Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____ / Т. Р. Змызгова /
«31» августа 2022 г.

Рабочая программа учебной дисциплины

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем

Специализация: (специализация№5) безопасность открытых информационных систем

Форма обучения: очная

Курган 2022

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» ((безопасность открытых информационных систем), утвержденным для очной формы обучения «30» 08 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» 08 2022, протокол № 1.

Рабочую программу составил:
ст. преподаватель В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 9 зачетных единицы трудоемкости (324 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр	
		8	9
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**176**	**96**	**80**
Лекции	62	32	30
Лабораторные работы	52	32	20
Практические занятия	62	32	30
Самостоятельная работа, всего часов в том числе:	**148**	**84**	**64**
Подготовка к экзамену	54	27	27
Другие виды самостоятельной работы (подготовка к практическим занятиям и лабораторным работам и рубежному контролю)	94	57	37
Вид промежуточной аттестации	**экзамен**	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**324**	**180**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной части Блока 1 модуля «информационная безопасность».

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

– Основы информационной безопасности.

– Теоретические основы компьютерной безопасности.

– Безопасность сетей ЭВМ.

– Безопасность операционных систем.

Результаты обучения по дисциплине необходимы для выполнения разделов курсового проекта по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем», а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является: приобретение обучаемыми необходимого объема знаний и практических навыков по анализу эффективности программно-аппаратных средств обеспечения информационной безопасности, управлению безопасностью автоматизированных систем в части, касающейся программно-аппаратных средств обеспечения информационной безопасности.

Задачи дисциплины:

- освоение принципов построения подсистем защиты в ОС, ВС и СУБД различной архитектуры;

- средств и методов несанкционированного доступа (НСД) к ресурсам ОС, ВС и СУБД;

- принципов функционирования современных систем идентификации и аутентификации;

- средств и методов реализации атак на сетевые ресурсы;

- принципов использования межсетевых экранов (МЭ);

- построения систем адаптивной безопасности в вычислительных сетях; построения виртуальных частных сетей.

Компетенции, формируемые в результате освоения дисциплины:

- способность применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2);

- способность решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации (ОПК-9);

- способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ

уязвимостей систем защиты информации автоматизированных систем (ОПК-13);

- осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем (ОПК-15);

- способность осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах (ОПК-5.3).

В результате изучения дисциплины обучающийся должен:

знать:

- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных систем (ОС), СУБД, компьютерных сетях (для ОПК-9);

- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы (для ОПК-2, ОПК-15);

- выявлять уязвимости информационно-технологических ресурсов АС, проводить мониторинг угроз безопасности АС (для ОПК-13, ОПК-5.3);

владеть:

- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем (для ОПК-2, ОПК-9, ОПК-13, ОПК-15).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
8 семестр					
Рубеж 1	1	***Введение***	2	-	-
	2	***Подсистемы защиты в современных ОС.*** Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ.	6	8	8
	3	Программно-аппаратные средства криптографической защиты.	2	2	8
	4	Защита программ.	6	10	8
	5	Подсистемы защиты информации в ОС Windows NT.	4	-	4
		Рубежный контроль № 1	-	2	-
Рубеж 2	6	Подсистема защиты информации в ОС UNIX.	2	-	4
	7	Защита информации при интеграции UNIX и Windows NT.	4	-	-

	8	Защита информации в вычислительных системах и сетях. Атаки на сетевые службы.	3	4	-
	9	Адаптивная безопасность в вычислительных сетях.	3	4	-
		Рубежный контроль № 2	-	2	-
		Итого за семестр	**32**	**32**	**32**
		9 семестр			
Рубеж 3	10	Межсетевые экраны.	2	8	4
	11	Удаленный доступ к сети.	2	-	-
	12	Виртуальные частные сети.	4	10	6
	13	Политика безопасности.	4	-	-
	14	Защита информации в системах управления базами данных. Понятия безопасности баз данных.	4	-	-
		Рубежный контроль № 3	-	2	-
Рубеж 4	15	Критерии защищенности баз данных.	4	-	
	16	Модели безопасности в системах управления баз данных.	4	-	-
	17	Механизмы обеспечения целостности систем управления баз данных.	4	8	6
	18	Механизмы обеспечения конфиденциальности в СУБД.	2	-	4
		Рубежный контроль № 4	-	2	-
		Итого за семестр	**30**	**30**	**20**
		Всего:	**62**	**62**	**52**

4.2. Содержание лекционных занятий

Тема 1. ***Введение***

Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчера доступа.

Тема 2. ***Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ.***

Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Методы и средства ограничения доступа к файлам.

Тема 3. ***Программно-аппаратные средства криптографической защиты.*** Построение аппаратных компонентов защиты данных. Защита файлов

от изменения. Электронно-цифровая подпись. Защита алгоритма шифрования, принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратных средств криптографической защиты.

Тема 4. ***Защита программ.***

Анализ программных реализаций. Защита программ от изучения. Защита от разрушающих программных воздействий. Построение изолированной программной среды. Защита программ от изменения и контроль целостности. Программные закладки. Компьютерные вирусы как особый класс программных закладок. Принципы работы антивирусных средств.

Тема 5. ***Подсистемы защиты информации в ОС Windows NT.***

Основные компоненты подсистемы защиты Windows NT и Windows 2000. Политики. Понятие домена. Особенности установления доверительных отношений. Создание и удаление бюджетов пользователей.

Тема 6. ***Подсистема защиты информации в ОС UNIX.***

Основные компоненты подсистемы защиты Unix. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Создание и удаление бюджетов пользователей. Основные проблемы с безопасностью и возможные решения в Unix-подобных системах.

Тема 7. ***Защита информации при интеграции UNIX и Windows NT.***

Основы взаимодействия элементов гетерогенных сетей. Шлюзы NFS, SMB в Unix. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене Windows NT.

Тема 8. ***Атаки на сетевые службы.***

Понятие атаки. Типы угроз. Классификация атак по основным механизмам реализации угроз. Сетевые сканеры.

Тема 9. ***Адаптивная безопасность в ВС.***

Понятие адаптивности безопасности и системы обнаружения атак. Классификация по используемым механизмам обнаружения атак, и по принципам их практической реализации. Особенности применения различных типов систем. Обнаружения атак. Особенности существующих свободно-распространяемых систем обнаружения атак.

Тема 10. ***Межсетевые экраны.***

Понятие межсетевых экранов. Их классификация. Основные примеры конфигурации защищенных сетей с использованием межсетевых экранов (МЭ). Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов. Программно-аппаратные средства защиты информации в сетях передачи данных.

Тема 11. ***Удаленный доступ к сети.***

Проблемы обеспечения безопасности при удаленном доступе. Протоколы аутентификации PAP и CHAP. Протоколы аутентификации удаленного доступа в программных средствах Microsoft. Система аутентификации и авторизации TACACS и Kerberos.

Тема 12. ***Виртуальные частные сети.***

Понятие виртуальной частной сети, ее предназначение. Стандартные возможности каналообразующего оборудования различных производителей. Основные принципы функционирования и использования протокола PPTP. Реализация в программных средствах Microsoft.

Тема 13. ***Политика безопасности.***

Понятие политики информационной безопасности для организации. Основные требования к политике безопасности. Этапы ее разработки.

Тема 14. ***Понятия безопасности БД.***

Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных.

Тема 15. ***Критерии защищенности БД.***

Критерии оценки надежных компьютерных систем. Современное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI). Концепция Гостехкомиссии.

Тема 16. ***Модели безопасности в СУБД.***

Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД. Дискреционные(избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS). Многозадачность (polyinstantiation) в БД.

Тема 17. ***Механизмы обеспечения целостности СУБД.***

Основные виды и причины возникновения угроз целостности. Способы противодействия. Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представление словаря. Фиксация транзакции. Прокрутки вперед и назад. Контрольная точка. Откат. Транзакции как средство изолированности пользователей. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности. Цели использования правил. Способы задания, моменты выполнения. Назначение механизма событий. Сигнализаторы событий. Типы уведомлений о происхождении события. Компоненты механизма событий.

Тема 18. ***Механизмы обеспечения конфиденциальности в СУБД.***

Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Основные понятия: субъекты и Объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа.

Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Метки безопасности. Использование предоставлений для обеспечения конфиденциальности информации в СУБД. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Журнализация. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

4.3 Практические занятия

Номер темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
		8 семестр	
2	Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ.	*Практическая работа №1.* Идентификация пользователей КС – субъектов доступа к данным	4
		Практическая работа №2. Защита информации в КС от НСД	4
3	Аппаратно-программные средства криптографической защиты	*Практическая работа №3.* Аппаратно-программные средства криптографической защиты	2
4	Защита программ.	*Практическая работа №4.* Защита программных средств от исследования	2
		Практическая работа №5. Защита программ от несанкционированного копирования	4
		Практическая работа №6. Защита информации от вредоносного программного обеспечения	4
5	***1-ой рубежный контроль***	***Тестирование***	***2***
8	Атаки на сетевые службы.	*Практическая работа №7.* Уязвимость компьютерных систем	4
9	Адаптивная безопасность в вычислительных сетях.	*Практическая работа №8.* Методы и средства ограничения доступа к компонентам ЭВМ (защита от утечек)	4
	2-ой рубежный контроль	***Тестирование***	***2***
		Итого	**32**
		9 семестр	
10	Межсетевые экраны.	*Практическая работа №9.* Программно-аппаратные средства защиты сети (МЭ и СОВ)	8
12	Виртуальные частные сети.	*Практическая работа №10.* Виртуальные частные сети	5
		Практическая работа №11. Управление криптографическими ключами	5
14	***3-ий рубежный контроль***	***Тестирование***	***2***
17	Механизмы обеспечения	*Практическая работа №12.* Средства	8

	целостности СУБД.	защиты СУБД	
18	***4-ый рубежный контроль***	***Тестирование***	***2***
		Итого	**30**
		Всего	***62***

4.4. Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторных работ	Норматив времени, час.
		8 семестр	
2	Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ.	*Лабораторная работа №1.* Анализ характеристик устройств аутентификации.	2
		Лабораторная работа №2. Системы защиты информации от НСД: «Страж NT», «Dallas Lock», «Secret NET».	4
		Лабораторная работа №3. Проверка механизма очистки памяти на примере использования программы «НКВД».	2
3	Аппаратно-программные средства криптографической защиты	*Лабораторная работа №4.* Системы защиты конфиденциальной информации «PGP» и « GPG».	2
		Лабораторная работа №5. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ.	2
		Лабораторная работа №6. Системы защиты конфиденциальной информации: «StrongDisk», «SecretDisk», «TrueCrypt».	4
4	Защита программ	*Лабораторная работа №7.* Защита программ от несанкционированной эксплуатации за счет привязки к носителю информации.	4
		Лабораторная работа №8. Программирование изменений характеристик файла	4
5	Подсистемы защиты информации в ОС Windows NT.	*Лабораторная работа №9.* Проверка настроек разрешительной системы доступа к файловым системам с использованием специализированных тестирующих средств и штатных средств из состава ОС.	4
6	Подсистема защиты информации в ОС UNIX.	*Лабораторная работа №10.* Основы использования средств защиты от несанкционированного доступа в операционной системе Linux.	4
		Итого за семестр	**32**
		9 семестр	
10	Межсетевые экраны	*Лабораторная работа №11.* Основы работы с персональным сетевым экраном «VipNet».	4
12	Виртуальные частные сети.	*Лабораторная работа №12.* Средства организации виртуальных частных сетей.	6

17	Механизмы обеспечения целостности СУБД.	*Лабораторная работа №13.* Контроль подсистемы обеспечения целостности.	6
18	Механизмы обеспечения конфиденциальности в СУБД.	*Лабораторная работа №14.* Программные средства защиты информации от утечек: DLP-система Secure Tower	4
		Итого за семестр	**20**
		Всего	**52**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных и практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной или практической работы.

Преподавателем запланировано применение на практических и лабораторных занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических и лабораторных занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным и практическим занятиям, к рубежным контролям, подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**37**

- Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ.	3
- Программно-аппаратные средства криптографической защиты.	2
- Защита программ.	2
- Подсистемы защиты информации в ОС Windows NT.	2
- Подсистема защиты информации в ОС UNIX.	2
- Защита информации при интеграции UNIX и Windows NT.	2
- Атаки на сетевые службы.	2
- Адаптивная безопасность в вычислительных сетях.	2
- Межсетевые экраны.	2
- Удаленный доступ к сети.	2
- Виртуальные частные сети.	2
- Политика безопасности.	2
- Понятия безопасности баз данных.	2
- Критерии защищенности баз данных.	2
- Модели безопасности в системах управления баз данных.	2
- Механизмы обеспечения целостности систем управления баз данных.	3
- Механизмы обеспечения конфиденциальности в СУБД.	3
Подготовка к практическим занятиям (по 1 часу на каждое занятие)	27
Подготовка к лабораторным работам (по 1 часу на каждое занятие)	26
Подготовка к рубежным контролям (по 1 часу на каждый рубежный контроль)	4
Подготовка к экзамену	54
Всего:	**148**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ (для очной формы обучения)
2. Отчеты обучающихся по лабораторным работам.
3. Отчеты обучающихся по практическим занятиям.
4. Банк тестовых заданий к рубежным контролям № 1, 2, 3 и 4.
5. Вопросы к экзамену

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="8">Содержание</td></tr>
<tr><td rowspan="6">1</td><td rowspan="6">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения обучающихся на первом учебном занятии)</td><td colspan="8">Распределение баллов</td></tr>
<tr><td colspan="8">8 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита отчетов по лабораторным работам</td><td>Выполнение практической работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ x 16 = $16_б$</td><td>$2_б$ x 10 = $20_б$</td><td>$2{,}5_б$ x 8 = $20_б$</td><td>7</td><td>7</td><td>30</td></tr>
<tr><td colspan="8">9 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита отчетов по лабораторным работам</td><td>Выполнение практической работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ x 15 = $15_б$</td><td>$5_б$ x 4 = $20_б$</td><td>$5_б$ x 4 = $20_б$</td><td>7</td><td>8</td><td>30</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре, зачета или экзамена</td><td colspan="8">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="8">Для допуска к промежуточной аттестации (экзамену) обучающийся должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и практические работы.
Для получения экзаменационной оценки «автоматически» обучающемуся необходимо набрать следующее минимальное количество баллов:
- 68 для получения «автоматически» оценки удовлетворительно».
По согласованию с преподавателем обучающемуся, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях и лабораторных работах, активное участие в научной и методической работе, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных и практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной или практической работы (при невозможности дополнительного проведения лабораторной или практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 2,5 и 2 баллов (8 семестр) и 5 баллов (9 семестр). Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий рубежного контроля состоят из 7 вопросов (для 1, 2, 3 рубежного контроля) и 8 (для 4 рубежного контроля) вопросов. Каждый вопрос оценивается в 1 балл. На каждое тестирование при рубежном контроле обучающемуся отводится 2 академических часа.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Экзамен состоит из 2 вопросов. Вопросы к экзамену доводятся до обучающихся на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа обучающемуся отводится 1 астрономический час.

Результаты текущего контроля успеваемости и экзамена заносятся преподавателем в экзаменационную ведомость, которая сдается в организационный отдел института в день экзамена, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежных контролей и экзамена

1-ый рубежный контроль

1. Для проведения процедур идентификации и аутентификации пользователя необходимо:

a) наличие аутентифицирующего объекта, хранящего уникальную информацию;

b)наличие соответствующего субъекта (модуля) аутентификации;

c) ответы a) и b).

2. Аппаратно-программные средства криптографической защиты информации выполняют функции:

a) проверяют на отсутствие закладок приборов, устройств.

b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС.

c) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.

2-ой рубежный контроль

1. К группе каналов утечки информации в которой основным средством является аппаратура, относятся следующие утечки:

a) хищение носителей информации (магнитных дисков, дискет, лент)

b) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;

c) копирование программой информации с носителей

2. Модификация ключа – это

a) генерирование нового ключа из предыдущего значения ключа с помощью двусторонней (двунаправленной) функции.

b) генерирование нового ключа из последующего значения ключа с помощью односторонней (однонаправленной) функции.

c) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции.

3-ый рубежный контроль

1. Сущность метода, основанного на использовании самогенерируемых кодов, заключается в том что:

a) исполняемые коды программы получаются самой программой до процесса ее выполнения.

b) исполняемые коды программы получаются самой программой после процесса ее выполнения.

c) исполняемые коды программы получаются самой программой в процессе ее выполнения.

2. В чем заключается правило разграничения доступа?

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности

документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, не содержатся все категории, определенные для данного документа.

4-ой рубежный контроль

1. Достоверная вычислительная база выполняет задачи:

a) функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности)

b) поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты

c) представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер.

2. Метод манипуляции с кодом программы:

a) в том, что на винчестере при инсталляции защищаемой от копирования программы формируется уникальный идентификатор, наличие которого затем проверяется инсталлированной программой при каждом ее запуске;

b) во включение в тело программы переходов по динамически изменяемым адресам и прерываниям, а также самогенерирующихся команд;

c) в изменении защищаемой программы.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ *(8 СЕМЕСТР)*

1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.
2. Концепция диспетчера доступа.
3. Основные компоненты подсистемы защиты Unix.
4. Файловая система – как основа подсистемы защиты.
5. Права доступа к элементам файловой системы. Управление процессами.
6. Основные компоненты подсистемы защиты Windows NT и Windows 2000. Понятие домена.
7. Особенности установления доверительных отношений.
8. Создание и удаление бюджетов пользователей.
9. Основы взаимодействия элементов гетерогенных сетей. Шлюзы NFS, SMB в Unix.
10. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене Windows NT.
11. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
12. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
13. Методы и средства ограничения доступа к компонентам ЭВМ.

14. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.

15. Методы и средства хранения ключевой информации.

16. Методы и средства ограничения доступа к файлам.

17. Анализ программных реализаций. Защита программ от изучения.

18. Защита от разрушающих программных воздействий.

19. Построение изолированной программной среды.

20. Защита программ от изменения и контроль целостности.

21. Программные закладки.

22. Компьютерные вирусы как особый класс программных закладок. Принципы работы антивирусных средств.

23. Понятие атаки. Типы угроз.

24. Классификация атак по основным механизмам реализации угроз.

25. Сетевые сканеры.

26. Понятие адаптивности безопасности и системы обнаружения атак.

27. Классификация по используемым механизмам обнаружения атак, и по принципам их практической реализации.

28. Особенности применения различных типов систем.

29. Обнаружения атак.

30. Особенности существующих свободно-распространяемых систем обнаружения атак.

31. Понятие межсетевых экранов. Их классификация.

32. Основные примеры конфигурации защищенных сетей с использованием межсетевых экранов (МЭ).

33. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов.

34. Программно-аппаратные средства защиты информации в сетях передачи данных.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ *(9 СЕМЕСТР)*

1. Проблемы обеспечения безопасности при удаленном доступе.

2. Протоколы аутентификации PAP и CHAP.

3. Протоколы аутентификации удаленного доступа в программных средствах Microsoft.

4. Система аутентификации и авторизации TACACS и Kerberos.

5. Понятие виртуальной частной сети, ее предназначение. Реализация в программных средствах Microsoft.

6. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД.

7. Защита от несанкционированного доступа.

8. Защита от вывода.

9. Целостность БД. Аудит.

10. Задачи и средства администратора безопасности баз данных.

11. Основные виды и причины возникновения угроз целостности.

12. Способы противодействия. Назначение словаря данных.

13. Доступ к словарю данных. Состав словаря. Представление словаря.

14. Фиксация транзакции. Прокрутки вперед и назад.

15. Контрольная точка. Откат.

16. Транзакции как средство изолированности пользователей. Режимы блокировок.

17. Внешний ключ. Способы поддержания ссылочной целостности.

18. Причины, виды, основные методы нарушения конфиденциальности.

19. Типы утечки конфиденциальной информации из СУБД, частичное разглашение.

20. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия.

21. Виды привилегий: привилегии безопасности и доступа.

22. Концепция и реализация механизма ролей.

23. Соотношение прав доступа, определяемых ОС и СУБД.

24. Метки безопасности.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Проскурин В.Г. Защита программ и данных. Учебное пособие 2-е изд., стер. – М.: «Академия», 2012 – 208 с.

2. Семенко В.А., Федоров Н.В. Программно-аппаратная защита информации [Электронный ресурс]: – М.: МГИУ, 2007– Режим доступа: https://studfiles.net/preview/3580869/page:4/

3. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учебное пособие. Издание 2-е испр. и доп. – М. : «Академия», 2006.

4. Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Издание 2-е испр. и доп.– М.: Машиностроение-1, 2006

7.2 Дополнительная литература

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: М: ИД «Форум», Инфра-М, 2014. – Доступ из ЭБС «znanium.com».

2. Касперский К. Компьютерные вирусы изнутри и снаружи [Электронный ресурс]: СПб: Питер, 2007 – Режим доступа: http://nemalo.net/books/490344-kris-kasperski-kompyuternye-virusy-iznutri-i-snaruzhi-2006.html

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Москвин В.В. Методические указания к выполнению лабораторной работы «Проверка настроек разрешительной системы доступа» по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для обучающихся направлений 10.05.03, 10.03.01. Курган: КГУ, 2017. – 37 с.

2. Москвин В.В. Методические указания к выполнению лабораторных работ по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для обучающихся очной формы обучения для направлений 10.05.03, 10.03.01. Курган: КГУ, 2017. – 59 с.

3. Москвин В.В. Методические указания к выполнению практических заданий по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для обучающихся очной формы обучения для направлений 10.05.03, 10.03.01. Курган: КГУ, 2017. – 22 с.

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Сайт федеральной службы по техническому и экспортному контролю - http:// fstec.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. http://www.securitycode.ru;
8. http://infotecs.ru.

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A, Oracle VirtualBox, Комплекс для защиты от НСД Strong Disk Net, Strong Disk Pro, Strong Disk Server, Фикс - 2.0.1, Анализатор механизма очистки внешней памяти НКВД-2.4 и НКВД -2.5, Ревизор 1XP и 2XP, "Secret Net 5.0 - C" с платой аппаратной поддержки Secret Net Touch Memory card.

12. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Программно-аппаратные средства защиты информации»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специализация №5: **Безопасность открытых информационных систем**

Трудоемкость дисциплины: 9 з.е. (324 академических часа)
Семестр: 8, 9 (очная форма обучения)
Форма промежуточной аттестации: Экзамен, экзамен
Содержание дисциплины. Основные разделы

Введение. Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ. Программно-аппаратные средства криптографической защиты. Защита программ. Подсистемы защиты информации в ОС Windows NT. Подсистема защиты информации в ОС UNIX. Защита информации при интеграции UNIX и Windows NT. Атаки на сетевые службы. Адаптивная безопасность в ВС. Межсетевые экраны. Удаленный доступ к сети. Виртуальные частные сети. Политика безопасности. Понятия безопасности БД. Критерии защищенности БД. Модели безопасности в СУБД. Механизмы обеспечения целостности СУБД. Механизмы обеспечения конфиденциальности в СУБД.