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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

Б.1.2.16 «Защита информации»

направления подготовки
09.03.01 «Информатика и вычислительная техника»
Профиль «Программное обеспечение средств вычислительной техники и автоматизированных систем»

форма обучения – заочная
курс – 5
семестр – 10
зачетных единиц – 5
академических часов – 180
в том числе:
лекции – 12
практические занятия – 4
лабораторные занятия – 16
самостоятельная работа – 148
экзамен – 10 семестр
курсовой проект – 10 семестр

1. Цели и задачи дисциплины

Изучение «Защиты информации» как дисциплины профессионального цикла направлено на достижение следующих целей:

- развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений.

Задачи дисциплины "Основы информационной безопасности"– дать знания, сформировать умения и навыки по вопросам:

- обеспечения информационной безопасности государства**;**
- методов и средств ведения информационных войн;
- правовых аспектов информационной безопасности;
- нормативного обеспечения в области информационной безопасности;
- каналов утечки информации;
- методов и средств защиты информации.

2. Место дисциплины в структуре ООП ВО:

Дисциплина «Защита информации» относится к числу дисциплин вариативной части Блока 1.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Информатика», «Физика», «Электротехника, электроника и схемотехника», «Программирование», «Сети и телекоммуникации», «Операционные системы», «ЭВМ и периферийные устройства», «Базы данных», «Теория языков программирования и методы трансляции», «Структуры и алгоритмы обработки данных», «Технология разработки программного обеспечения», «Операционная система UNIX».

Изучение курса дисциплины «Защита информации» обеспечивает подготовку к итоговой государственной аттестации.

3. Требования к результатам освоения дисциплины:

Изучение дисциплины направлено на формирование следующих компетенций:

ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности;

ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

В результате изучения дисциплины студент должен:

знать:

- основные законодательные акты в области информационной безопасности;
- значение информации в жизни современного общества, понятие информационного общества, его основные признаки;

- источники и классификацию угроз безопасности компьютерной информации;

уметь:

- пользоваться нормативно-правовой и методической документацией по обеспечению информационной безопасности;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;
- составлять аналитические обзоры по вопросам обеспечения информационной безопасности;
- анализировать источники угроз безопасности компьютерной информации;

владеть:

- навыками работы с нормативно-правовыми и методическими документами;
- навыками анализа и систематизации технической информации;
- методами оценки информационных рисков.

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

№ модуля	№ недели	№ темы	Наименование темы	Часы				
				Всего	Лекции	Лаб. занятия	Практ занятия	СРС
10 семестр								
1	1-6	1	Основы информационной безопасности.	36	4			32
1	7-12	2	Основные угрозы безопасности компьютерной информации	84	4	8	2	70
1	13-18	3	Классификация видов, методов и средств защиты компьютерной информации	60	4	8	2	46
Всего				180	12	16	4	148

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	4	1,2	**Основы информационной безопасности.** Безопасность в информационном обществе. Информационная безопасность в системе национальной безопасности Российской Федерации. Цели, задачи, принципы и методы обеспечения информационной безопасности государства. Государственная система обеспечения информационной безопасности РФ.	2,3,7,12,16
2	4	3,4	**Основные угрозы безопасности компьютерной информации.** Каналы утечки информации ограниченного доступа. Методы несанкционированного доступа к конфиденциальной информации. Основные угрозы безопасности автоматизированных систем обработки информации.	1,2,3,4,6,16

3	4	5,6	**Классификация видов, методов и средств защиты компьютерной информации.** Виды защиты информации и сферы их действия. Общие способы защиты информации. Общая классификация средств защиты информации. Характеристика способов и средств по видам защиты информации.	1,2,3,4,5,6,16

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
Учебным планом не предусмотрены				

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	1	Обзор нормативно-правовых и методических документов в области информационной безопасности	3,12,13,16
2	2	2	Анализ защищенности объекта защиты информации	1,4,6,12,13,16

7. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
2,3	4	Исследование свойств и характеристик технических устройств скрытого получения информации	4,6,16
2,3	4	Методы инженерно-технической защиты информации. Подавление электроакустического канала утечки информации и предотвращение прослушивания телефонных линий.	4,6,16
2,3	4	Исследование технических характеристик и методов организации радиомониторинга при помощи поисково-разведывательного комплекса Р-375 «Кайра»	4,6,16
2,3	4	Техническое обеспечение и практика радиомониторинга	4,6,16

8. Задания для самостоятельной работы студентов

№ темы	Всего часов	Вопросы для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	4	Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.	2,7-15
1	4	Виды информации и основные методы ее защиты.	2,7-15
1	4	Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	
1	4	Виды угроз информационной безопасности Российской Федерации.	
1	4	Источники угроз информационной безопасности РФ.	
1	4	Анализ информационной инфраструктуры государства.	
1	4	Информационное оружие, его классификация и возможности.	1,2,3,7-15

1	4	Цели информационной войны в мирное и военное время. Объекты информационного воздействия в информационной войне	1,2,3,7-15
2	8	**Понятие защиты информации.** Базовые свойства безопасности информации. Понятие информации, защиты информации, информационной системы, безопасности автоматизированных систем обработки информации. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность.	2,3,7-15
2	8	**Санкционированный и несанкционированный доступ.** Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации.	2,7-15
2	8	**Понятие угрозы, уязвимости, риска.** Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Задача специалиста по информационной безопасности.	2,7-15
2	4	Материально-вещественный канал утечки информации.	1,4,6,8-15
2	4	Визуально-оптический канал утечки информации.	1,4,6,8-15
2	6	Вибро-акустический канал утечки информации.	1,4,6,8-15
2	8	Электромагнитный канал утечки информации.	1,4,6,8-15
2	8	Канал ПЭМИН.	1,4,6,8-15
3	8	**Понятие идентификации и аутентификации.** Понятие идентификации, идентификатора, авторизации, аутентификации. Определение и назначение подсистемы идентификации и аутентификации.	1,2,3,4,5,6,8-15
3	8	**Парольные системы идентификации и аутентификации пользователей** Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей.	1,2,3,4,5,6,8-15
3	8	Идентификация и аутентификация с использованием технических устройств.	1,2,3,4,5,6,8-15
3	4	Биометрическая аутентификация.	1,2,3,4,5,6,8-15
3	8	**Политики безопасности.** Принципы организации разноуровневого доступа в автоматизированных информационных системах. Понятие политики безопасности, цель создания политик безопасности. Классификация политик безопасности.	1,2,3,4,5,6,8-15
2	8	**Компьютерные вирусы как класс разрушающего программного воздействия.** Свойства вирусов, фазы исполнения вирусов, основные подходы к классификации компьютерных вирусов. Средства борьбы с компьютерными вирусами. Признаки заражения, виды проявлений компьютерных вирусов. Способы обнаружения заражения.	1,2,3,8-15
2	8	**Защита от разрушающих программных воздействий**. Общие и специализированные методы защиты программного обеспечения от разрушающих программных воздействий. Потенциально возможные злоумышленные действия.	1,2,3,8-15
3	10	**Принципы криптографической защиты информации.** Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем.	1,2,3,4,5,6,8-15

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [16].

10. Расчетно-графическая работа

Учебным планом не предусмотрена

11. Курсовая работа

Учебным планом не предусмотрена

12. Курсовой проект

Целью курсового проекта является практическое применение знаний и навыков, приобретенных в результате усвоения теоретической части курса, а также при выполнении практических и лабораторных работ.

Результатом выполнения курсового проекта является программа, реализующая стеганографическое скрытие информации либо криптографический алгоритм защиты информации.

В случае разработки студентом программы стеганографическоо скрытия информации контейнером для скрытия текстовой информации может быть видео-, аудио-, графические файлы формата avi, mp4, mp3, bmp и другие по согласованию с преподавателем. Внесение скрываемого текста может осуществляться как непосредственно в окно программы, так и загружаться в форматах doc, txt.

В случает разработки студентом программы криптографической защиты информации реализуется любой существующий криптографический алгоритм.

Отчет по курсовому проекту должен содержать теоретическую часть, описывающую, в зависимости от варианта курсового проекта, суть стеганографии, описание алгоритма стеганографического скрытия информации, либо суть криптографической защиты и реализуемый алгоритм; обоснование используемых средств разработки. К отчету в обязательном порядке прикладывается техническая документация, включающая в себя:

1. Техническое задание на курсовой проект
2. Руководство оператора
3. Руководство программиста
4. Программа и методика испытаний

При защите курсового проекта студент должен продемонстрировать работу программы, показать ее функционал, пояснить реализацию алгоритма в программном коде, пояснить теоретические основы реализуемого алгоритма с точки зрения обеспечения информационной безопасности.

Результаты защиты курсового проекта оцениваются «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценки «отлично» заслуживает студент, полностью выполнивший задание, показавшему глубокое и всестороннее знание теоретической части, а именно сути, алгоритмов, методов стеганографической и криптографической защиты информации;

использовавшему при разработке программы оригинальные и эффективные алгоритмы; грамотно оформившему программную документацию.

Оценки «хорошо» заслуживает студент, полностью выполнивший задание, показавшему знание теоретической части, а именно сути, алгоритмов, методов стеганографической и криптографической защиты информации; использовавшему при разработке программы оригинальные алгоритмы; грамотно оформившему программную документацию.

Оценки «удовлетворительно» заслуживает студент полностью выполнивший задание, однако, при защите обнаруживший пробелы в знаниях теоретической части, а именно сути, алгоритмов, методов стеганографической и криптографической защиты информации; допустивший ошибки при оформлении программной документации.

Оценка «неудовлетворительно» выставляется студенту, не выполнившему задание по курсовому проекту в полном объеме, не освоившему умения и навыки в рамках формируемых компетенций на достаточном уровне освоения.

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

В рамках изучения дисциплины формируются следующие компетенции: ОК-4, ОПК-5.

Карта компетенции ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: основные законодательные акты в области информационной безопасности.	Лекции Самостоятельная работа Практические занятия	Тестирование
Умеет: пользоваться нормативно-правовой и методической документацией по обеспечению информационной безопасности.	Практические занятия Лабораторные работы Курсовой проект Самостоятельная работа.	Тестирование Рефераты Защита курсового проекта
Владеет: навыками работы с нормативно-правовыми и методическими документами в области обеспечения информационной безопасности.	Лабораторные работы Практические занятия Курсовой проект Самостоятельная работа	Экзамен Защита курсового проекта

УРОВНИ ОСВОЕНИЯ КОМПЕТЕНЦИИ ОК-4

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	Знает: показывает достаточное для дальнейшей учебы и предстоящей работы по профессии знание основных законодательных актов в области информационной безопасности. Умеет: на достаточном уровне освоения умеет пользоваться нормативно-правовой и методической документацией по обеспечению информационной безопасности.

	Владеет: при выполнении заданий достаточном уровне освоения демонстрирует навыки работы с нормативно-правовыми документами.
Продвинутый (хорошо)	Знает: показывает полное знание основных законодательных актов в области информационной безопасности. Умеет: на хорошем уровне освоения демонстрирует умение пользоваться нормативно-правовой и методической документацией по обеспечению информационной безопасности. Владеет: при выполнении заданий показывает хорошее владение навыками работы с нормативно-правовыми документами.
Высокий (отлично)	Знает: показывает всестороннее, систематическое и глубокое знание основных законодательных актов в области информационной безопасности. Умеет: на высоком уровне освоения демонстрирует умение пользоваться нормативно-правовой и методической документацией по обеспечению информационной безопасности. Владеет: при выполнении заданий свободно владеет навыками работы с нормативно-правовыми документами.

Карта компетенции ОПК-5: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: значение информации в жизни современного общества, понятие информационного общества, его основные признаки; источники и классификацию угроз безопасности компьютерной информации.	Лекции Самостоятельная работа Практические занятия	Тестирование
Умеет: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; анализировать источники угроз безопасности компьютерной информации.	Практические занятия Лабораторные работы Курсовой проект Самостоятельная работа.	Тестирование Рефераты Защита курсового проекта
Владеет: навыками анализа и систематизации технической информации; методами оценки информационных рисков.	Лабораторные работы Практические занятия Курсовой проект Самостоятельная работа	Экзамен Защита курсового проекта

УРОВНИ ОСВОЕНИЯ КОМПЕТЕНЦИИ ОПК-5

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	Знает: показывает достаточное для дальнейшей учебы и предстоящей работы по профессии знание значения информации в жизни современного общества, понятия информационного общества, его основные признаков; источников и классификации угроз безопасности компьютерной информации. Умеет: на достаточном уровне освоения умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; анализировать источники угроз безопасности компьютерной информации. Владеет: на достаточном уровне освоения владеет навыками анализа и систематизации технической информации; методами оценки информационных рисков.
Продвинутый (хорошо)	Знает: показывает полное знание значения информации в жизни современного общества, понятия информационного общества, его основные признаков; источников и классификации угроз безопасности компьютерной информации. Умеет: на хорошем уровне освоения демонстрирует умение пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; анализировать источники угроз безопасности компьютерной информации. Владеет: при выполнении заданий показывает хорошее владение навыками анализа и систематизации технической информации; методами оценки информационных рисков.
Высокий (отлично)	Знает: показывает всестороннее, систематическое и глубокое знание значения информации в жизни современного общества, понятия информационного общества, его основные признаков; источников и классификации угроз безопасности компьютерной информации. Умеет: на высоком уровне освоения демонстрирует умение пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; анализировать источники угроз безопасности компьютерной информации. Владеет: при выполнении заданий свободно владеет навыками анализа и систематизации технической информации; методами оценки информационных рисков.

Формирование профессиональных компетенций по дисциплине производится на лабораторных, практических и лекционных занятиях, при выполнении курсового проекта (85%); закрепление достигается при сдаче экзамена (15%).

Вопросы для зачета

Учебным планом не предусмотрен.

Итоговое оценивание усвоения дисциплины осуществляется путем приема экзамена. Результаты экзамена оцениваются «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При выставлении экзаменационных оценок преподаватель руководствуется следующим:

- оценки «отлично» заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на высоком уровне освоения. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины и их значение для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

- оценки «хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе, продемонстрировавший умения и навыки в рамках формируемых компетенций на хорошем уровне освоения, способный к самостоятельному пополнению знания в ходе дальнейшей учебной работы и профессиональной деятельности;

- оценки «удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, освоившийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «удовлетворительно» выставляется студенту, допустившему неточность в ответе на экзамене;

- оценка «неудовлетворительно» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившего принципиальные ошибки в выполнении предусмотренных программой заданий, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Вопросы для экзамена

1. Понятие информационного общества, его основные признаки.
2. Основы государственной информационной политики, отраженные в Стратегии развития информационного общества в РФ.
3. Понятие национальной безопасности.
4. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
5. Виды защищаемой информации.
6. Роль информационной безопасности в обеспечении национальной безопасности государства.
7. Национальные интересы Российской Федерации в информационной сфере.
8. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
9. Угрозы информационной безопасности РФ.
10. Источники угроз информационной безопасности государства.
11. Задачи обеспечения информационной безопасности РФ.
12. Принципы обеспечения информационной безопасности РФ.
13. Методы обеспечения информационной безопасности РФ.
14. Информационная война как угроза национальной безопасности.
15. Концепция информационной войны.
16. Информационное оружие.
17. Назначение и функции системы обеспечения информационной безопасности РФ.
18. Организационная структура системы обеспечения информационной безопасности.
19. Система правового обеспечения информационной безопасности России.
20. Каналы утечки информации ограниченного доступа.
21. Методы несанкционированного доступа к конфиденциальной информации.
22. Компьютерная система как объект информационной защиты.
23. Основные угрозы безопасности автоматизированных систем обработки информации.
24. Виды защиты информации и сферы их действия.
25. Общие способы защиты информации.
26. Общая классификация средств защиты информации.
27. Характеристика способов и средств по видам защиты информации.

Тестовые задания по дисциплине

1 Вставьте пропущенное слово:
«Под информационной безопасностью будем понимать защищенность информации и …….. от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры

а) поддерживающей инфраструктуры
б) человека
в) конфиденциальных данных

2 Защита информации – это …

а) комплекс мероприятий, направленных на обеспечение информационной безопасности

б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

г) все определения корректны

3 Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:

а) обнаружение угроз
б) пресечения и локализация угроз
в) ликвидация угроз

4 Возможность за приемлемое время получить требуемую информационную услугу называется:

а) доступностью информации
б) целостностью информации
в) предоставлением информации

5 Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:

а) доступностью информации
б) целостностью информации
в) предоставлением информации
г) конфиденциальностью информации

6 Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера
какой-либо правительственной организации

а) доступность информации
б) целостность информации

в) предоставление информации
г) конфиденциальность информации

7 Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:

а) законодательного уровня
б) административного уровня
в) процедурного уровня
г) программно-технического уровня
д) программно-аппаратного уровня

9 Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:

а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации

10 Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:

а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
г) учетными записями пользователей

11 Потенциальная возможность определенным образом нарушить информационную безопасность – это ….

а) угроза
б) атака
в) взлом

12 Некоторая уникальная информация, позволяющая различать пользователей называется:

а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

13 Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:

а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

14 Совокупность идентификатора и пароля пользователя называется:

а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя

15 Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:

а) идентификацией пользователя
б) аутентификацией пользователя
в) опознанием пользователя
г) созданием учетной записи пользователя

16 Проверка принадлежности пользователю предъявленного им идентификатора является:

а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя
г) созданием учетной записи пользователя

17 Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) перехват передаваемой по сети информации (Sniffing)
д) спуфинг
е) сканирование портов

18 Атака, целью которой является трафик локальной сети, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

19 Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называе т-ся:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

20 Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

21 Разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ относится к:

а) правовым методам защиты информации
б) организационно-техническим методам защиты информации
в) организационно-распорядительным методам защиты информации
г) инженерно-технической защите

22 Контроль за выполнением специальных требований по защите информации относится к:

а) правовым методам защиты информации
б) организационно-техническим методам защиты информации
в) организационно-распорядительным методам защиты информации
г) экономическим методам защиты информации

23 Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

а) правовым методам защиты информации
б) организационно-техническим методам защиты информации
в) организационно-распорядительным методам защиты информации
г) экономическим методам защиты информации

24 Разработка программ обеспечения информационной безопасности РФ и определение порядка их финансирования относится к:

а) правовым методам защиты информации
б) организационно-техническим методам защиты информации
в) организационно-распорядительным методам защиты информации
г) нормативно-правовым методам защиты информации
д) экономическим методам защиты информации

25 Регулирование вопросов, связанных с защитой имущественных, авторских (неимущественных) и иных интересов собственников информации относят к:

а) правовым методам защиты информации
б) организационно-техническим методам защиты информации
в) организационно-распорядительным методам защиты информации
г) нормативно-правовым методам защиты информации
д) экономическим методам защиты информации

26 Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

а) собственник информации
б) владелец информации
в) пользователь

27 К какому виду конфиденциальной информации относится научно-техническая, технологическая, производственная, финансово-экономическая и иная деловая информация, в том числе информация о секретах производства?

а) коммерческая тайна
б) персональные данные

в) государственная служебная тайна
г) процессуальная тайна

28 К какому виду конфиденциальной информации относятся сведения, которые могут стать известными в ходе расследования преступлений и правонарушений, при проведении криминалистических экспертиз, при заслушивании дел в суде?

а) коммерческая тайна
б) персональные данные
в) государственная служебная тайна
г) процессуальная тайна

29 Особая категория информации, основной задачей защиты которой является охрана прав человека, который является создателем, называется:

а) коммерческая тайна
б) персональные данные
в) процессуальная тайна
г) авторское или патентное право

30 Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:

а) незаконного оборота информации
б) взлома информации
в) несанкционированного использования информации

31 Какое направление защиты в основном применяется для охраны материальных ценностей?

а) инженерно-техническая
б) организационно-техническая
в) организационно-распорядительная
г) нормативно-правовая
д) экономическая

32 Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

а) контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память

б) инфракрасный светодиод лазерного принтера, посылающий кратковременные

вспышки на электризованную поверхность фоточувствительного барабана

в) модулированный по силе тока поток электронов, засвечивающий в определенном порядке пиксели люминофора электронно-лучевой трубки

г) экран компьютерного монитора и глаза пользователя
д) оптический канал связи
е) все варианты могут быть отнесены к техническим каналам связи

33 Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

а) визуально-оптический канал
б) электромагнитный канал

в) виброакустический канал
г) материально-вещественный канал

34 Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

а) визуально-оптического канала
б) электромагнитного канала
в) виброакустического канала
г) материально-вещественного канала

35 Процесс разведки за объектами на территории другого государства с космических аппаратов является примером утечки информации:

а) визуально-оптического канала
б) электромагнитного канала
в) виброакустического канала
г) материально-вещественного канала

36 Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

а) визуально-оптический канал
б) электромагнитный канал
в) виброакустический канал
г) материально-вещественный канал

37 Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

а) визуально-оптического канала
б) электромагнитного канала
в) виброакустического канала
г) материально-вещественного канала

38 Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

а) визуально-оптический канал
б) электромагнитный канал
в) виброакустический канал
г) материально-вещественный канал

39 Примером какого канала утечки информации служит звук голоса человека?

а) визуально-оптического канала
б) электромагнитного канала
в) виброакустического канала
г) материально-вещественного канала

40 Выбрасывание на свалки отходов производства, низкая дисциплина при распечатке и размножении конфиденциальных документов, пренебрежение правилами учета, хранения и уничтожения вещественных носителей информации создают предпосылки для использования противником канала утечки информации …

а) визуально-оптического канала

б) электромагнитного канала
в) виброакустического канала
г) материально-вещественного канала

41 Установление подлинности идентифицированного пользователя – это ...
а) санкционирование
б) авторизация
в) аутентификация
г) идентификация

42 Процедура опознавания пользователя по предъявленному идентификатору – это …
а) санкционирование
б) авторизация
в) аутентификация
г) идентификация

43 Некое уникальное количество информации, позволяющее различать субъекты и объекты доступа – это …
а) идентификатор
б) пароль
в) учетная запись
г) регистрация

44 Процедура ввода идентифицирующей и аутентифицирующей информации с протоколированием действий – это …
а) идентификатор
б) пароль
в) учетная запись
г) регистрация

45 Из каких двух этапов состоит процедура распознавания личности?
а) регистрация
б) идентификация
в) аутентификация
г) реагирование

46 Какой из этапов распознавания личности проходит первым?
а) идентификация
б) аутентификация
в) авторизация

47 Парольная информация, известная только пользователю и проверяющей системе нужна пользователю для прохождения процедуры:
а) регистрации
б) идентификации
в) аутентификации
г) реагирования

48 Уникальный индивидуальный признак, свойственный лишь этому пользователю (голос, отпечаток пальца) нужен пользователю для прохождения процедуры:
а) регистрации
б) идентификации

в) аутентификации
г) реагирования

49 Самый хороший пароль становится плохим, если:
а) записать его где-нибудь в открытом месте
б) набирать его в присутствии посторонних
в) забыть его
г) все варианты подходят для того, чтобы испортить хороший пароль

50 Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?
а) 2
б) 3
в) 4
г) 5
д) 6

51 Сертификации подлежат:
а) средства криптографической защиты информации
б) средства выявления закладных устройств и программных закладок
в) защищенные технические средства обработки информации
г) защищенные информационные системы и комплексы телекоммуникаций
д) все вышеперечисленные средства

52 Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
а) просчеты при администрировании информационных систем
б) необходимость постоянной модификации информационных систем
в) сложность современных информационных систем

53 Уголовный кодекс РФ не предусматривает наказания за:
а) создание, использование и распространение вредоносных программ
б) ведение личной корреспонденции на производственной технической базе
в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

54 Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:
а) средства выявления злоумышленной активности
б) средства обеспечения отказоустойчивости
в) средства контроля эффективности защиты информации

55 Политика безопасности строится на основе:
а) общих представлений об ИС организации
б) изучения политик родственных организаций
в) анализа рисков

56 Действие Закона "О лицензировании отдельных видов деятельности" распространяется на:
а) деятельность по использованию шифровальных (криптографических) средств
б) деятельность по рекламированию шифровальных (криптографических) средств
в)деятельность по распространению шифровальных (криптографических) средств

57 Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

а) средства выявления злоумышленной активности

б) средства обеспечения отказоустойчивости

в) средства контроля эффективности защиты информации

58 Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:

а) деятельность по технической защите конфиденциальной информации

б) образовательную деятельность в области защиты информации

в) предоставление услуг в области шифрования информации

59 Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

а) средства выявления злоумышленной активности

б) средства обеспечения отказоустойчивости

в) средства контроля эффективности защиты информации

60 Что представляет собой Доктрина информационной безопасности РФ?

а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности

б) федеральный закон, регулирующий правоотношения в области информационной безопасности

в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации

61 Какие из перечисленных ниже угроз относятся к классу преднамеренных?

а) заражение компьютера вирусами

б) физическое разрушение системы в результате пожара

в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.)

г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации

д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств

е) вскрытие шифров криптозащиты информации

14. Образовательные технологии

С целью приведения учебного процесса в соответствие с требованиями ФГОС ВПО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий. Предусмотрено применение мультимедийных средств, обсуждение докладов студентов, дискуссии, тестирование, консультации.

15. Перечень учебно-методического обеспечения для обучающихся по дисциплине

1. Малюк А.А. Введение в информационную безопасность [Электронный ресурс]: учебное пособие/ Малюк А.А., Горбатов В.С., Королев В.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 288 с.— Режим доступа: http://www.iprbookshop.ru/11979

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430

3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677

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

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5. Рябко Б.Я. Криптографические методы защиты информации [Электронный ресурс]: учебное пособие/ Рябко Б.Я., Фионов А.Н.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 229 с.— Режим доступа: http://www.iprbookshop.ru/11994

6. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Креопалов В.В.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 с.— Режим доступа: http://www.iprbookshop.ru/10871

7. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс]: монография/ Куняев Н.Н.— Электрон. текстовые данные.— М.: Логос, 2010.— 348 с.— Режим доступа: http://www.iprbookshop.ru/9084

ПЕРИОДИЧЕСКИЕ ИЗДАНИЯ

8. Безопасность. Достоверность. Информация [Текст]: рос. журн. о безопасности бизнеса и личности. - СПб.: ООО "Журнал "БДИ", (2004-2012), №1-6.

9. Защита информации Inside [Текст]: информ.-метод. журн. - СПб. : ООО "Издательский Дом "Афина", (2003-2010), №1-6.

10.Научно-техническая информация. Сер.1. Организация и методика информационной работы [Текст]: науч.-техн. сб. - М.: ВИНИТИ РАН, 2009, №1-6. - ISSN 0548-0019

11.Научно-техническая информация. Сер. 2. Информационные процессы и системы [Текст]: науч.техн. сб. - М.: ВИНИТИ РАН, (2009-2012), №1-6. - ISSN 0548-0027

ИНТЕРНЕТ-РЕСУРСЫ

12. Сайт Федеральной службы по техническому и экспортному контролю ФСТЭК России http://www.fstec.ru (Дата обращения 01.07.2015)
13. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. http://www.securitylab.ru/ (Дата обращения 01.07.2015)
14. Anti-Malware – независимый информационно-аналитический центр, посвященный информационной безопасности http://www.anti-malware.ru/ (Дата обращения 01.07.2015)
15. Энциклопедия хакера. Взлом, защита от взлома, взлом email. http://www.inattack.ru/ (Дата обращения 01.07.2015)

ИСТОЧНИКИ ИОС

16. Узел дисциплины https://portal.sstu.ru/Fakult/FETIP/IBS/b314_1/default.aspx

16. Материально-техническое обеспечение дисциплины.

Для проведения лекционных занятий используется типовая лекционная аудитория со стандартным мультимедийным оснащением.

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:

- персональный компьютер (в конфигурации не хуже: процессор Intel Pentium или AMD 2 ГГц, 2 ОЗУ Гбайта, 320 Гбайт НЖМД);
- проектор (разрешение не менее 1024x768);
- экран для проектора.

Для проведения практических занятий и самостоятельной работы студентов используется компьютерный класс или учебная лаборатория каф. ИБС, оснащенная компьютерами.

Для проведения практических занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Intel Pentium или AMD 2 ГГц, ОЗУ 2 Гбайта, НЖМД 80 Гбайт. Компьютеры должны иметь подключение к локальной сети СГТУ и доступ к сети Интернет.

При проведении практических занятий в качестве инструментальных средств используется следующее программное обеспечение:

1. Операционные системы: Windows XP/7 в составе DreamsPark Premium MS ИНЭТМ.
2. Офисный пакет Microsoft Office Профессиональный плюс 2007 для подготовки и оформления отчетов.
3. ГАРАНТ аэро (Клиент)

При проведении лабораторных работ используется следующее оборудование:

1. Генератор GFG8210
2. Источник питания PPE-3323/RS
3. Анализатор спектра Agilent E4405B

4. Осциллограф DSO3102A
5. Прибор ГРОМ-ЗИ-4
6. Прибор ГРОМ-ЗИ-6
7. Ручной измеритель частоты РИЧ-3
8. Генератор HAMEG HM8135
9. Поисково-разведывательный комплекс Р375 «Кайра»
10. Поисково-разведывательный комплекс «Волна-К»
11. Приемник трехпрограммный СИБИРЯК 303
12. Имитатор СТС (беспроводное закладное устройство, лаб. стенд)
13. Телефонный аппарат
14. Радиоприемник бытовой