МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины
Защита в операционных системах

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целями изучения дисциплины «Защита в операционных системах» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий построения защищенных операционных систем, а также средств и методов обеспечения защиты информации в операционных системах.

Задачи дисциплины:

- изучение терминологии, понятийного аппарата и общих подходов к обеспечению информационной безопасности операционных систем;
- изучение средств и методов управления доступом в защищенных операционных системах;
- изучение средств и методов аутентификации пользователей в защищенных операционных системах;
- изучение средств и методов реализации аудита в защищенных операционных системах;
- изучение средств и методов интеграции защищенных операционных систем в защищенную сеть.

2. Место дисциплины в структуре ОП

Дисциплина «Защита в операционных системах» относится к числу дисциплин базовой части профессионального цикла.

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

«Информатика» - работа с программными средствами общего назначения;

«Аппаратные средства вычислительной техники» - знание архитектуры основных типов современных компьютерных систем;

«Операционные системы» - знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем.

Дисциплина «Защита в операционных системах» является предшествующей для следующих базовых дисциплин: «Основы построения защищенных сетей», «Основы построения защищенных баз данных», «Защита программ и данных». Знания и практические навыки, полученные в результате изучении дисциплины «Защита в операционных системах», используются студентами при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС по специальности «Компьютерная безопасность» и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах,	ИД-ОПК-9.4: способен настроить систему безопасности ОС, соответствующую поставленной задаче	**Знать** и учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, знать как работать с программными средствами безопасности в ОС. **Уметь** учитывать современные

компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;		тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, а также работать с программными средствами безопасности в ОС. **Владеть навыками** учета современных тенденций развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, а также навыками работы с программными средствами безопасности в ОС.
	ИД-ОПК-9.5: способен выбрать, установить и настроить стороннее ПО в соответствии с поставленной задачей	**Знать** и учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, знать как работать с программными средствами общего и специального назначения в системном ПО сторонних поставщиков (антивирусы, системы резервного копирования и прочее). **Уметь** учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, а также работать с программными средствами общего и специального назначения в системном ПО сторонних поставщиков (антивирусы, системы резервного копирования и прочее). **Владеть навыками** учета современных тенденций развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, а также навыками работы с программными средствами общего и специального назначения системном ПО сторонних поставщиков (антивирусы, системы резервного копирования и прочее).
ОПК-11: Способен разрабатывать политики безопасности, политики управления доступом и	ИД-ОПК-11.1: способен создать и поддерживать в актуальном состоянии политику информационной безопасности, исходя из поставленной задачи	**Знать** как используются современные ОС и их средства настройки политик безопасности. **Уметь** использовать современные ОС и их средства настройки

информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;		политик безопасности при изучении и исполнении поставленной задачи. **Владеть навыками** использования современные ОС и их средства настройки политик безопасности для решения профессиональных, исследовательских и прикладных задач.
	ИД-ОПК-11.3: способен обнаружить причину угрозы безопасности и устранить её	**Знать** механизмы, инструменты и базовые шаблоны безопасности современных ОС, средства администрирования пользователей, средства аудита событий. **Уметь** используя средства аудита событий, средства администрирования и инструменты безопасности современных ОС, настроить политики и шаблоны безопасности для устранения причины обнаруженной уязвимости. **Владеть навыками** анализа результатов работы системы аудита событий современных ОС, владеть штатными утилитами безопасности и штатными средствами администрирования ОС.
ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;	ИД-ОПК-12.3: способен работать с утилитами администрирования ОС для решения поставленной задачи	**Знать** базовые требования современных ОС, их утилиты администрирования и шаблоны настройки ОС в соответствии с поставленной задачей **Уметь** использовать утилиты администрирвоания и шаблоны настройки ОС в соответствии с поставленной задачей **Владеть навыками** создания, удаления и настройки объектов системы безопасности ОС для решения поставленной задачи.
	ИД-ОПК-12.2: способен восстановить ОС встроенными средствами и утилитами после возникновения внештатных ситуаций различного характера	**Знать** файловую структуру современных ОС, утилиты и возможности восстановления ОС в случае сбоя **Уметь** использовать утилиты восстановления ОС в случае сбоев разной природы, выбирать подходящий метод восстановления в зависимости от степени повреждений и характера сбоя **Владеть навыками** резервного

		копирования, восстановления ОС из резервной копии
ОПК-2.3: Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов	ИД-ОПК-2.3.1: способен подобрать ПО исходя из поставленной задачи	**Знать** содержание работ по установке, наладке, тестированию и обслуживанию современного общего и специального программного обеспечения, включая операционные системы. **Уметь** производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы. **Владеть навыками** по установке, наладке, тестированию и обслуживанию современного общего и специального программного обеспечения, включая операционные системы.
	ИД-ОПК-2.3.2: способен провести аудит имеющего ПО на соответствие поставленной задаче	**Знать** содержание работ по установке, наладке, тестированию и обслуживанию современного общего и специального программного обеспечения, включая операционные системы. **Уметь** производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы. **Владеть навыками** по установке, наладке, тестированию и обслуживанию современного общего и специального программного обеспечения, включая операционные системы.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад.часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Понятие защищенной операционной системы	7	4					3	
2	Управление доступом	7	6	6		2		10	Опрос по заданиям для самостоятельной работы
3	Идентификация, аутентификация и авторизация	7	6	6		2		10	Опрос по заданиям для самостоятельной работы
4	Аудит и обнаружение вторжений	7	6	6		2		10	Опрос по заданиям для самостоятельной работы
5	Резервирование и резервное копирование	7	2	4				10	Опрос по заданиям для самостоятельной работы
6	Ограничение пользователей	7	2	2				10	Опрос по заданиям для самостоятельной работы
7	Мультизагрузчики и шифрование	7	2	4				10	Опрос по заданиям для самостоятельной работы
8	Дополнительные вопросы обеспечения безопасности	7	4	4		1		10	Опрос по заданиям для самостоятельной работы
						2	0,5	33,5	Экзамен
	Всего за 7 семестр		32	32		7		106,5	
	Всего	180	**32**	**32**		**9**	**0,5**	**106,5**	

Содержание разделов дисциплины:

Тема № 1. Понятие защищенной операционной системы.

1.1. Угрозы безопасности операционной системы. Классификация угроз, наиболее распространенные угрозы.

1.2. Понятие защищенной операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.

Тема № 2. Управление доступом.

2.1. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом.

2.2. Дискреционное управление доступом. Матрица доступа.

2.3. Изолированная программная среда.

2.4. Мандатное управление доступом. Метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах.

2.5. Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов

доступа. Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом.

2.6. Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа, привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам. Средства динамического изменения полномочий субъектов: олицетворение субъектов доступа. Расширения дискреционной системы управления доступом: автоматическое наследование атрибутов защиты объектов, ограниченные маркеры доступа, мандатный контроль целостности, контроль учетных записей, элементы изолированной программной среды.

Тема № 3. Идентификация, аутентификация и авторизация.

3.1. Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.

3.2. Парольная аутентификация в UNIX, библиотеки PAM.

3.3. Парольная аутентификация в Windows, средства управления параметрами аутентификации. Аутентификация на основе внешних носителей ключа.

Тема № 4. Аудит.

4.1. Необходимость аудита в защищенной системе. Требования к подсистеме аудита. Система контроля целостности данных Tripwire.

4.2. Системы обнаружения и предотвращения вторжений

4.2. Реализация аудита в ОС Windows.

4.3. Реализация аудита в ОС UNIX.

Тема № 5. Резервирование и резервное копирование.

5.1 Основные определения, механизмы реализации, причины необходимости резервирования и резервного копирования

5.2. Резервирование штатными средствами ОС

5.3. Резервное копирование на примере BareOS

Тема № 6. Ограничение пользователей.

6.1. Дисковые квоты

6.2 Ограничение процессов в потребляемых ресурсах

6.3. Штатные механизмы Windows и Linux

Тема № 7. Мультизагрузчики и шифрование.

7.1. Задачи и условия реализации мультисистемного использования компьютеров. Мультизагрузчики, их особенности, преимущества и недостатки. Примеры организации работы нескольких разных ОС на одном компьютере.

7.2. Виртуальные машины, их особенности, преимущества и недостатки. Примеры организации работы нескольких разных ОС на одном компьютере на базе виртуальных машин.

7.3. Обзор и применение штатных механизмов шифрования ОС.

Тема № 8. Дополнительные вопросы обеспечения безопасности.

8.1. Средство изолирования потенциально опасного кода - контейнеры.

8.2. Средство изолирования потенциально опасного кода - SeLinux

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:
Электронны учебный курс «Операционные системы» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены тексты лекций по всем темам теоретического раздела дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине и итоговой аттестации (при необходимости) в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса по дисциплине «Защита в операционных системах» используются:
-программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:
- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Microsoft OfficeSTD 2013;
Dr. Web Desktop Security Suite;
- Kaspersky Endpoint Security;
- ViPNet Administrator 4.x (КС3);
- Сеть 11565. ViPNet Client for Windows 4.x (КС3);
- XSpyder 7.8.
- СЗИ НСД Dallas Lock 8.0-K;
- Средства защиты информации Secret Net 7;

- Linux (GNU GPL v.3).
- OpenVPN
- BareOS

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

а) основная литература:

1. Мельников, В. П., Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стереотип., М., Академия, 2009, 331с
2. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для вузов. / В. В. Платонов - 2-е изд., стер. - М.: Академия, 2014. - 331 с.
3. Шелухин О.И. Системы обнаружения вторжений в компьютерные сети [Электронный ресурс] : учебное пособие / О.И. Шелухин, А.Н. Руднев, А.В. Савелов. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2013. — 88 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63360.html

б) дополнительная литература

4. Шаньгин, В. Ф., Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин, М., ДМК Пресс, 2012, 592с
5. Руссинович М. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000.: мастер-класс.: пер. с англ. / М. Руссинович, Д. Соломон - 4-е изд. - СПб.: Питер; М.: Русская Редакция, 2008. - 968 с**. .**
6. Синицын С. В. Операционные системы: учебник для вузов. / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин; УМО по образованию в обл. прикладной информатики - М.: Академия, 2010. - 297 с.
7. Ромель А.П. Windows 10. Все об использовании и настройках. Самоучитель [Электронный ресурс] / А.П. Ромель, М.А. Финкова, М.Д. Матвеев. — Электрон. текстовые данные. — СПб. : Наука и Техника, 2016. — 336 c. — 978-5-94387-986-9. — Режим доступа: http://www.iprbookshop.ru/60646.html
8. Lehey G. FreeBSD Operating System [Электронный ресурс] / G. Lehey. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 814 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57366.html
9. Джон Роббинс Отладка Windows-приложений [Электронный ресурс] / Роббинс Джон. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 447 c. — 978-5-4488-0106-8. — Режим доступа: http://www.iprbookshop.ru/63940.html
10. Матвеев М.Д. Полное руководство Windows 8.1 [Электронный ресурс] / М.Д. Матвеев, М.В. Юдин, Р.Г. Прокди. — Электрон. текстовые данные. — СПб. : Наука и Техника, 2015. — 656 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/43320.html
11. Мошков М.Е. Введение в системное администрирование Unix [Электронный ресурс] / М.Е. Мошков. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-

Университет Информационных Технологий (ИНТУИТ), 2016. — 208 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/73672.html
12. "Требования безопасности информации к операционным системам" (приказ ФСТЭК России № 119 от 19.08.2016): http:// www.fstec.ru.

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
2. Электронно-библиотечная система «Юрайт https://www.biblio-online.ru/
3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru)
4. Электронно-библиотечная система «Лань» http://e.lanbook.com/
4. Библиотека документации портала «Тэчнет» корпорации Microsoft, включающая официальные руководства, описания и интерактивные документы по безопасности большинства программных продуктов: https://technet.microsoft.com/ru-ru/library/aa991542.
5. Портал «Технологии программ с открытым кодом Линукс» и его постоянная рубрика «безопасность» по адресу: https://losst.ru/security.
6. Новости в сфере угроз безопасности и защиты компьютерной информации российских журнала «Хакер»:https://xakep.ru/tag/news и журнала «Информационная безопасность»: http://itsec.ru/main.php.
7. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»:http://www.kaspersky.ru/internet-security-center.
8. Материалы ежегодного (с 27 по 30 декабря) всемирного конгресса хакеров «ChaosCommunicationCongress» в Гамбурге (на английском языке), где рассказывается о новых выявленных уязвимостях в аппаратных решениях и программном обеспечении: https://events.ccc.de/congress/2015/wiki/Static:Main_Page, видеоматериалы с субтитрами конгресса CCC: https://www.youtube.com/user/CCCen/videos.
9. Разделы «Документы» и «Техническая защита информации» официального сайта ФСТЭК России: http:// www.fstec.ru.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа;
-учебные аудитории для проведения практических занятий: лаборатории информационных технологий и программно-аппаратных средств обеспечения информационной безопасности;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы):

старший преподаватель Д.А.Савинов

Приложение №1 к рабочей программе дисциплины
«Защита в операционных системах»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Задания для самостоятельной работы (ИД-ОПК-2.3.1, ИД-ОПК-2.3.2):

1. Найти самостоятельно в рекомендованной литературе и в электронных источниках информации описание подсистем безопасности ОС и сопоставить с описанием типовой архитектуры, дать пояснения.
2. Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Windows, функционирующей в составе локальной вычислительной сети, построенной на основе «лесной» доменной архитектуры и физически изолированной от глобальных вычислительных сетей общего пользования..
3. Разработать спецификации задания по безопасности для подсистемы аудита операционной системы Windows..
4. Разработать спецификации задания по безопасности для подсистемы аутентификации пользователей операционной системы Windows..
5. Разработать спецификации задания по безопасности для подсистемы разграничения доступа в Linux- Unix-подобной операционной системе..
6. Разработать спецификации задания по безопасности для подсистемы разграничения доступа операционной системы Windows Server..
7. Разработать спецификации задания по безопасности аудита для Windows Server для версии 2008, используемой в качестве файл-сервера вычислительной сети, построенной на основе «лесной» доменной архитектуры, причем доступ к удаленным доменам осуществляется через сеть Интернет.
8. Разработать сценарий последовательной установки ОС Windows, Linux и MacOS посредством мультизагрузчика на единичную ЭВМ с тремя жесткими дисками и настройки подсистем их безопасности для работы в Интернет и защиты от внешних угроз.
9. Разработать сценарий последовательной установки ОС Windows, Linux и MacOS с использованием виртуальных машин на единичную ЭВМ с двумя жесткими дисками и настройки подсистем их безопасности для работы в Интернет и защиты от внешних угроз.

Перечень вопросов для контрольной работы(ИД-ОПК-11.1):

1. Субъекты, объекты, методы, права и привилегии ОС Linux.
2. Субъекты, объекты, методы, права и привилегии ОС Windows.
3. Средства обнаружения и противодействия атакам и вторжениям в современных операционных системах ОС Linux.
4. Средства обнаружения и противодействия атакам и вторжениям в современных операционных системах ОС Windows.
3. Особенности резервирования и восстановления после сбоев современных операционных системах ОС Linux.

4. Особенности резервирования и восстановления после сбоев современных операционных системах Linux и Windows.

5. Особенности аудита в операционных системах Linux.

6. Особенности аудита в операционных системах Windows.

7. Штатные средства резервирования и резервного копирования Linux.

8. Штатные средства резервирования и резервного копирования Windows.

9. Понятие и примеры средств изолирования потенциально опасного кода .

10. Штатные средства шифрования ОС Windows.

11. Штатные средства шифрования ОС Linux.

Перечень вопросов для опросов на практических занятиях:

1. Базовые средства управления доступом в Windows: маркеры доступа, дескрипторы защиты. (ИД-ОПК-9.4).

2. Особенности управления доступом в UNIX-LINUX ОС классических и современных решений.

3. Охарактеризовать назначение и состав средств управления доступом, подобных применяемых в ОС Windows.

4. Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты. (ИД-ОПК-9.5).

5. Управление средствами аутентификации в Linux.

6. Управление средствами аутентификации в Windows.

7. Управление средствами аудита в Linux. (ИД-ОПК-12.3).

8. Управление средствами аудита в Windows. (ИД-ОПК-12.3).

9. Средства резервного копирования (ИД-ОПК-12.2)

10. Средства резервирования (ИД-ОПК-12.2)

11. Средства шифрования устройств

12. Шифрование на уровне файловой системы

13. Работа с systemd в Linux. Основная цель – обнаружить сервис, выполняющий определенные действия в процессе загрузки. (ИД-ОПК-11.3).

14. Выбор способа восстановления ОС Windows после сбоя. исходя из типа случившегося системного сбоя. Выработка рекомендаций по выбору ПО для предотвращения или минимизации последствий последующих инцидентов(ИД-ОПК-9.4)

1.2 Список вопросов и (или) заданий для проведения итоговой аттестации

Список вопросов к экзамену

1. Типовая архитектура подсистемы защиты защищенной ОС.

2. Функции низкого и высокого уровня подсистемы обеспечения безопасности защищенной ОС.

3. Разграничение доступа защищенной ОС (объекты и субъекты доступа, метод доступа и разграничение доступа, право доступа и полномочия доступа (привилегия), матрица доступа, дискреционный и мандатный метод доступа).

4. Идентификация, аутентификация и авторизация в защищенной ОС (авторизация с помощью паролей, внешних носителей ключевой информации, по биометрическим параметрам, комплексная авторизация).

5. Средства администрирования в защищенной ОС (система управления списком пользователей и политикой безопасности, менеджер ресурсов, аудит, сервисы)

6. Криптографические функции обеспечения безопасности в защищенной ОС (защита фалов средствами взаимодействия файловой системы и ОС, защита парольной информации при авторизации, защита передаваемой информации и поддержка криптопротоколов).

7. Средства защиты сетевых функций в защищенной ОС (средства маскирования ресурсов сети, фильтрация пакетов, средства межсетевого экранирования, средства криптозащиты информации при межсетевом взаимодействии, средства поддержки разграничения доступа для распределенных сетевых ресурсов для сетевых и распределенных информационных систем и систем удаленного хранения данных, средства сетевого дублирования и архивирования информации, а также ее резервирования, средствами систем сертификатов и ЭЦП, средства синхронизации времени).

8. Сервисные функции защищенной ОС для обеспечения устойчивости работы и защиты от несанкционированного доступа.

9. Методы и права доступа в ОС Windows.

10. Привилегии субъектов доступа в ОС Windows.

11. Маркер доступа пользователя в ОС Windows.

12. Дескриптор защиты объекта в ОС Windows.

13. Порядок проверки прав доступа субъекта к объектам в ОС Windows.

14. Назначение дескрипторов защиты создаваемым объектам в ОС Windows.

15. Мандатный контроль целостности в ОС Windows.

16. Элементы изолированной программной среды в ОС Windows.

17. Атрибуты защиты и векторы доступа семейства ОС Unix.

18. Методы проверки прав доступа субъекта к объекту семейства ОС Unix.

19. Механизм SUID/SGID семейства ОС Unix.

20. Пользователь root, повышение и минимизация полномочий, утилиты su и sudo семейства ОС Unix.

21. Парольная аутентификация и основные угрозы парольной аутентификации - компрометация и подбор паролей, методы уменьшения угрозы от компрометации и подбора паролей.

22. Аутентификация с использованием внешних носителей.

23. Биометрическая аутентификация.

24. Аутентификация в ОС UNIX.

25. Аутентификация в ОС Windows.

26. Общие сведения по аудиту защищенных ОС.

27. Аудит в ОС Windows.

28. Аудит в ОС UNIX.

29. Системы обнаружения вторжений в ОС.

30. Понятия резервирования и резервного копирования. Способы, особенности и преимущества резервирования

31. Резервное копирование: способы, особенности и преимущества разных методов. Общая схема системы резервного копирования на примере BareOS.

32. Понятие среды окружения пользователя. Ограничение пользователей в ресурсах на примере MS Windows и Linux.

33. Организация нескольких ОС на одном физическом компьютере: способы реализации, особенности и преимущества каждого из способов. Необходимость и способы обеспечения безопасности ОС.

34. Шифрование в ОС : способы реализации, преимущества каждого из способов. Примеры механизмов шифрования.

35. Контейнеры и изолированные окружения: назначение, примеры, отличия контейнеров и изолированных сред, отличия от виртуальных машин, примеры

36. Системы изоляции процессов на основе правил на примере SELinux

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

– владение основным объемом знаний по программе дисциплины;

– знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;

– владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;

– способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;

– усвоение основной литературы, рекомендованной рабочей программой дисциплины;

– знание базовых теорий, концепций и направлений по изучаемой дисциплине;

– самостоятельная работа на практических занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

– достаточно полные и систематизированные знания в объёме программы дисциплины;

– использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

– владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;

– способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

– усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

– умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;

– самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

– систематизированные, глубокие и полные знания по всем разделам дисциплины;

– точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

– безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

– способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;

– полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;

– умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;

– активная самостоятельная работа на практических занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение № 2 к рабочей программе дисциплины «Защита в операционных системах»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Защита в операционных системах» являются лекции, причем в достаточно большом объеме. Это связано с тем, что данная дисциплина находится как бы на стыке между дисциплинами «Аппаратные средства вычислительной техники» и «Операционные системы» в части аппаратного обеспечения защиты вычислительных процессов и использования памяти, методов хранения данных, и дисциплинами «Основы построения защищенных компьютерных сетей» и «Основы построения защищенных баз данных». Кроме того, очевидно, что данные о механизмах безопасности ОС ежегодно пополняются сериями

патчей подсистем безопасности к актуальным операционным системам и дополняются с выходом новых версий ОС.

Для успешного освоения дисциплины важно углубленное изучение некоторых разделов «Защита в операционных системах» самостоятельно, в качестве выполняемых в домашних условиях заданий. Основная цель самостоятельных работ – помочь не только усвоить теоретические основы и практические методы защиты в операционных системах, но и расширить свои знания до полных и системных. Для этого необходимо знать и понимать лекционный материал. Материал, законспектированный на лекциях, дополняет представленный в предлагаемой учебной литературе. Необходимо дома прорабатывать этот материал и дополнять новейшей актуальной информацией, полученной на консультациях, практических занятиях и из рекомендованных ресурсов сети Интернет.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков использования учебной литературы, в течение обучения проводятся мероприятия текущей аттестации в виде контрольной работы и ряда самостоятельных работ в домашних условиях. Варианты заданий выдаются учащимся на последнем часе лекционных занятий по каждой изучаемой теме. Оценка и обсуждение выполненных студентами заданий по самостоятельной работе производится на практических занятиях и учитывается, на ряду с результатами практических занятий, при оценке текущей успеваемости. Также при необходимости проводятся консультации по разбору заданий для самостоятельной работы, которые могут вызывать у студентов затруднения.

В конце семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Самостоятельно освоить вопросы дисциплины «Защита в операционных системах» студенту крайне сложно. Это обусловлено тем, что студенты слабо представляют объемы и характер постоянно проводимой разработчиками ОС работы в интересах доработки кода ОС для совместимости с различными аппаратными решениями и более адекватного соответствия защитных мер постоянно растущим по уровню и характеру угрозам безопасности.

Проблемы защиты в операционных системах осложняются наличием «багов» и «эксплойтов», заложенных зарубежными производителями аппаратно-программных решений в соответствии с законодательством по национальной безопасности. Поэтому, является совершенно необходимым посещение студентами всех аудиторных занятий, где им разъясняется цель и суть неполного представления информации российским потребителям о западных информационных технологиях и, конкретно, о составе и назначении защитных механизмов иностранных ОС. В результате формируется патриотическая позиция, непримиримость к любым аспектам иностранного проникновения к защищаемой в России информации и управления российскими информационными системами, нетерпимость к идеологии терроризма, экстремизма, иностранного промышленного и государственного шпионажа. В результате аргументированно формируется убежденность в необходимости профессионального противодействия методам компьютерной разведки и стремления более полно владеть имеющимися в операционных системах средствами компьютерной безопасности. Именно на этой основе и разъясняются основные учебные вопросы «Защиты в операционных системах».

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы особенно рекомендуется, кроме основной литературы, использовать материалы, рекомендованные в разделе дополнительной учебной литературы, ряд которых не потерял актуальности несмотря на давнее время издания(см. раздел 8)

А также, для подбора учебной литературы и актуализации неизбежно устаревающих знаний учебников, рекомендуется использовать спектр интернет-ресурсов(см. раздел 8).