) проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

4) проверка пользователем введенных им данных

10. Что такое BruteForce-атака?

1) получение конфиденциальной информации с компьютера методом электронной рассылки

2) взлом методом заражения системы через вредоносный файл

3) метод, заставляющий пользователя самому раскрыть информацию

4) взлом методом перебора паролей

11. Процесс авторизации -это процесс

1) ввода пользователем учетной информации

2) доказательство того, что пользователь тот, за кого выдает

3) выполнение действий, необходимых для того, чтобы пользователь мог начать работу в системе

4) получения идентификатора пользователя в системе

12. Аудит ОС заключается в :

1) фиксации всех событий, от которых зависит безопасность системы

2) безопасном входе в систему

3) контроле доступа к файлам и папкам

4) средствах защиты от замены файлов

13. Что является основным методом выявления вторжений?
1) ведение аудита
2) антивирусное программное обеспечение
3) пороговое обнаружение
4) профильное обнаружение

14. Какую функцию в системе Kerberos выполняет ключ сеанса?
1) используется для шифрования (дешифрования) аутентификатора, состоящего из квитанции и секретного ключа, разделяемого сервером квитанций и ресурсным сервером
2) используется для шифрования (дешифрования) аутентификатора, состоящего из идентификатора пользователя, его сетевого адреса и временной отметки
3) используется для шифрования квитанции
4) используется для шифрования квитанции и пароля пользователя

15. Политика безопасности – это:
1) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.
2) состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
3) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения
4) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

Общее количество занятий, проводимых в интерактивных формах, не менее 18 часов.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Алешин Л.И. Информационные технологии: учеб. пособие / Л.И.Алешин. - М.: Маркет ДС, 2011. - 384 с. Экземпляры всего: 22.
2. Мельников В.П. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - Электрон. текстовые дан. - М.: ИЦ "Академия", 2011. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/Ld_154.pdf
3. Губенков А.А. Обеспечение безопасности персональных данных: учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А.А. Губенков. - Саратов: СГТУ, 2015. - 84 с. Экземпляры всего: 3.
4. Губенков А.А. Обеспечение безопасности персональных данных [Электронный ресурс]: учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А. А. Губенков ; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2015. - 1 эл. опт. диск (CD-ROM). - ISBN 978-5-7433-2786-7. Электронный аналог печатного издания. Режим доступа: http://lib.sstu.ru/books/zak 51_15.pdf

Дополнительные издания

5. Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Саратов: СГТУ, 2010. - 96 с. Экземпляры всего: 40.
6. Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей [Электронный ресурс]: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2010. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 260_10.pdf
7. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов : СГТУ, 2009. - 88 с. Экземпляры всего: 2.
8. Губенков, А. А. Информационная безопасность вычислительных сетей [Электронный ресурс]: учеб. пособие / А.А. Губенков; Сарат. гос. техн. ун-т (Саратов). - Электрон. текстовые дан. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 479_09.pdf
9. Терещенко С. Н. Информационная безопасность и защита информации : учеб. пособие / С. Н. Терещенко. - Саратов : СГТУ, 2009. - 136 с. Экземпляры всего: 3.
10.Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – М.: Академия, 2006. – 240 с. Экземпляры всего: 19.

11.Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П. Б. Хорев. - М. : ИЦ "Академия", 2005, 2006, 2007, 2008. - 256 с. Экземпляры всего: 33.
12. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для вузов / П.Н. Девянин. - М.: ИЦ "Академия", 2005. - 144 с. Экземпляры всего: 12.
13. Правовое обеспечение информационной безопасности : учеб. пособие для вузов / С.Я. Казанцев, О.Э. Згаздай, Р.М. Оболенский и др.; под ред. С.Я. Казанцева. - М.: ИЦ "Академия", 2008. - 240 с. Экземпляры всего: 10.
14. Бузов Г.А. Защита от утечки информации по техническим каналам : учеб. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. - М. : Горячая линия - Телеком, 2005. - 416 с. Экземпляры всего: 5.
15. Шумский А.А. Системный анализ в защите информации: учеб. пособие / А.А. Шумский, А.А. Шелупанов. - М.: Гелиос АРВ, 2005. - 224 с. Экземпляры всего: 10.
16. Расторгуев С.П. Основы информационной безопасности: учеб. пособие / С.П. Расторгуев. - М.: ИЦ "Академия", 2007. - 192 с. Экземпляры всего: 8.

Методические указания для обучающихся по освоению дисциплины

17. Программное обеспечение анализа информационных рисков "Гриф". Использование модели угроз и уязвимостей [Электронный ресурс]: метод. указания / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - Режим доступа: http://lib. sstu.ru/books/zak 88_08.pdf.
18. Программное обеспечение анализа информационных рисков "Гриф". Использование модели угроз и уязвимостей [Текст]: метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - 16 с. Экземпляры всего: 5.
19. Программное обеспечение анализа информационных рисков "Гриф". Использование модели информационных потоков [Электронный ресурс] : метод. указания / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - Режим доступа: http://lib.sstu.ru/books/zak 87_08.pdf.
20.Программное обеспечение анализа информационных рисков "Гриф". Использование модели информационных потоков [Текст] : метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т ; сост.: А.А. Губенков. - Саратов : СГТУ, 2008. - 18 с. Экземпляры всего: 5.
21.Использование программного обеспечения "КОНДОР" для разработки политики безопасности автоматизированных систем [Электронный ресурс] : метод. указания / Сарат. гос. техн. ун-т; сост. А.А. Губенков. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). - Режим доступа: http://lib. sstu.ru/books/zak 149_09.pdf.
22. Использование программного обеспечения "КОНДОР" для разработки политики безопасности автоматизированных систем [Текст] : метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т (Саратов) ; сост. А.А. Губенков. - Саратов : СГТУ, 2009. - 16 с. Экземпляры всего: 5.

Периодические издания

23. Вестник Саратовского государственного технического университета: науч.-техн. журнал. - Саратов: Изд-во СГТУ, (2003-2015). - ISSN 1999-8341. Режим доступа: http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan
24. Инновационная деятельность: науч.-аналит. журнал. - Саратов: Саратовский ГТУ им. Ю.А. Гагарина, (2010-2015). - ISSN 2071-5226. Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/
25. Журнал «Инновации + Паблисити». Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/
26. Журнал «BIS Journal - Информационная безопасность банков». Режим доступа: https://journal.ib-bank.ru.

Интернет-ресурсы

27. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
28. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. URL:http://www.securitylab.ru/ (дата обращения: 1.06.2015).
29. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
30. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
31. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

32. Весь лекционный материал размещен в электронной форме в ИОС направления ИФБС интернет-ресурсов СГТУ имени Гагарина Ю.А.
https://portal3.sstu.ru/Facult/MFPIT/MFPIT-IBS/10.03.01/1.1.29/default.aspx - лекционный материал за 5 семестр.

16. Материально-техническое обеспечение.

Для проведения лекционных занятий используется типовая лекционная аудитория со стандартным мультимедийным оснащением.

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:

- персональный компьютер (в конфигурации не хуже: процессор Intel Pentium или AMD 2 ГГц, 2 ОЗУ Гбайта, 320 Гбайт НЖМД);
- проектор (разрешение не менее 1024x768);
- экран для проектора.

Для проведения практических занятий и самостоятельной работы студентов используется компьютерный класс или учебная лаборатория каф. ИБС, оснащенная компьютерами.

Для проведения практических занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Intel Pentium или AMD 2 ГГц, ОЗУ 2 Гбайта, НЖМД 80 Гбайт. Компьютеры должны иметь подключение к локальной сети СГТУ и доступ к сети Интернет.

При проведении практических занятий в качестве инструментальных средств используется следующее программное обеспечение:

1. Операционные системы: Windows XP/7 в составе DreamsPark Premium MS ИНЭТМ (Windows, Visual Studio), Ubuntu Linux.
2. Средства разработки программ: Microsoft Visual Studio Express в составе DreamsPark Premium MS ИНПИТ, среда разработки NetBeans.
3. Антивирусные средства защиты Kaspersky Endpoint Security для Windows, Антивирус Касперского 6.0 для Windows Workstations.
4. Свободно распространяемые средства построения виртуальных машин. Например: VMWare Player или Virtual Box.
5. Архиватор RARLabs WinRAR.
6. Офисный пакет Microsoft Office Профессиональный плюс 2007 для подготовки и оформления отчетов.

Для проведения тестирования используется система тестирования знаний Ast-Test версия 3.