

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ

Первый заместитель Министра
образования Республики Беларусь

_____ И.А. Старовойтова
«_____» _____ 2018 г.
Регистрационный № ТД-_____/тип.

ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**Типовая учебная программа по учебной дисциплине
для специальностей**

**1-98 01 01 Компьютерная безопасность (математические
методы и программные системы)**

1-97 01 02 Прикладная криптография

СОГЛАСОВАНО

Председатель Учебно-
методического объединения по
естественнонаучному образованию
_____ О.А. Ивашкевич
«_____» _____ 2018 г.

СОГЛАСОВАНО

Начальник Главного управления
профессионального образования
Министерства образования
Республики Беларусь
_____ А.С. Касперович
«_____» _____ 2018 г.

СОГЛАСОВАНО

Проректор по научно-методической
работе Государственного
учреждения образования
«Республиканский институт высшей
школы»
_____ И.В. Титович
«_____» _____ 2018 г.

Эксперт-нормоконтролер

_____ 2018 г.
«_____» _____

Минск 2018

СОСТАВИТЕЛИ:

А.Н.Курбацкий, заведующий кафедрой технологий программирования Белорусского государственного университета, доктор технических наук, профессор,

А.А.Марковский, ассистент кафедры технологий программирования Белорусского государственного университета.

РЕЦЕНЗЕНТЫ:

Кафедра микропроцессорных систем и сетей Учреждения образования «Институт информационных технологий БГУИР»;

Ю.И.Иванченко, заведующий НИЛ прикладной информатики НИИ прикладных проблем математики и информатики, кандидат технических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой технологий программирования Белорусского государственного университета
(протокол № 12 от 17 мая 2018 г.).

Научно-методическим Советом Белорусского государственного университета
(протокол № 6 от 16 июня 2018 г.).

Научно-методическим Советом по компьютерной безопасности учебно-методического объединения по естественнонаучному образованию
(протокол № 15 от 29 мая 2018 г.).

Ответственный за редакцию: А.А.Марковский

Ответственный за выпуск: А.Н.Курбацкий

Пояснительная записка

Дисциплина «Программно-аппаратные и технические средства защиты информации» ориентирована на обучение студентов знаниям, умениям и навыкам в области построения программных и программно-аппаратных средств защиты информации. Изучаемые темы базируются на использовании современных информационных технологий, новейшего программного, программно-аппаратного и аппаратного (технического) обеспечения средств защиты информации и компьютеров.

Дисциплина ориентирована на подготовку специалиста, умеющего проектировать и применять средства защиты информации, выбирать наиболее подходящие программные и программно-аппаратные средства защиты, отвечающие современным требованиям и новейшим технологиям в области защиты информации.

Дисциплина имеет целью подготовить специалистов, владеющих знаниями, навыками и умениями в области обеспечения безопасности информации, обрабатываемой на компьютерах и в информационно-телекоммуникационных сетях.

Задачами курса являются изучение основных принципов обеспечения информационной безопасности, методов и средств защиты программных и аппаратных средств от несанкционированного доступа и копирования, принципов их построения, методов и средств обеспечения информационной безопасности в типовых операционных системах, СУБД и сетях, в том числе с использованием средств криптографической защиты информации, системных вопросов защиты программ и данных.

В результате изучения дисциплины студенты должны:

знать:

–методы и аппаратно-программные средства комплексной защиты информационно-телекоммуникационных систем на уровнях защиты программ и данных ПЭВМ, операционных систем, сетей и баз данных

уметь:

–применять методы и средства защиты ПЭВМ;
–строить решения по защите корпоративных информационно-телекоммуникационных систем;

владеть:

–основными приемами обеспечения информационной безопасности с использованием средств криптографической защиты информации, защиты программ и данных;

–знаниями, навыками и умениями в области обеспечения безопасности информации, обрабатываемой на компьютерах и в информационно-телекоммуникационных сетях.

Учебные и воспитательные цели обучения достигаются путем чтения лекций, проведения лабораторных работ, а также самостоятельной подготовки.

Фундаментальная подготовка осуществляется на лекциях. На лекционных занятиях по дисциплине «Программно-аппаратные средства

обеспечения информационной безопасности» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично поискового метода.

Базовые знания формируются на лабораторных занятиях, на которые выносятся вопросы схемно-конструктивного и теоретического характера, нуждающиеся в демонстрации и моделировании на ПЭВМ. На лабораторных занятиях по дисциплине рекомендуется использовать индивидуальный, творческий подход: студенту назначаются индивидуальные алгоритмические задачи по основным разделам курса; студент разрабатывает свой алгоритм решения индивидуальной задачи (доказывает его эффективность с точки зрения трудоемкости и объема используемой памяти) с последующей его реализацией на некотором языке программирования.

Активные методы обучения являются основополагающими для всех видов учебных занятий. В то же время занятия организуются и проводятся с учетом реализации для каждого студента принципа доступности знаний, являющегося важнейшим психологическим условием гуманизации процесса обучения.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются:

- наличием и использованием в учебном процессе открытых систем автоматического тестирования, которые доступны пользователям через Интернет в любое удобное для них время;
- наличием и полной доступностью электронных (и бумажных) вариантов курсов лекций, учебно-методических пособий и сборников задач по основным разделам дисциплины.

В соответствии с ОСВО 1-98 01 01-01 перечень формируемых компетенций студента должен включать компетенции с кодами АК-4,7, СЛК-3, ПК-1,2,13,15,17, 18,21,22.

Требования к академическим компетенциям специалиста

АК-4. Уметь работать самостоятельно.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

Требования к социально-личностным компетенциям специалиста

СЛК-3. Обладать способностью к межличностным коммуникациям.

Требования к профессиональным компетенциям специалиста

Научно-исследовательская деятельность

ПК-1. Работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации.

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

Организационно-управленческая деятельность

ПК-13. Владеть современными средствами телекоммуникаций.

ПК-15. Организовывать процесс создания, оценки и эксплуатации средств и систем защиты информации, поддерживать и повышать их безопасность; осуществлять контроль за их использованием.

Проектно-конструкторская деятельность

ПК-17. Находить оптимальные проектные решения.

ПК-18. Разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

Производственно-технологическая деятельность

ПК-21. Эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; осуществлять контроль за их использованием; вести необходимую для этого документацию.

ПК-22. Осуществлять поддержку и повышать эффективность эксплуатируемых программных, аппаратно-программных и технических средств и систем защиты информации.

В соответствии с ОСВО 1-98 01 01-01, 1-97 01 02 программа предусматривает для изучения дисциплины всего 104 учебных часов, в том числе 68 часа аудиторных занятий: лекции - 34 часов, лабораторные занятия - 34 часов.

Примерный тематический план

№	Название раздела, темы	Количество аудиторных часов		
		Всего	В том числе	
			Лекции	Лабораторные занятия
1	Основные задачи подсистемы защиты информации	8	4	4
2	Защита информации в ПЭВМ	8	4	4
3	Защита от разрушающих программных воздействий	12	6	6
4	Методы и средства ограничения доступа к компонентам ПЭВМ. Особенности защиты информации в операционных системах	12	6	6
5	Программно-аппаратные средства защиты информации в вычислительных сетях	20	10	10

6	Особенности защиты информации в системах управления базами данных	8	4	4
	ВСЕГО	68	34	34

Содержание

1 Основные задачи подсистемы защиты информации

Разграничения доступа к объектам системы. Идентификация, аутентификация и авторизация пользователей: задачи идентификации, аутентификации и авторизации, основные схемы аутентификации, аутентификация на основе паролей, методы подбора паролей, многофакторная аутентификация пользователя с использованием внешних носителей информации (ключевые дискеты, Touch Memory, Smart Card), аутентификация на основе биометрических характеристик пользователя, достоинства и недостатки различных схем аутентификации. Методы и средства хранения ключевой информации. Аудит: необходимость регистрации потенциально опасных действий пользователей, проблемы практической реализации аудита. Управление списком пользователей и политикой безопасности. Критерии защищенности.

2 Защита информации в ПЭВМ

Методы и средства привязки ПО к аппаратному окружению и физическим носителям. Задача анализа машинного кода. Метод экспериментов, статический метод, динамический метод. Факторы, ограничивающие возможности отладчиков. Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение. Защита от изменения и контроль целостности.

3 Защита от разрушающих программных воздействий

Понятие о вредоносных программах. Классификация компьютерных вирусов. Стелс-технология, полиморфик-технология. Методы заражения программ. Деструктивные функции вредоносных программ. Методы выявления и уничтожения компьютерных вирусов. Антивирусные сканеры, мониторы и сетевые фильтры.

4 Методы и средства ограничения доступа к компонентам ПЭВМ. Особенности защиты информации в операционных системах

Объекты и субъекты доступа. Группирование пользователей, специальные субъекты доступа. Избирательное разграничение доступа. Монитор ссылок. Различные подходы к хранению в системе матрицы доступа. Понятие владельца объекта. Привилегии пользователей. Полномочное разграничение доступа. Контроль информационных потоков. Проблемы реализации контроля потоков. Изолированная программная среда. Методы и средства ограничения доступа к компонентам ПЭВМ. Особенности технической реализации разграничения доступа. Проблемы контроля информационных потоков. Программные средства организации защиты информации в ОС семейств Windows и UNIX.

5 Программно-аппаратные средства защиты ПЭВМ и средства защиты информации в вычислительных сетях

Анализ сетевых протоколов. Специфические атаки на вычислительные сети и их виды. Удаленные атаки в сети Internet. Организация безопасной распределенной обработки информации. Протоколы аутентификации при удаленном доступе. Использование межсетевых экранов (Firewall), возможные способы их реализации. Средства и методы обеспечения целостности и конфиденциальности (программно-аппаратные криптографические средства защиты). Защита от изменения и контроль целостности. Требования к средствам криптографической защиты информации. Особенности разработки средств криптографической защиты информации.

6 Особенности защиты информации в системах управления базами данных

Средства обеспечения защиты информации в системах управления базами данных; средства идентификации и аутентификации объектов баз данных, управление доступом; средства контроля целостности информации, организация аудита; причины, виды, основные методы нарушения конфиденциальности в системах управления базами данных; задачи и средства администратора безопасности баз данных. Специфические атаки на базы данных.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Литература

Основная

1. Белкин П.Ю., Михальский О.О., Першаков А.С. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов. – М.: Радио и связь, 1999. – 168 с.
2. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов. — М.: Радио и связь, 2000. — 168 с.
3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб: Наука и Техника, 2004. — 384 с.: ил.
4. Теория и практика обеспечения информационной безопасности. Под ред. П.Д. Зегжды. М. “Яхтсмен”. 1996.
5. С. Мафтик. Механизмы защиты в сетях ЭВМ. М. Мир. 1993.
6. Щербаков А.Ю.. Разрушающие программные воздействия. Москва. "Эдель". 1993.
7. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через "INTERNET". Санкт-Петербург: НПО "Мир и семья", 1997.
8. Баранов А.П., Борисенко Н.П., Зегжда П.Д, Корт С.С., Ростовцев А.Г. Математические основы информационной безопасности – ВИПС, Орел, 1997.

9. Расторгуев С.П. Программные методы защиты информации в компьютерных сетях. – М: Издательство агентства «Яхтсмен», 1993 – 188 с.
10. СТБ 34.101.8-2006 Программные средства защиты от вредоносных программ и антивирусное программное обеспечение.

Дополнительная:

1. Барсуков В.С., Романцов А.П. Опасность и безопасность в сети INTERNET//Специальная техника – 1999, № 1-2, С. 74-83.
2. Борн Г. Руководство разработчика на Microsoft Windows Script Host 2.0 Мастер-класс/Пер. с англ. – СПб.: Питер; М.: Издательско-торговый дом «Русская редакция», 2001. – 480 с.
3. Бэндел Д. Защита и безопасность в сетях Linux. Для профессионалов. — СПб.: Питер, 2002. — 480 с.
4. М.Купер Анализ типовых нарушений безопасности в сетях – М.: Вильямс, 2001.
5. Х. Кастер. Основы Windows NT и NTFS. “Русская Редакция”. М. 1996.
6. Б. Ключевский. Программные закладки//Системы безопасности связи и телекоммуникаций. – 1998, № 22. – С.60-66.
7. Б. Кришнамурти, Дж. Рексворд. Web-протоколы. Теория и практика. – М.: ЗАО «Издательство БИНОМ», 2002. – 592 с.
8. В. Столингс. Основы защиты сетей - М.: Вильямс, 2002.
9. Т. Оглтри. Практическое применение межсетевых экранов – М.: ДМК, 2001

Методические рекомендации по организации и выполнению самостоятельной работы

Самостоятельная работа студентов организуется в виде выполнения серии индивидуальных заданий, подготовки и представления докладов по отдельным изучаемым темам.

Диагностика компетенций студента

Контроль приобретенных студентами знаний, навыков и умений в процессе текущих занятий проводится с целью определения в течение семестра степени усвоения учебного материала, своевременного вскрытия недостатков в подготовке студентов и принятия необходимых мер по совершенствованию методики преподавания, а также побуждения их к систематической планомерной работе над учебным материалом.

Текущий контроль по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» рекомендуется осуществлять в течение всего семестра в виде вопросов для самоконтроля, проведения 1-2 коллоквиумов и 1-2 контрольных работ (лекционная часть курса).

Для закрепления и проверки знаний и умений студентов (практическая часть курса) рекомендуется разработать систему из 2-3 индивидуальных заданий, которые предполагают разработку эффективного с точки зрения трудоемкости алгоритма с последующей его реализацией на некотором языке программирования. Успеваемость студентов в рамках дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» рекомендуется оценивать в конце семестра в форме экзамена.