МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Институт прикладной математики и компьютерных наук
Кафедра «Информационная безопасность»

Утверждено на заседании кафедры
«Информационная безопасность»
«14» январь 2020 г., протокол № 6

Заведующий кафедрой ИБ
_____ А.А.Сычугов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Методы и средства защиты компьютерной информации»

основной профессиональной образовательной программы
высшего образования – программы бакалавриата

по направлению подготовки
09.03.03 Прикладная информатика

с профилем
Прикладная информатика в промышленности

Форма обучения: *заочная*

Идентификационный номер образовательной программы: 090303-01-20

Тула 2020 год

ЛИСТ СОГЛАСОВАНИЯ
рабочей программы дисциплины (модуля)

Разработчик(и):

Баранов А.Н., доцент каф. ИБ, доцент, канд. техн. наук _____
(ФИО, должность, ученая степень, ученое звание) *(подпись)*

1 Цель и задачи освоения дисциплины (модуля)

Целью изучения дисциплины является освоение методов и средств защиты информации в компьютерных системах и сетях.

Задачами изучения дисциплины являются:

– рассмотрение методов построения модели политики безопасности для организации;

– изучение вопросов идентификации и аутентификации пользователей в системах;

– изучение вопросов криптографической защиты и вопросов контроля целостности информации;

– формирование представлений об организация ключевых систем защиты компьютерной информации;

– изучение организационных, технических и программных методов защиты информации в компьютерных сетях.

2 Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Дисциплина (модуль) относится к обязательной части основной профессиональной образовательной программы.

Дисциплина (модуль) изучается в 7 семестре.

3 Перечень планируемых результатов обучения по дисциплине (модулю)

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы (формируемыми компетенциями) и индикаторами их достижения, установленными в общей характеристике основной профессиональной образовательной программы, приведён ниже.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

1) принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. (код компетенции – ОПК-3 код индикатора – ОПК-3.1)

Уметь:

1) решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (код компетенции – ОПК-3, код индикатора – ОПК-3.2)

Владеть:

1) навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности (код компетенции – ОПК-3, код индикатора – ОПК-3.3).

Полные наименования компетенций и индикаторов их достижения представлены в общей характеристике основной профессиональной образовательной программы.

4 Объем и содержание дисциплины (модуля)

4.1 Объем дисциплины (модуля), объем контактной и самостоятельной работы обучающегося при освоении дисциплины (модуля), формы промежуточной аттестации по дисциплине (модулю)

Номер семестра	Формы промежуточной аттестации	Общий объем в зачетных единицах	Общий объем в академических часах	Объем контактной работы в академических часах						Объем самостоятельной работы в академических часах
				Лекционные занятия	Практические (семинарские) занятия	Лабораторные работы	Клинические практические занятия	Консультации	Промежуточная аттестация	
7	ДЗ	5	180	4	4	4	-	0	0,25	167,75
Итого	-	5	180	4	4	4	-	0	0,25	167,75

Условные сокращения: Э – экзамен, ЗЧ – зачет, ДЗ – дифференцированный зачет (зачет с оценкой), КП – защита курсового проекта, КР – защита курсовой работы.

4.2 Содержание лекционных занятий
Очная форма обучения

№ п/п	Темы лекционных занятий
1	Анализ угроз информационной безопасности
1.1	Основные понятия защиты информации и информационной безопасности
1.2	Анализ угроз информационной безопасности
2	Методы обеспечения информационной безопасности
2.1	Структуризация методов обеспечения информационной безопасности
2.2	Основные методы реализации угроз информационной безопасности
2.3	Основные принципы обеспечения информационной безопасности в автоматизированных системах
2.4	Причины, виды и каналы утечки информации
3	Анализ угроз сетевой безопасности
3.1	Проблемы безопасности IP-сетей
3.2	Угрозы и уязвимости проводных корпоративных сетей
3.3	Угрозы и уязвимости беспроводных сетей
4	Обеспечение информационной безопасности сетей
4.1	Способы обеспечения информационной безопасности
4.2	Пути решения проблем защиты информации в сетях
4.3	Основные понятия политики безопасности
5	Управленческие меры обеспечения информационной безопасности
5.1	Структура политики безопасности организации
5.2	Базовая политика безопасности
5.3	Специализированные политики безопасности
5.4	Процедуры безопасности
6	Стандарты информационной безопасности

№ п/п	Темы лекционных занятий
6.1	Роль стандартов информационной безопасности
6.2	Международные стандарты информационной безопасности
6.3	Отечественные стандарты безопасности информационных технологий
7	Криптографические модели защиты информации
7.1	Перечень средств криптографической защиты информации
7.2	Требования к СКЗИ
7.3	Способы и особенности реализации криптографических подсистем
7.4	Криптографическая защита транспортного уровня АС
7.5	Криптографическая защита на прикладном уровне АС
7.6	Особенности сертификации и стандартизации криптографических средств
8	Принципы криптографической защиты информации
8.1	Основные понятия криптографической защиты информации
8.2	Симметричные криптосистемы шифрования
8.3	Асимметричные криптосистемы шифрования
8.4	Комбинированная криптосистема шифрования
8.5	Электронная подпись и функция хэширования
8.6	Управление криптоключами
8.7	Классификация криптографических алгоритмов
9	Современные симметричные криптосистемы
9.1	Принципы работы симметричных криптосистем
9.2	Американский стандарт шифрования данных DES
9.3	Комбинирование блочных алгоритмов
9.4	Алгоритм шифрования данных IDEA в действии
10	Отечественный стандарт шифрования данных
10.1	Общие сведения об отечественном стандарте шифрования данных
10.2	Работа алгоритмов шифрования отечественного стандарта
11	Обеспечение безопасности операционных систем
11.1	Проблемы обеспечения безопасности ОС
11.2	Архитектура подсистемы защиты ОС
12	Организационно-режимные меры защиты носителей информации
12.1	Парольные системы защиты от несанкционированного доступа к информации
12.2	Парольные системы для защиты от несанкционированного доступа к информации
13	Алгоритмы аутентификации пользователей
13.1	Основные понятия и концепции
13.2	Идентификация и механизмы подтверждения подлинности пользователя
13.3	Взаимная проверка подлинности пользователей
13.4	Протоколы идентификации с нулевой передачей знаний
13.5	Упрощенная схема идентификации с нулевой передачей знаний
14	Технологии межсетевых экранов
14.1	Функции межсетевых экранов
14.2	Особенности функционирования межсетевых экранов на различных уровнях модели OSI
14.3	Схемы сетевой защиты на базе межсетевых экранов
15	Основы технологии виртуальных защищенных сетей VPN
15.1	Концепция построения виртуальных защищенных сетей VPN
15.2	Защита беспроводных сетей
16	Защита на канальном и сеансовом уровнях

№ п/п	Темы лекционных занятий
16.1	Протоколы формирования защищенных каналов на канальном уровне
16.2	Протоколы формирования защищенных каналов на сеансовом уровне
17	Защита на сетевом уровне — протокол IPSEC
18	Защита на прикладном уровне
18.1	Управление идентификацией и доступом
18.2	Организация защищенного удаленного доступа
18.3	Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)
18.4	Протокол Kerberos
18.5	Инфраструктура управления открытыми ключами PKI
19	Анализ защищенности и обнаружение атак
19.1	Концепция адаптивного управления безопасностью
19.2	Технология анализа защищенности
19.3	Технологии обнаружения атак

4.3 Содержание практических (семинарских) занятий
Очная форма обучения

№ п/п	Наименования лабораторных работ
1	Практическая работа №1. Алгоритмы симметричного шифрования. Гаммирование
2	Практическая работа №2. Шифрование перестановкой
3	Практическая работа №3. Алгоритмы симметричного шифрования. Алгоритмы замены
4	Практическая работа №4. Блочные алгоритмы симметричного шифрования. Часть 1
5	Практическая работа №5. Блочные алгоритмы симметричного шифрования. Часть 2.

4.4 Содержание лабораторных работ
Очная форма обучения

№ п/п	Наименования лабораторных работ
1	Лабораторная работа №1. Симметричные криптографические системы
2	Лабораторная работа №2. Электронная подпись
3	Лабораторная работа №3. Отечественный стандарт вычисления хэш-функции
4	Лабораторная работа №4. Парольные системы
5	Лабораторная работа №5. Отечественный стандарт шифрования данных
6	Лабораторная работа №6. Стандарт шифрования данных DES
7	Лабораторная работа №7. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации
8	Лабораторная работа №8. Использование функций криптографического интерфейса Windows для защиты информации
9	Лабораторная работа №9. Разработка программы для шифрования текстовых файлов на основе функций CRYPTOAPI
10	Лабораторная работа № 10. Количественная оценка стойкости парольной защиты

4.5 Содержание клинических практических занятий

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.6 Содержание самостоятельной работы обучающегося

Очная форма обучения

№ п/п	Виды и формы самостоятельной работы
1	Подготовка к лабораторным и практическим работам
2	Оформление лабораторных и практических работ
2	Подготовка к промежуточной аттестации и ее прохождение

5 Система формирования оценки результатов обучения по дисциплине (модулю) в рамках текущего контроля успеваемости и промежуточной аттестации обучающегося

Очная форма обучения

Мероприятия текущего контроля успеваемости и промежуточной аттестации обучающегося			Максимальное количество баллов
Текущий контроль успеваемости		**Оцениваемая учебная деятельность обучающегося:**	
		Посещение лекционных занятий	20
		Выполнение лабораторной работы № 1	5
		Выполнение лабораторной работы № 2	5
		Выполнение лабораторной работы № 3	5
		Выполнение лабораторной работы № 4	5
		Выполнение лабораторной работы № 5	5
		Выполнение лабораторной работы № 6	5
		Выполнение лабораторной работы № 7	5
		Выполнение лабораторной работы № 8	5
		Итого	60
Промежуточная аттестация	*Дифференцированный зачет*		40 (100*)

* В случае отказа обучающегося от результатов текущего контроля успеваемости

Шкала соответствия оценок в стобалльной и академической системах оценивания результатов обучения по дисциплине (модулю)

Система оценивания результатов обучения	Оценки			
Стобалльная система оценивания	0 – 39	40 – 60	61 – 80	81 – 100
Академическая система оценивания (экзамен, дифференцированный зачет, защита курсового проекта, защита курсовой работы)	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Академическая система оценивания (зачет)	Не зачтено	Зачтено		

6 Описание материально-технической базы (включая оборудование и технические средства обучения), необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для осуществления образовательного процесса по дисциплине (модулю) требуется: для проведения лекционных занятий по дисциплине требуется стандартная аудитория, оснащенная доской, или аудитория, оснащенная видеопроектором, настенным экраном, ноутбуком; для проведения лабораторных работ требуется компьютерный класс.

Компьютерный класс должен быть оснащен операционными системами Windows/ Linux, средой разработки программного обеспечения на любом из языков программирования высокого уровня (например, Geany, IDLE, Qt Creator, CLion, Eclipse, Xcode), а также офисными программами, содержащими текстовые редакторы.

Специализированное оборудование не требуется.

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература

1. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина .— Москва : Академия, 2009 .— 269 с.

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. Учебное пособие для вузов / П.Б.Хорев – М.: Академия, 2012. – 256 с.

7.2 Дополнительная литература

1. Девянин П.Н. Модели безопасности компьютерных систем. Учебное пособие для вузов. – М.: Академия, 2015. – 144 с.

2. Журнал "HARD"n"SOFT"

3. Журнал "PC Magazine" / RE

4. Журнал "Вопросы защиты информации"

5. Журнал "Защита информации. Инсайд"

8 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Защита информации. Инсайд [Электронный ресурс] – Режим доступа: http://www.inside-zi.ru

2. Защита информации. Конфидент [Электронный ресурс] – Режим доступа: http://www.confident.ru

3. Электронный читальный зал "БИБЛИОТЕХ" : учебники авторов ТулГУ по всем дисципли6. нам. [Электронный ресурс] – Режим доступа: https://tsutula.bibliotech.ru/, по паролю.- Загл. с экрана

4. ЭБС IPRBooks универсальная базовая коллекция изданий. [Электронный ресурс] – Режим доступа: http://www.iprbookshop.ru/, по паролю.- Загл. с экрана

5. Научная Электронная Библиотека eLibrary - библиотека электронной периодики.- [Электронный ресурс] – Режим доступа: http://elibrary.ru/, по паролю.- Загл. с экрана.

6. НЭБ КиберЛенинка научная электронная библиотека открытого доступа/ [Электронный ресурс] – режим доступа http://cyberleninka.ru/, свободный.- Загл. с экрана.

9 Перечень информационных технологий, необходимых для осуществления образовательного процесса по дисциплине (модулю)

9.1 Перечень необходимого ежегодно обновляемого лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. ОС Windows (Linux).
2. ПО МойОфис.
3. Среды разработки программного обеспечения: Geany, IDLE, Qt Creator, CLion, Eclipse, Xcode.

9.2 Перечень необходимых современных профессиональных баз данных и информационных справочных систем

Современные профессиональные базы данных и информационные справочные системы не требуются.