Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Технология и системы управления в машиностроении»

РАБОЧАЯ ПРОГРАММА

по дисциплине

М.1.1.6 «Хранение и защита компьютерной информации»

направления подготовки
15.04.04 - Автоматизация технологических процессов и производств
профиль "Информационные технологии автоматизации"

форма обучения – очная
курс – 1
семестр - 1
зачётных единиц – 4
часов в неделю – 2
академических часов – 144
в том числе:
лекции – 8
коллоквиум – нет
практические занятия – 28
самостоятельная работа – 108
экзамен – 1-й семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины «Хранение и защита компьютерной информации»: формирование профессиональных компетенций в соответствие с федеральным государственным образовательным стандартом; фундаментализация образования; ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами хранения и защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами и перспективами их развития; приобретение студентами знаний, практических умений и навыков в применении методов и средств защиты информации в компьютерных системах, необходимых для эффективного проведения политики информационной безопасности.

Задачи изучения дисциплины: общая концепция информационной безопасности, правовые и организационные аспекты защиты информации, характер организации атак на информационные системы, понятийный аппарат в области защиты информации, законодательство в области защиты информации, основные положения по защите авторских прав в информационных системах, основные проблемы и перспективы криптографической защиты информации, базовые механизмы защиты информации в персональных компьютерах, нетрадиционные методы защиты информации, методы и средства защиты локальных сетей, методы и средства защиты информации при работе в Internet, специфика защиты баз данных, протоколы сетевой безопасности.

2. Место дисциплины в структуре ООП ВО

Данная учебная дисциплина входит в базовую часть дисциплин учебного плана подготовки магистра по направлению 15.04.04 - Автоматизация технологических процессов и производств.

Данная дисциплина является логической и методической основой для дисциплин « Информационные технологии в автоматизации и управлении», «Проектирование систем автоматизации и управления», « Интегрированные системы проектирования и управления автоматизированных и автоматических производств», а также для научно-исследовательской практики.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ПК-16 *способностью проводить математическое моделирование процессов, оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления с использованием современных технологий научных исследований, разрабатывать алгоритмическое и программное обеспечение средств и систем автоматизации и управления;*

Знает: концептуальные основы информационной безопасности, законодательство Российской Федерации в сфере информационной

безопасности, руководящие документы в области информационной безопасности
Умеет: осуществлять выбор и планировать применение средств защиты информации в компьютерных системах
Владеет: навыками организационного обеспечения информационной безопасности
ОПК-3 *способностью разрабатывать (на основе действующих стандартов) методические и нормативные документы, техническую документацию в области автоматизации технологических процессов и производств, в том числе жизненному циклу продукции и ее качеству, руководить их созданием*;
Знает: общую концепцию информационной безопасности, правовые и организационные аспекты защиты информации, характер организации атак на информационные системы, понятийный аппарат в области защиты информации, законодательство в области защиты информации, основные положения по защите авторских прав в информационных системах, основные проблемы и перспективы криптографической защиты информации, специфику защиты баз данных, протоколы сетевой безопасности;
Умеет: осуществлять выбор и планировать базовые механизмы защиты информации в персональных компьютерах, нетрадиционные методы защиты информации, методы и средства защиты локальных сетей, методы и средства защиты информации при работе в Internet;
Владеет: навыками разработки (на основе действующих стандартов) методических и нормативных документов, технической документации в области хранения и защиты компьютерной информации.
ПК-5 *способностью разрабатывать функциональную, логическую и техническую организацию автоматизированных и автоматических производств, их элементов, технического, алгоритмического и программного обеспечения на базе современных методов, средств и технологий проектирования*;
Знает: организационное обеспечение информационной безопасности, основы криптографической защиты информации в информационных системах, методы и средства защиты и хранения информации в персональных компьютерах и локальных компьютерных сетях, особенности защиты информации в базах данных, средства обеспечения безопасной работы в глобальных компьютерных сетях, возможные сетевые атаки и технологию защиты от них, основы построения отказоустойчивых компьютерных систем, организацию комплексного подхода к обеспечению информационной безопасности на объектах;
Умеет: использовать современные системные программные средства и средства для защиты информации в сети и на отдельных рабочих станциях, применять антивирусные программы для профилактики заражения и дезинфекции компьютера, устанавливать права доступа различным группам пользователей и оперативно вносить изменения в политику безопасности информационной системы, проводить поиск слабых мест в компьютерной системе и принимать меры по их устранению;

Владеет: навыками организации криптографической защиты информации в автоматизированных системах управления, обеспечения безопасной работы в компьютерных сетях, по технологии защиты от возможных сетевых атак.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ модуля	№ недели	№ темы	Наименование темы	Часы				
				Всего	Лекции	Практические	СРС	Коллоквиум
1	2	3	4	5	6	7	8	9
2 семестр								
1	1-2	1	Законодательные и правовые основы защиты компьютерной информации	13	1	2	10	
	2-3	2	Проблемы защиты информации в системах управления	17	1	2	14	
	4-6	3	Теоретические основы компьютерной безопасности	21	1	6	14	
	7-10	4	Современные криптосистемы для защиты компьютерной информации	21	1	6	14	
2	11-12	5	Методы идентификации и проверки подлинности пользователей	17	1	2	14	
	13-14	6	Защита систем от удаленных атак	17	1	2	14	
	15-16	7	Методы защиты от разрушающих программных воздействий (программных закладок и вирусов)	19	1	4	14	
	17-18	8	Комплексная защита процесса обработки информации в компьютерных системах	19	1	4	14	
Всего				144	8	28	108	

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
1-2	2	1	**Законодательные и правовые основы защиты компьютерной информации.**	[1,3,5,7,8]

			Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности. Нормативно правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления. **Проблемы защиты информации в системах управления.** Угрозы информационной безопасности. Меры противодействия угрозам безопасности. Меры по обеспечению сохранности информации. Основные задачи обеспечения безопасности информации. Защита локальных сетей и операционных систем.	
3	1	2	**Теоретические основы компьютерной безопасности.** Модели безопасности, политика безопасности, критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем, стандарты по оценке защищенных систем, парольные системы, криптографические методы, системы с симметричными и несимметричными ключами, концепция защищенного ядра, методы верификации данных, защищенные домены, применение иерархического метода для построения защищенной операционной системы, корректность систем защиты, обследование и проектирования защиты, модель политики контроля целостности.	**[1,2,7,8]**
4	1	3	**Современные криптосистемы для защиты компьютерной информации.** Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Симметричные системы шифрования	**[1,3,4,7]**

			(системы с секретным ключом): поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы использования.	
5-6	2	4	**Методы идентификации и проверки подлинности пользователей.** Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы и схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль-Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи. **Защита систем от удаленных атак.** Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.	**[1,2,5,8]**

7-8	2	5	**Методы защиты от разрушающих программных воздействий (программных закладок и вирусов).** Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды. **Комплексная защита процесса обработки информации в компьютерных системах.** Функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности в технологическую среду.	**[1,3,6,8]**

6. Содержание коллоквиумов

Не предусмотрены учебным планом.

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4	5
1, 2	4	1-2	**Основы шифрования данных.** Изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.	**[1,2,4,12,13,18]**
3	6	3-5	**Блочное симметричное шифрование** Изучение структуры и основных принципов работы современных алгоритмов блочного симметричного шифрования, приобретение навыков программной реализации блочных симметричных шифров.	**[2,3,5,15,18]**

4	6	6-8	**Поточное симметричное шифрование.** Изучение структуры и основных принципов работы современных алгоритмов поточного симметричного шифрования, приобретение навыков программной реализации поточных симметричных шифров.	**[1,2,5,16,18]**
5, 6	4	9-10	**Асимметричная криптография и электронная цифровая подпись на примере системы GnuPG.** Знакомство с принципами криптографической защиты информации с использованием алгоритмов асимметричного шифрования и электронной цифровой подписи, приобретение навыков практического применения указанных методов защиты информации на основе системы GnuPG.	**[1,2,4,12,18]**
7, 8	8	11-14	**Средства обеспечения безопасности ОС Windows.** Изучение модели безопасности операционной системы Windows, получение навыков практического использования ее средств обеспечения безопасности.	**[2,3,6,17,18]**

8. Перечень лабораторных работ

Не предусмотрены учебным планом.

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Вопросы для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	**2**	**3**	**4**
1	10	Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления.	**[1,3,5,18]**
2	14	Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-	**[1,2,7,8]**

		аналитического обеспечения СУ. Защита информации в Internet.	
3	14	Архитектура электронных систем обработки данных; формальные модели; модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем; особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; концепция защищенного ядра; методы верификации; защищенные домены; применение иерархического метода для построения защищенной операционной системы; исследование корректности систем защиты; методология обследования и проектирования защиты; модель политики контроля целостности. Архивация данных, общие принципы, классификация методов. Алгоритм Хаффмана и Лемпеля-Зива.	**[1,3,4,18]**
4	14	Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89:	**[1,2,5,8]**

		алгоритм, скорость работы на различных платформах, режимы пользования. Асимметричные системы шифрования (системы с открытым ключом). Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля.	
5	14	Основные понятия и концепции идентификации и механизмов подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Механизм распространения открытых ключей. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль-Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.	**[1,3,6,7,18]**
6	14	Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. Администрирование в информационных системах. Программно-аппаратные средства защиты ПЭВМ и сетей; методы средства ограничения доступа к компонентам сети; методы и средства привязки программного обеспечения к аппаратному окружению к	**[1,2,4,8]**

		физическим носителям: методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.	
7	14	Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Разрушающее программное воздействие. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.	**[1,2,5,18]**
8	14	Состав компонентов комплексной системы обеспечения информационной безопасности; функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности в технологическую среду; этапы проектирования и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение; особенности проектирования на современном уровне и синтез; типовая структура комплексной системы защиты информации от несанкционированного доступа; мониторинг и контроль окружающей среды; ведение специальной информационной базы данных.	**[2,3,6,7,8,17]**

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС

10. Расчетно-графическая работа

Не предусмотрена учебным планом.

11. Курсовая работа

Не предусмотрена учебным планом.

12. Курсовой проект

Не предусмотрен учебным планом.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Процедура оценивания знаний, умений и навыков проводится в соответствии со следующими методическими материалами и заключается в проведении устного экзаменационного опроса в виде диалога преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала, оценка способности студента применить полученные ранее знания; в проведении модулей и коллоквиумов, как способов межсессионной проверки знаний, умений, навыков студента в середине семестра по пройденным темам изучаемого предмета.

Показателем оценивания степени усвоения знаний является оценка, полученная на экзамене при ответе на вопросы для экзамена. Оценка выставляется по четырехбалльной шкале, соответствующей оценкам «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и осуществляется путем анализа ответа на вопросы для экзамена. При этом руководствуются следующими критериями.

Оценка	Критерии оценивания результатов обучения (дескрипторы)
Отлично	заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой.
Хорошо	заслуживает обучающийся, обнаруживший полное знание учебного материала, усвоивший основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.
Удовлетворительно	заслуживает обучающийся, обнаруживший знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей

	работы по профессии, знакомых с основной литературой, рекомендованной программой. Оценка выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.
Неудовлетворительно	выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине.

Умения и навыки, приобретенные студентом на этапе освоения указанной части компетенций при преподавании рассматриваемой дисциплины, оцениваются по результатам выполнения практических заданий, включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить. Показателем оценивания степени усвоения знаний этого элемента компетенции, является оценка, полученная при представлении материалов и докладе по выданной теме. Оценка выставляется по четырехбальной шкале, соответствующей оценкам «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и осуществляется путем анализа представленного материала в ответ на практические контрольные задания. При этом руководствуются следующими критериями:

Оценка	Критерии оценивания результатов обучения (дескрипторы)
Отлично	5 баллов выставляется студенту, если задание выполнено в полном объёме с соблюдением необходимой последовательности. Студенты работают полностью самостоятельно: подбирают необходимые для выполнения предлагаемых работ в задании источники знаний, показывают необходимые для проведения практической работы теоретические знания, практические умения и навыки.
Хорошо	4 балла выставляется студенту, если задание выполнено в полном объёме и самостоятельно. Допускаются отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Студенты используют указанные преподавателем источники знаний, включая страницы атласа, таблицы из приложения к учебнику, страницы из справочной литературы по предмету. Задание

	показывает знание учащихся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Могут быть неточности и небрежность в оформлении результатов работы.
удовлетворительно	3 балла выставляется студенту, если задание на практическую работа выполняется и оформляется студентами при помощи преподавателя или хорошо подготовленных и уже выполненных на «отлично» данную работу студентов. На выполнение задания затрачивается много времени (можно дать возможность доделать работу дома). Студенты показывают знания теоретического материала, но испытывают затруднение при самостоятельной работе с физическими приборами, графиками, таблицами справочной литературы.
неудовлетворительно	2 балла выставляется, если студенты показывают плохое знание теоретического материала и отсутствие умения применить знания к решению практической задачи. Руководство и помощь со стороны преподавателя и хорошо подготовленных студентов неэффективны по причине плохой подготовки студента.

Процедура оценивания знаний, умений, навыков включает учет успешности выполнения практических работ, самостоятельной работы и сдачу экзамена.

Вопросы для экзамена

1. Стратегия информационной безопасность в Российской Федерации и основные группы документов, ее определяющие.
2. Доктрина информационной безопасности Российской Федерации. Основные виды возможных угроз информации.
3. Доктрина информационной безопасности Российской Федерации. Общие методы, первоочередные меры и организационно-техническим мероприятия, направленные на обеспечения информационной безопасности.
4. Закон РФ «Об информации, информатизации и защите информации» №24-ФЗ от 20 февраля 1995 года.
5. Уголовное законодательство в сфере защиты информации.
6. Основные термины и определения в области защиты информации.

7. Организационные мероприятия по защите информации.
8. Организационно-технологические мероприятия по защите информации в автоматизированных системах.
9. Задачи технологии обеспечения безопасности информации.
10. Основные документы по информационной безопасности в организации (на предприятии).
11. Организационные мероприятия по пресечению попыток негласного получения информации.
12. Мероприятия аттестации объектов вычислительной техники.
13. Уровни автоматизированных систем и классы их уязвимостей.
14. Классификация и модели компьютерных атак.
15. Локальные атаки.
16. Удаленные атаки.
17. Атаки на потоки данных.
18. Модели "традиционной" атаки.
19. Модели распределенных (скоординированных) атак.
20. Этапы компьютерных атак.
21. Сбор информации перед компьютерной атакой.
22. Реализация компьютерной атаки.
23. Завершение компьютерной атаки.
24. Классификация нарушителей компьютерной безопасности, их цели и мотивация.
25. Основные понятия криптографии.
26. Требования к современным криптосистемам.
27. Классификация методов шифрования.
28. Стойкость шифров.
29. Понятие о хэш-функции.
30. Общие схемы блочного и поточного шифрования.
31. Шифрование заменой (подстановкой). Таблица замены. Шифр Цезаря.
32. Шифрование заменой (подстановкой). Буквенная ключевая последовательность. Шифр Вижинера.
33. Числовая ключевая последовательность. Условия нераскрываемости шифра Шеннона.
34. Шифрование с использованием алгебры матриц.
35. Блочная подстановка (замена) – блочный шифр.
36. Шифрование перестановками.
37. Перестановка по маршрутам Гамильтона.
38. Шифры и способы перестановки.
39. Шифры взбивания (скремблеры).
40. Идеи комбинационного шифрования К. Шеннона.
41. Гаммирование двоичного текста.
42. Недостатки шифра замены с помощью операции *XOR*.
43. Потоковое шифрование. Недостатки блочного шифрования.
44. Синхронное потоковое шифрование. Классификация.
45. Самосинхронизирующееся поточное шифрование.

46. Стеганография. Примеры методов с использованием и без использования технических средств.
47. Компьютерная стеганография. Принципы, достоинства и недостатки.
48. Требования к стегосистемам.
49. Методы компьютерной стеганографии.
50. Криптофония. Скремблирование сообщений.
51. Программа *PGP*.
52. Алгоритм Диффи-Хеллмана.
53. Алгоритм Эль-Гамаля.
54. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.
55. Механизмы подтверждения подлинности пользователя.
56. Аутентификации данных и электронная цифровая подпись.
57. Алгоритм цифровой подписи DSA.
58. Отечественный стандарт цифровой подписи.
59. Функционирования межсетевых экранов и их основные компоненты.
60. Маршрутизаторы.
61. Шлюзы сетевого уровня.
62. Применение межсетевых экранов.
63. Защита от закладок и дизассемблирования.
64. Способы встраивания защитных механизмов в программное обеспечение.
65. Понятие разрушающего программного воздействия.
66. Модели взаимодействия прикладной программы и программной закладки.
67. Методы перехвата и навязывания информации.
68. Методы внедрения программных закладок.
69. Компьютерные вирусы.
70. Защита от разрушающих программных воздействий.

Тестовые задания по дисциплине

1?
Базовым документом, определяющим стратегию информационной безопасность в Российской Федерации является

- Закон РФ «О Государственной тайне» №5151-1 от 21 июля 1993 года;
- «Об информации, информатизации и защите информации» №24-ФЗ от 20 Февраля 1995 года;
- Указ Президента РФ «О защите информационных и телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» № 644 от 8 сентября 1993 года;
- Решение Государственной технической комиссии (Гостехкомиссии) при Президенте Российской Федерации «Основы концепции защиты информации в Российской Федерации» №6 от 16 ноября 1993 года;
- «Доктрина информационной безопасности Российской Федерации», утвержденная Президентом РФ 9 сентября 2000 года;
- ГОСТ РВ 50600-93. Защита информации от технической разведки. Система документов. Общие положения.

2?
Распределение реквизитов разграничения доступа относится к
- периодически проводимым мероприятиям;
- мероприятиям, проводимым по необходимости;
- разовым мероприятиям;
- постоянно проводимым мероприятиям.
3?
Специсследование технических средств обработки информации это
- проверка технических средств на предмет выявления внедренных радиоэлектронных средств несанкционированного съема информации;
- проверка технических средств на предмет выявления каналов утечки информации;
- проверка объекта на предмет выполнения требований нормативно-методических и руководящих документов по защите информации.
4?
Проверкой объекта на предмет выполнения требований нормативно-методических и руководящих документов по защите информации называется
- спецпроверкой технических средств обработки информации;
- аттестацией объекта вычислительной техники;
- специсследованием технических средств обработки информации.
5?
не используемый на узле сети сервис удаленного доступа (*Telnet*) относится к классу уязвимости
- реализации;
- эксплуатации;
- проектирования.
6?
Социальная инженерия –
- обход парольной защиты базовой системы ввода-вывода (BIOS);
- атаки на средства аутентификации;
- сбор сведений об автоматизированной системе, основанный на человеческом факторе.
7?
Установка закладок в аппаратном обеспечении - это
- получение доступа за счет передачи первоначального обращения не к стационарному (жесткий диск, сетевая карта) а к внешнему носителю;
- наличие в системе устройства, выполняющего некоторые недокументированные или недекларированные функции в ущерб пользователю;
- обход парольной защиты базовой системы ввода-вывода (BIOS).
8?
К локальным атакам относятся
- Атаки на устройства с уникальными параметрами;
- атаки посредством постороннего программного обеспечения;
- атаки на целостность;

- интерактивные атаки.

9?

Атака типа "*маскарад"* относится к

- удаленной атаке;
- локальной атаке;
- атаке на поток данных.

10?

Ренегатство- это тип атаки, когда

- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель посылает законному пользователю сообщение от имени другого законного пользователя;
- нарушитель повторяет ранее переданное сообщение, которое один законный пользователь посылал другому;
- нарушитель «заявляет», что он не посылал сообщения законному пользователю, хотя в действительности он его передавал;
- нарушитель изменяет полученное сообщение и «заявляет», что сообщение в таком виде получено от законного пользователя;
- нарушитель самостоятельно формирует сообщение и «заявляет», что получил его от законного пользователя.

11?

Подделка - это тип атаки, когда

- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель посылает законному пользователю сообщение от имени другого законного пользователя;
- нарушитель повторяет ранее переданное сообщение, которое один законный пользователь посылал другому;
- нарушитель «заявляет», что он не посылал сообщения законному пользователю, хотя в действительности он его передавал;
- нарушитель изменяет полученное сообщение и «заявляет», что сообщение в таком виде получено от законного пользователя;
- нарушитель самостоятельно формирует сообщение и «заявляет», что получил его от законного пользователя.

12?

Переделка - это тип атаки, когда

- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель посылает законному пользователю сообщение от имени другого законного пользователя;
- нарушитель повторяет ранее переданное сообщение, которое один законный пользователь посылал другому;
- нарушитель «заявляет», что он не посылал сообщения законному пользователю, хотя в действительности он его передавал;

- нарушитель изменяет полученное сообщение и «заявляет», что сообщение в таком виде получено от законного пользователя;
- нарушитель самостоятельно формирует сообщение и «заявляет», что получил его от законного пользователя.

13?

Маскарад- это тип атаки, когда

- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель посылает законному пользователю сообщение от имени другого законного пользователя;
- нарушитель повторяет ранее переданное сообщение, которое один законный пользователь посылал другому;
- нарушитель «заявляет», что он не посылал сообщения законному пользователю, хотя в действительности он его передавал;
- нарушитель изменяет полученное сообщение и «заявляет», что сообщение в таком виде получено от законного пользователя;
- нарушитель самостоятельно формирует сообщение и «заявляет», что получил его от законного пользователя.

14?

Повтор - это тип атаки, когда

- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель посылает законному пользователю сообщение от имени другого законного пользователя;
- нарушитель повторяет ранее переданное сообщение, которое один законный пользователь посылал другому;
- нарушитель «заявляет», что он не посылал сообщения законному пользователю, хотя в действительности он его передавал;
- нарушитель изменяет полученное сообщение и «заявляет», что сообщение в таком виде получено от законного пользователя;
- нарушитель самостоятельно формирует сообщение и «заявляет», что получил его от законного пользователя.

15?

Активный перехват - это тип атаки, когда

- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель перехватывает сообщения, которые передают друг другу законные пользователи, и изменяет их;
- нарушитель посылает законному пользователю сообщение от имени другого законного пользователя;

- нарушитель повторяет ранее переданное сообщение, которое один законный пользователь посылал другому;
- нарушитель «заявляет», что он не посылал сообщения законному пользователю, хотя в действительности он его передавал;
- нарушитель изменяет полученное сообщение и «заявляет», что сообщение в таком виде получено от законного пользователя;
- нарушитель самостоятельно формирует сообщение и «заявляет», что получил его от законного пользователя.

16?

Способ атаки подменой адреса источника атаки заключается в
- замене в пакетах злоумышленника IP-адреса другими;
- реализации злоумышленником своих атак с промежуточных узлов (серверов);
- в разбиение IP-пакета на множество более мелких;
- в модификации сценария из базы данных известных атак;
- в удалении всех записей журнала регистрации, фиксирующих несанкционированные действия;
- в изменение идентификаторов сетевого протокола или сервиса.

17?

Способ атаки созданием фальшивых пакетов заключается в
- замене в пакетах злоумышленника IP-адреса другими;
- реализации злоумышленником своих атак с промежуточных узлов (серверов);
- в разбиение IP-пакета на множество более мелких;
- в модификации сценария из базы данных известных атак;
- в удалении всех записей журнала регистрации, фиксирующих несанкционированные действия;
- в изменение идентификаторов сетевого протокола или сервиса.

18?

Способ атаки фрагментацией заключается в
- замене в пакетах злоумышленника IP-адреса другими;
- реализации злоумышленником своих атак с промежуточных узлов (серверов);
- в разбиение IP-пакета на множество более мелких;
- в модификации сценария из базы данных известных атак;
- в удалении всех записей журнала регистрации, фиксирующих несанкционированные действия;
- в изменение идентификаторов сетевого протокола или сервиса.

19?

Способ атаки отказом от значений по умолчанию заключается в
- замене в пакетах злоумышленника IP-адреса другими;
- реализации злоумышленником своих атак с промежуточных узлов (серверов);
- в разбиение IP-пакета на множество более мелких;
- в модификации сценария из базы данных известных атак;

- в удалении всех записей журнала регистрации, фиксирующих несанкционированные действия;
- в изменение идентификаторов сетевого протокола или сервиса.

20?

Способ атаки изменением стандартного сценария атаки заключается в

- замене в пакетах злоумышленника IP-адреса другими;
- реализации злоумышленником своих атак с промежуточных узлов (серверов);
- в разбиение IP-пакета на множество более мелких;
- в модификации сценария из базы данных известных атак;
- в удалении всех записей журнала регистрации, фиксирующих несанкционированные действия;
- в изменение идентификаторов сетевого протокола или сервиса.

21?

Способ атаки чисткой записей регистрации заключается в

- замене в пакетах злоумышленника IP-адреса другими;
- реализации злоумышленником своих атак с промежуточных узлов (серверов);
- в разбиение IP-пакета на множество более мелких;
- в модификации сценария из базы данных известных атак;
- в удалении всей информации из журнала регистрации, фиксирующей несанкционированные действия;
- в изменение идентификаторов сетевого протокола или сервиса.

21?

Практически стойким является шифр

- если размер ключа меньше, чем объем исходного текста;
- если не существует более результативной атаки на него, кроме как полным перебором всех возможных ключей;
- когда размер ключа не меньше размера исходного текста.

22?

Атакой на основе шифротекста называется попытка

- выяснить либо исходный текст, либо ключ шифрования по определенному объему зашифрованных данных;
- определить ключ шифрования по известному исходному тексту и его зашифрованному отображению;
- определить ключ шифрования путем навязывания криптографическому каналу передачи известного текста и перехвата результата шифрования.

23?

Атакой на основе открытого текста называется попытка

- выяснить либо исходный текст, либо ключ шифрования по определенному объему зашифрованных данных;
- определить ключ шифрования по известному исходному тексту и его зашифрованному отображению;

- определить ключ шифрования путем навязывания криптографическому каналу передачи известного текста и перехвата результата шифрования.

24?

Атакой на основе выбранного открытого текста называется попытка

- выяснить либо исходный текст, либо ключ шифрования по определенному объему зашифрованных данных;
- определить ключ шифрования по известному исходному тексту и его зашифрованному отображению;
- определить ключ шифрования путем навязывания криптографическому каналу передачи известного текста и перехвата результата шифрования.

25?

Абсолютная стойкость шифра имеет место,

- когда размер ключа не меньше размера исходного текста;
- если не существует более результативной атаки на него, кроме как полным перебором всех возможных ключей.

26?

Практическая стойкость шифра имеет место,

- когда размер ключа не меньше размера исходного текста;
- если не существует более результативной атаки на него, кроме как полным перебором всех возможных ключей.

27?

Свойством хэш-функции является

-на вход алгоритма преобразования может поступать двоичный блок данных произвольной длины;

-на выходе алгоритма получается двоичный блок данных произвольной длины;

-значения на выходе алгоритма распределяются по произвольному закону во всем диапазоне возможных результатов;

-при изменении хотя бы одного бита на входе алгоритма его выход меняется незначительно;

-зная результат на выходе, невозможно подобрать, кроме как полным перебором, какой-либо входной блок данных;

-невозможно подобрать, кроме как полным перебором, пару различных входных блоков, дающих на выходе произвольный, но одинаковый результат.

28?

Инициализирующая двоичная посылка является принадлежностью

- блочного алгоритма шифрования;
- поточного алгоритма шифрования;
- обоих алгоритмов шифрования.

29?

Какова разрядность ключа шифрования алгоритма DES?

- 56 бит;

- 64 бита;
- 128 бит;
- 256 бит.

30?

Какова разрядность ключа шифрования алгоритма GOST?

- 56 бит;
- 64 бита;
- 128 бит;
- 256 бит.

31?

В которых алгоритмах шифрования используется расширение входных данных?

- ГОСТ;
- DES;
- в обоих.

32?

Сеть Файштеля – это принадлежность

- алгоритма ГОСТ;
- алгоритма DES;
- обоих алгоритмов.

33?

Входная и выходная перестановка бит при шифровании – это процедура

- алгоритма ГОСТ;
- алгоритма DES;
- обоих алгоритмов.

14. Образовательные технологии

Для успешного освоения дисциплины в ходе изложения материала используются лекции на основе мультимедийных презентаций. При изложении материала лектор обсуждает проблемные вопросы, направленные на практическую и самостоятельную деятельность студента. Большое внимание на лекционных и практических занятиях уделяется решению практических задач из курса «Хранение и защита компьютерной информации».

Для развития самостоятельной активности в изучении материала студентам предлагается использование интернет-ресурсов (электронных каталогов, специализированных порталов и сайтов), подготовка к участию в дискуссиях по предлагаемым темам курса, выступление с рефератами. По всем практическим и самостоятельным работам студентам предлагается индивидуальное задание.

При решении задач по программированию студенты делятся на пары. Члены каждой микрогруппы придумывают тесты для проверки задачи коллеги, а также проверяют решения друг друга.

Удельный вес занятий, проводимых в интерактивных формах, составляет 50% аудиторных занятий.

При обучении лиц с ограниченными возможностями и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Для достижения планируемых результатов также используются следующие образовательные технологии:

1. Дистанционные на основе информационно-образовательной среды СГТУ имени Гагарина Ю.А., основе реализации возможности самостоятельного изучения материалов по всем видам образовательной деятельности в соответствии с учебным планом, в том числе до прохождения занятий, текущего дистанционного консультирования студентов.

2. Развивающее проблемно-ориентированное обучение, направленное на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения на основе рассмотрения примеров из практической деятельности преподавателей, в области научно-практических исследований.

3. Личностно ориентированное обучение, обеспечивающее в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе в рамках самостоятельной работы.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Основная литература.

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.

Режим доступа: http://www.iprbookshop.ru/16710

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.

Режим доступа: http://www.iprbookshop.ru/16713

3. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебник/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 442 с.

Режим доступа: http://www.iprbookshop.ru/12053

Дополнительные издания.

4. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 616 с.

Режим доступа: http://www.iprbookshop.ru/12054

5. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ Васильев В.И.— Электрон. текстовые данные.— М.: Машиностроение, 2013.— 172 с.

Режим доступа: http://www.iprbookshop.ru/18519

6. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами [Электронный ресурс]: методические указания к самостоятельной работе студентов. Учебно-методическое пособие/ Бурняшов Б.А.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 55 с.

Режим доступа: http://www.iprbookshop.ru/23077

7. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

8. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

Периодические издания

9. Прикладная информатика –

Режим доступа: http://www.iprbookshop.ru/11770.html

10. Вестник Российского нового университета. Серия Управление, вычислительная техника и информатика –

Режим доступа: http://www.iprbookshop.ru/26390.html

11. Вестник Томского государственного университета. Управление, вычислительная техника и информатика –

Режим доступа: http://www.iprbookshop.ru/8348.html

Интернет-ресурсы

12. Основные Российские образовательные порталы

www.edu.ru - Федеральный портал «Российское образование»

www.informika.ru - Государственный научно-исследовательский институт информационных технологий и телекоммуникаций

13. Интернет - энциклопедия Wikipedia: http://ru.wikipedia.org

14. «Программирование в среде Visual Studio.Net: разработка приложений на языке C#» (2010-2015г.г.)

http://school.sgu.ru/course/view.php?id=29

Учебный постоянно обновляемый ресурс для обучения программированию на языке С.

15. «Программирование на языке С++» (2010-2015г.г.)

http://course.sgu.ru/course/view.php?id=137

Учебный ресурс для обучения программированию на языке С++.

16. Информационно-справочный портал корпорации Microsoft
http://msdn.microsoft.com/ru-ru/default.aspx

Справочный материал по особенностям работы с продуктам Microsoft (Microsoft Office, Visual Studio).

17. Образовательном портале Виртуальной академии Microsoft *http://www.microsoftvirtualacademy.com/*

Справочный материал по особенностям работы с продуктами Microsoft (Microsoft Office, Visual Studio).

Материалы ИОС

18. https://portal3.sstu.ru/Facult/INETM/AUM/15.04.04_1/%D0%9C.1.1.6_1/

17. Материально-техническое обеспечение дисциплины.

Лекционные и практические занятия проходят с использованием компьютеров в компьютерном классе, оборудованном специализированной учебной мебелью, технических средств обучения (мультимедийный проектор, интерактивная доска).

Электронная библиотека вуза:
http://lib.sstu.ru/index.php/elmrazdel/melellib

Электронная информационно-образовательная среда:
https://portal.sstu.ru

Для проведения практических занятий требуются компьютерные классы с программным обеспечением (Microsoft Office 2007/2010,Visual C++, Matlab, MathCad 13, Power Point), рассчитанные на обучение группы студентов из 10–15 человек, удовлетворяющие санитарно-гигиеническим требованиям, работающие под управлением операционной системы Microsoft Windows XP или Windows 7 с подключением к сети Internet.