МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
«__» _____ 2018 г.

ПРОГРАММНО-АППАРАТНЫЕ СИТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Методические указания для самостоятельной работыдля студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность»

Курск 2018

УДК 621.(076.1)

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» А.Л. Марухленко

Программно-аппаратные системы защиты информации [Текст] : методические указания для самостоятельной работы/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2018. – 11 с. – Библиогр.: с. 11.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается содержание курса, порядок выполнения самостоятельных работ.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать 07.02.18. Формат 60х84 1/16.
Усл.печ. л. 0,64. Уч.-изд. л. 0,58. Тираж 100 экз. Заказ. Бесплатно. 469
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание курса

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение.	Цели и задачи программно–аппаратной защиты информации
2.	Доступ к данным. идентификация и аутентификация субъектов доступа.	Идентификация и аутентификация субъектов доступа. Разграничение доступа к устройствам. Замкнутая программная среда. Вопросы корректности идентификации объекта доступа.
3.	Аппаратная идентификация пользователей.	Основные виды аппаратной идентификации. Электронные устройства ввода идентификационных признаков. Биометрическая идентификация пользователей.
4.	Технологии аутентификации.	Протоколы аутентификации.
5.	Системы аппаратной поддержки механизмов разграничения доступа.	Организация, функции, компоненты, защитные механизмы
6.	Принципы организации контроллера защиты информации.	Реализация средства аппаратной поддержки. Основные функции аппаратного контроллера.
7.	Аппаратные системы разграничения доступа.	Использование архитектур, отличных от фоннеймановской. Системы перлюстрации запросов на обращения к данным. Защита от считывания со сменных носителей.
8.	Программно – аппаратные криптосистемы.	Пригодность различных подходов к шифрованию данных. Общие сведения об аппаратных криптосистемах.

	Технологии шифрования.	Механизмы аппаратной шифрации. Криптографический контроль целостности. Варианты реализации криптосистем. Сравнение аппаратных и программных шифраторов.
9.	Защита программ от несанкционированного копирования	Защита программ от несанкционированного копирования
10.	Защита программ от изучения.	Цели, методы и средства изучения программ. Защита программ от дизассемблирования. Борьба с трассировкой программы пошаговыми отладчиками. Ошибки в созданных и предлагаемых защитах от копирования.
11.	Деструктивные программные воздействия.	Компьютерные вирусы. Шпионские программы. Методы противодействия.
12.	Кейлоггеры.	Программные кейлоггеры. Принципы построения и работы программных кейлоггеров, варианты реализации. Аппаратные кейлоггеры. Устройство, назначение, меры борьбы.

График выполнения СРС

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Введение.	1-2 недели	4
2.	Доступ к данным. идентификация и аутентификация субъектов доступа.	2-3 недели	5

3.	Аппаратная идентификация пользователей.	3-4 недели	6
4.	Технологии аутентификации.	5-6 недели	8
5.	Системы аппаратной поддержки механизмов разграничения доступа.	6-8 недели	10
6.	Принципы организации контроллера защиты информации.	8-9 недели	5
7.	Аппаратные системы разграничения доступа.	9-10 недели	8
8.	Программно – аппаратные криптосистемы. Технологии шифрования.	11-12 недели	5
9.	Защита программ от несанкционированного копирования	12-14 недели	5
10.	Защита программ от изучения.	14-15 недели	6
11.	Деструктивные программные воздействия.	15-16 недели	5
12.	Кейлоггеры.	16-18 недели	5
Итого			72

Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Программно-аппаратные средства защиты информации» являются лекции, практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия

темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Программно-аппаратные системы защиты информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность операционных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Программно-аппаратные системы защиты информации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

Вопросы для самоконтроля

Тема 1. Введение.

1. Предмет и задачи изучения дисциплины
2. Необходимость использования дополнительных программных и аппаратных СЗИ
3. Требования руководящих органов по использованию программно-аппаратных СЗИ

Тема 2. Доступ к данным. Идентификация и аутентификация субъектов доступа.

1. Процедура доступа к данным в современных компьютерных системах
2. Как осуществляется выбор объекта для доступа
3. Форма хранения прав доступа субъектов к объектам
4. Средства осуществления доступа к объектам со стороны пользователей

Тема 3. Аппаратная идентификация пользователей.

1. Причины использования аппаратной идентификации пользователей в компьютерных системах

2. Виды аппаратных идентификаторов, присутствующих на рынке, их характеристики и области применения
3. Технологии биометрической идентификации пользователей (перечислить)
4. Области использования различных систем биометрической идентфкации

Тема 4. Технологии аутентификации.

1. Термины и определения
2. Виды аутентификации
3. Преимущества и недостатки одного из методов аутентификации
4. Пример практической реализации одного из методов аутентификации
5. Предложите схему интеграции одного из методов аутентификации в существующую информационную систему

Тема 5. Системы аппаратной поддержки механизмов разграничения доступа.

1. Варианты реализации средств аппаратной поддержки механизмов обеспечения ИБ
2. Пример использования аппаратной идентфкации пользователя
3. Существующие на рынке решения, использующие механизмы аппаратной поддержки механизмов разграничения доступа

Тема 6. Принципы организации контроллера защиты информации.

1. Назначение контроллера защиты информации
2. Преимущества и недостатки использования контроллеров защиты информации
3. Интеграция контроллера ЗИ в компьютерную систему
4. Дополнительные функции, возникающие у СЗИ с использованием контроллеров ЗИ
5. Области применения контроллеров ЗИ
6. Назовите факторы, препятствующие использованию контроллеров ЗИ

Тема 7. Аппаратные системы разграничения доступа.

1. Примеры аппаратных систем разграничения доступа
2. Предложите вариант реализации исключительно аппаратной СЗИ для защиты определённого компонента компьютерной системы
3. Недостатки аппаратных СЗИ
4. Трудности интеграции аппаратных СЗИ в существующие информационные системы
5. Предложите модель злоумышленника и модель нарушителя, для нейтрализации которых требуются аппаратные СЗИ
6. Предложите модель злоумышленника в систем с использованием исключительно аппаратного СЗИ

Тема 8. Программно – аппаратные криптосистемы. Технологии шифрования.

1. Технологии шифрования (перечислить, указать области применния)
2. Существующие на рынке решения в области криптографической защиты информации
3. Дать сравнительные характеристики программных и аппаратных криптосистем
4. Предложите модель угроз для программной и аппаратной СЗИ

Тема 9. Защита программ от несанкционированного копирования

Классификация методов защиты программного обеспечения от копирования

1. Предложите оптимальные варианты реализации схемы защиты от копирования для: прикладной программы, программы математического моделирования, операционной системы, программного СЗИ
2. Трудности использования средств защиты от копирования
3. Критерии выбора средств защиты ПО от несанкционированного копирования

Тема 10. Защита программ от изучения.

1. Правовые основы защиты программного обеспечения от изучения
2. Модель нарушителя целостности и конфиденциальности программного кода
3. Средства изучения программного кода
4. Последствия взлома программного обеспечения
5. Методы противодействия изучению и отладке программного обеспечения
6. Правовые основы использования антиотладочных средств
7. Устранение человеческого фактора при проектировании защищённого программного обеспечения

Тема 11. Деструктивные программные воздействия.

1. Классифицируйте деструктивные программные воздействия по методам реализации угроз безопасности
2. Опасность самореплицирующихся программ
3. Классификация разработчиков деструктивного программного беспечения
4. Классификация компьютерных вирусов
5. Классификация программ-шпионов
6. Организационные меры противодействия деструктивным программным воздействиям
7. Технические средства противодействия деструктивным программным воздействиям различных типов
8. Классифицируйте разработчиков деструктивного программного обеспечения

Тема 12. Кейлоггеры.

1. Угрозы безопасности, исходящие от кейлоггеров
2. Типы программных кейлоггеров
3. Оцените опасность различных типов кейлоггеров
4. Создайте модель злоумышленника, реализующего различные типы кейлоггеров
5. Меры борьбы с программными кейлоггерами различных типов
6. Опасность аппаратных кейлоггеров
7. Предложите организационные меры борьбы с аппаратными кейлоггерами

8. Технические меры противодействия аппаратным кейлоггерам

Список литературы

1) Программно-аппаратные системы защиты информации [Текст]: учебное пособие / М. О. Таныгин; Министерство образования и науки Российской Федерации, Юго-Западный государственный университет. - Курск: ЮЗГУ, 2012. - 147 с.: ил.табл..

2) Программно-аппаратные средства защиты информационных систем [Текст]: учебное пособие / И. В. Калуцкий, А. Г. Спеваков ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2014. - 179, [2] с.

3) Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - М. : Горячая линия - Телеком, 2012. - 616 с.

4)Информационная безопасность: учебник. [Текст] / Ярочкин В. И. - М.: Академический проект, 2008. - 544 с // http://biblioclub.ru / index.php?page = book&id=211164&sr=1

5)Правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. С. Я. Казанцева. - 3-е изд., стер. - М.: Академия, 2008. - 240 с.

6)Стандарты информационной безопасности: Курс лекций [Текст] / под ред. В. Б. Бетелина. - М.: ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004.

7)Архитектура компьютера [Текст] / Э. Таненбаум - 4-е изд. - СПб. : Питер, 2003. - 704 с.

8)Комплексная защита информации в компьютерных системах [Текст]: учеб. Пособие для студентов вузов / В.И. Завгородний - М.: Логос, 2001.

9) Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах [Текст]: Учебное пособие для студ. вуз. / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. - М.: Радио и связь, 2000. - 168 с. : ил.

10) Зегжда Д. П. Способы безопасности информационных систем: Учеб. пособие для студ. вуз. / А. М. Ивашко. - М.: Горячая линия - Телеком, 2000. - 452 с.