Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИСТЕТ»

В. В. Подтопельный

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности 10.05.03 " Информационная безопасность автоматизированных систем",
специализация «Безопасность открытых информационных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент

Доцент кафедры информационной безопасности института информационных технологий ФГБОУ ВО «Калининградский государственный технический университет» А. Г. Жестовский.

Подтопельный, В. В.
Программно-аппаратные средства защиты информации: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 42 с.

Учебное пособие включает в себя рассмотрение теоретических вопросов в области защиты информации по дисциплине «Программно-аппаратные средства защиты информации». В учебно-методическом пособии приведен тематический план изучения дисциплины. Представлены методические указания по изучению дисциплины. Даны рекомендации по подготовке к промежуточной аттестации в форме зачета и экзамена, и по выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины «Безопасность вычислительных сетей».

Пособие предназначено для студентов 4 – 5 курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей

Учебно-методическое пособие рассмотрено и одобрено в качестве электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину «Программно-аппаратные средства защиты информации».

Цель освоения дисциплины:

В результате освоения дисциплины ожидается, что студенты получат знания о принципах построения систем защиты информации (СЗИ) и их использования в операционных системах (ОС), способах эксплуатации программно-аппаратных средств защиты информации, поиска и деактивации вредоносных объектов в операционной среде.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Безопасность операционных систем.

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных/практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребует больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе Содержание дисциплины приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

В разделе «Балльно-рейтинговая система» приведен порядок применения балльно-рейтинговой системы контроля успеваемости.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение по Договору о сотрудничестве с ООО "Конфидент"

– СЗИ DALLAS LOCK 8.0-К. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"/лицензии:26 шт./ Дата: 01.11.2018 г. (срок действия: три года);

– СЗИ DALLAS LOCK 8.0-К. Сервер безопасности. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:1 шт./ Дата: 01.11.2018 г.(срок действия: три года);

– СЗИ DALLAS LOCK 8.0-С. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"/лицензии:26 шт./ Дата: 01.11.2018 г.(срок действия: три года)

– СЗИ DALLAS LOCK 8.0-С. Сервер безопасности. Договор о сотрудничестве №252-18-113/1 ООО "Конфидент"./лицензии:1 шт./ Дата: 01.11.2018 г.(срок действия: три года).

3.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года)

4.Антивирусная программа Kaspersky Total Space Security Russian Edition (госконтракт № 13/18АВ от 23.01.2018 г.);

5.Программное обеспечение распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU , по которой автор передаёт программное обеспечение в общественную собственность): IDS Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом), операционная система Linux, ПО Virtual Box, OpenVAS (средство сканирования защищенности компьютерных сетей).

6. Комплексная DLP система предотвращения утечек конфиденциальной информации Falcongaze SecureTower, перехват агентами (контроль: Mail; Web;Messengeres; FTP; Audit; Printers; Activity; Indexing) (25 лицензий)

- Лицензия на ПО Falcongaze SecureTower, сервер обработки данных (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, сервер контроля агентов (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, сервер перехвата данных (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, сервер ICAP (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, сервер распознавания изображений (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, сервер обработки почты (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, перехват сервером обработки почты(1 шт.)
- Лицензия на ПО Falcongaze SecureTower, сервер распознавания речи (1 шт.)
- Лицензия на ПО Falcongaze SecureTower, центр расследований (1 шт.)

Лицензионный договор №12/05/2018-1
от 05.12.2018 (1 год)
Типовое ПО на всех ПК:

1.Microsoft Desktop Education (операционные системы Microsoft Windows Desktop operating system, офисные приложения Microsoft Office, по соглашению V9002148 Open Value Subscription). Дата заключения контракта 05.07.2018. Номер контракта 0335100016118000073-0484577-02.

2.Антивирусное программное обеспечение Kaspersky Total Space Security Russian Edition, лицензия 17EO-171225-104659-470-270, срок использования с 2017-12-26 до 2020-03-13.

Специализированное ПО:

1. Программное обеспечение виртуализации VMWare Workstation, (по государственному контракту №10/13А от 19 апреля 2013 года), (на 2 компьютера – Vmware License Purchase Information № 22033811OB);

2. Средство защиты информации (СЗИ) от несанкционированного доступа (НСД) Страж NT (версия 3.0) по государственному контракту № 10\13А от 19 апреля 2013 г. (2 шт.);

3. Программно-аппаратный комплекс защиты информации: комплексная система защиты информации (КСЗИ) «Панцирь-С», включает криптографический модуль по государственному контракту № 10\13А от 19 апреля 2013 г. (1 шт.).

2. ТЕМАТИЧЕСКИЙ ПЛАН

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции (8-й семестр - 34 ч ауд.)		
1.1	Методы защиты ПО	Тема 1.1 Введение. Основные понятия.	4	
1.2	Методы защиты ПО	Тема 1.2 Методы защиты ПО	4	18
1.3	Методы защиты ПО	Тема 1.3 Подсистемы и модулей системы защиты ПО от несанкционированного использования.	4	12
1.4	Методы защиты ПО	Тема 1.4 Методы и средства обратного проектирования.	4	
1.5	Методы защиты ПО	Тема 1.5 Методы противодействия обратному проектированию.	4	
1.6	Методы защиты ПО	Тема 1.6 Общие методы защиты программ	4	20
1.7	Методы защиты ПО	Тема 1.7 Идентификация и аутентификация с использованием технических устройств.	4	
2.1	Защита от разрушающих программных воздействий.	Тема 2.1 Защита от разрушающих программных воздействий.	4	
2.2	Защита от разрушающих программных воздействий.	Тема 2.2 Классификация компьютерных вирусов	2	23,85
		Лекции (9-й семестр -34 ч ауд.)		
2.3	Защита от разрушающих программных воздействий.	Тема 2.3 Программные закладки	4	

2.4	Защита от разрушающих программных воздействий.	Тема 2.4 Особенности функционирования троянских программ.	4	20
3.1	Системы защиты информации	Тема 3.1 Особенности систем защиты информации	4	
3.2	Системы защиты информации	Тема 3.2 Контроль целостности	4	
3.3	Системы защиты информации	Тема 3.3 Подсистема управления доступом.	4	
3.4	Системы защиты информации	Тема 3.4 Подсистема регистрации	4	
3.5	Системы защиты информации	Тема 3.5 Криптографическая подсистема СЗИ	4	20
3.6	Системы защиты информации	Тема 3.6 Гарантирование уничтожение.	4	
3.7	Системы защиты информации	Тема 3.7 Системы активного аудита и АПКШ	2	21
			68	**134,85**

		Лабораторные занятия (8-й семестр)		
1.	Методы защиты ПО	Проверка работоспособности средств защиты компьютера от вирусов	2	-
2.	Методы защиты ПО	Защита информации с помощью пароля	8	-
3.	Методы защиты ПО	Программирование под HASP с использованием API-функций	4	-
4.	Методы защиты ПО	Изучение функций программы отслеживании обращений к	4	-

		файловой системе		
5.	Методы защиты ПО	Исследование моделей защит ПО. Защита от дизассемблеров	4	-
6.	Методы защиты ПО	Исследование моделей защит ПО. Изучение средств динамического исследования программ на примере отладчика. Защита от отладчиков	6	-
7.	Защита от разрушающих программных воздействий.	Определение жизненно цикла вредоносных программ и извлечение компьютерного вируса средствами антивирусных программ и утилит. Исследование особенностей внедрения вредоносных программного обеспечения	6	-
Всего за семестр:			34	
Лабораторные занятия (9-й семестр)				
1.	Защита от разрушающих программных воздействий.	Определение специфики работы вредоносного программного обеспечения	4	-
2.	Защита от разрушающих программных воздействий.	Обнаружение и извлечение вредоносного программного обеспечения помощью антивирусных программ и утилит	8	-
3.	Системы защиты информации	Изучение функций СЗИ. Подсистема управления доступом. Разграничение доступа	8	-
4.	Системы защиты информации	Организация контроля и построение изолированной программной среды средствами СЗИ. Контроль целостности и регистрация событий СЗИ. Идентификация и аутентификация субъекта доступа в СЗИ	6	-
5.	Системы защиты информации	Работа с системой анализа защищенности. Применение программ аудита	6	-
6.	Системы защиты информации	Использование резервирования	2	-

		Всего за семестр:	**34**	
		Курсовой проект		
2.1	Название первого раздела	Контрольная точка 1. Раздел проекта 1	-	-
3.1	Название третьего раздела	Контрольная точка 2. Раздел проекта 2	-	-
		Оформление проекта. Защита	42,75	-
			42,75	**0**
		Рубежный (текущий) и итоговый контроль		
2.1	Название второго раздела	Контроль 1 (не предусмотрен)	-	-
3.1	Название третьего раздела	Контроль 2 (не предусмотрен)	-	-
		Итоговый контроль (зачет)		
		Итоговый контроль (экзамен)		
			0	**0**
		Всего	**40**	**32**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1. Раздел 1. Методы защиты ПО

3.1.1. Тема 1.1 Введение. Основные понятия.

Перечень изучаемых вопросов:

Уязвимость компьютерных систем.

Классификация программных средств защиты.

Механизмы защиты.

Проблема защиты программного обеспечения от несанкционированного использования.

Методические указания к изучению:

Предварительно требуется определить понятие уязвимости. Рассмотреть классификации уязвимостей по областям, по типам и тп. Требуется рассмотреть стандарт (ГОСТ) по классификациям уязвимостей.

Предварительно требуется определить понятие средство защиты. Рассмотреть классификации средств защиты по областям, по типам и т. п. Требуется рассмотреть руководящие документы по классификациям средств, механизмов и систем защиты.

Рассмотреть проблемы полного и неполного перекрытия угроз средствами защиты информации.

При работе над курсовым проектом обратите внимание на:

- описание уязвимостей, которые требуется приводить в первой (теоретической) главе.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Приведите классификацию уязвимостей компьютерных систем.
2. Приведите классификации программных средств защиты.

3. Охарактеризуйте проблема защиты современного программного обеспечения от несанкционированного использования.

3.1.2. Тема 1.2 Методы защиты ПО

Перечень изучаемых вопросов:

Методы защиты ПО от несанкционированного использования.

Модульная архитектура технических средств защиты ПО от несанкционированного использования.

Методические указания к изучению:

Требуется обратить внимание на архитектуру технических средств защиты ПО от несанкционированного использования, средства, способы защиты ПО от несанкционированного использования.

Система защиты ПО от несанкционированного использования состоит из двух основных частей:

1. Подсистемы внедрения механизмов системы защиты;
2. Внедряемого защитного кода.

Основными требованиями к системе защиты ПО от несанкционированного использования являются следующие:

- система защиты должна выявлять факт несанкционированного запуска программы;
- система защиты должна реагировать на факт несанкционированного запуска программы;
- система защиты должна противостоять возможным атакам злоумышленников, направленных на нейтрализацию системы защиты.

Литература:

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

4. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Охарактеризуйте методы защиты ПО от несанкционированного использования.
2. Охарактеризуйте модульную архитектуру технических средств защиты ПО от несанкционированного использования.

3.1.3 Тема 1.3 Подсистемы и модулей системы защиты ПО от несанкционированного использования

Перечень изучаемых вопросов:

Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования.

Электронные ключи.

Модель защиты структурным кодом

Методические указания к изучению:

Требуется обратить внимание на связь подсистем и модулей системы защиты ПО от несанкционированного использования, типы, архитектуру электронных ключей, способы, позитивные и негативные факторы защиты структурным кодом.

Базовой основой ключей HASP является специализированная заказная микросхема (ASIC – Application Specific Integrated Circuit), имеющая уникальный для каждого ключа алгоритм работы. В процессе своего исполнения защищенная программа опрашивает подключенный к ПК HASP. Если HASP возвращает правильные ответы, работает по требуемому алгоритму и обладает требуемыми эталонными характеристиками, то программа выполняется нормально.

Существует два способа внедрения защитных механизмов в ПО с помощью электронных ключей HASP.

1. HASP API – с помощью API функций.
2. Пакетный режим (HASP Envelope).

Защита структурным кодом (Pattern Code Security – PCS) является средством, значительно повышающим защищенность приложения, защищаемого с помощью электронных ключей HASP.

PCS реализуется в процессе защиты с помощью HASP API. Использование PCS возможно лишь при наличии доступа к исходным текстам защищаемого приложения.

PCS осуществляет последовательность скрытых вызовов процедуры hasp(), не включая эти вызовы в исходный код явно. После каждого вызова процедуры hasp() происходит переключение на следующий скрытый вызов. Если вызов hasp() вдруг удален из защищенной программы, скрытые вызовы не выполняются, а это означает, что кто-то вмешался в работу программы. Тем самым, PCS не дает удалить либо «заклеить» обращения к процедуре hasp().

Преимуществами использования PCS являются:

- скрывание обращения к HASP;
- трассировка вызовов hasp() для шаблонов практически невозможна, так как их нет в исходном коде;

- легче обнаруживается вмешательство извне (если процедуру отключили); если вызов hasp() будет удален, то шаблоны не обновятся, а это значит – кто-то вмешался в работу приложения;
- PCS препятствует эмуляции процедуре hasp().

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.
2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования.
2. Электронные ключи.
3. Модель защиты структурным кодом

3.1.4 Тема 1.4 Методы и средства обратного проектирования.

Перечень изучаемых вопросов:

Методы обратного проектирования.

Средства обратного проектирования.

Классификация и особенности методов и средств атаки на средства защиты программного обеспечения

Наиболее распространенные способы, используемые злоумышленником при реализации первой либо второй угрозы – использование специализированных средств исследования работы программ, а также их кода.

Существует несколько задач, которые злоумышленник должен решить при реализации данных угроз.

1. Задача обнаружения в коде программы модуля защиты. Следует отметить, что без использования специализированных программных средств эта задача в принципе не решаема за приемлемое время. Это обусловлено следующими обстоятельствами.

2. Задача исследования модуля защиты и понимания принципов его действия. Злоумышленник должен понять, каким образом построена защита, где она хранит (если хранит) ключевую информацию, где сохраняет (если сохраняет) свои метки и ключи, на каком этапе принимается решение о регистрации программы, либо об отклонении регистрации.

Специфика атак на модули проверки корректности ключевой информации

Для вскрытия данного типа защит в первую очередь необходимо найти в коде программы код модуля защиты и, а в нем – процедуру данной проверки.

Специфика атак на модули проверки истечения временного срока работы программы или ограничения по количеству ее запусков

Взлом данных модулей во многом практически аналогичен взлому модулей проверки корректности ключевой информации. Специфика взлома здесь состоит в том, что у данных модулей появляются дополнительные уязвимости, которые могут быть использованы злоумышленником.

Отлов злоумышленником вызова WinAPI функций при взломе ПО

Одна из основных задач, которую необходимо решить злоумышленнику при реализации взлома – локализовать модуль защиты в коде программы. Грубая локализация данного модуля решается без существенных затрат с помощью современных средств отладки программного обеспечения. В случае взлома Windows – приложения данная задача решается практически мгновенно путем отслеживания вызовов WinAPI функций, используемых разработчиком.

Средства мониторинга событий - утилиты, отслеживающие операции, производимые программным обеспечением над файлами, реестром, портами, а также отслеживающие потоки системных сообщений.

Методические указания к изучению:

Требуется обратить внимание на:

Методы обратного проектирования, средства обратного проектирования и средства атаки на средства защиты программного обеспечения

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Привести методы обратного проектирования.
2. Охарактеризовать средства обратного проектирования.
3. Привести классификацию и особенности методов и средств атаки на средства защиты программного обеспечения

3.1.5 Тема 1.5 Методы противодействия обратному проектированию.

Перечень изучаемых вопросов:

Методы противодействия отладчикам защищенного режима.

Методы противодействия отладчикам реального режима.

Методические указания к изучению:

Рассмотреть трики противодействия отладчикам защищенного режима.

Рассмотреть трики противодействия отладчикам реального режима.

Для вычисления файлов, в которых модуль защиты хранит для себя служебную, ключевую информацию, цифровые подписи, и т. д.

Для вычисления секретных недокументируемых файлов, в которых модуль защиты хранит конфиденциальную информацию. Такие файлы иногда используются в слабых программных защитах и, как правило, хранятся во временных либо системных папках.

Для вычисления тех файлов, в которые модуль защиты записывает информацию при установке ПО. Как правило, это бывает необходимо для снятия защит, ограничивающих функционирование во времени использования.

Для вычисления записей в системном реестре Windows, в которых модуль защиты сохраняет служебную информацию при регистрации.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Охарактеризуйте методы противодействия отладчикам защищенного режима.

2. Охарактеризуйте методы противодействия отладчикам реального режима.

3.1.6 Тема 1.6 Общие методы защиты программ

Перечень изучаемых вопросов:

Методы противодействия дизассемблированию программного обеспечения.

Общие методы защиты программ от отладки и дизассемблирования

Выделяют несколько общих подходов к защите ПО от дизассемблирования.

1. Шифрование кода. Защищаемый участок кода шифруется каким-либо алгоритмом, а в программу добавляется модуль расшифровки, который в нужный момент расшифровывает его и передает ему управление. В данном случае, защищаемый участок кода перед дизассемблером предстанет в зашифрованном виде, и будет воспринят дизассемблером неверно.

2. Самомодификация кода программой.

3. Различные ходы, приводящие к обману дизассемблера. Этот способ заключается в том, чтобы с помощью различных «хитрых» ходов запутать дизассемблер, подсунув данные вместо кода, или дезориентировать его логику, повести его по ложному следу. В качестве примеров такой защиты можно привести следующие участки кода.

4. Сокрытие команд передачи управления.

Сокрытие команд передачи управления приводит к тому, что дизассемблер не может построить граф передачи управления. Например, можно модифицировать адреса переходов в ходе выполнения программы (только для реального режима).

5. Использование методики косвенной передачи управления также затрудняет анализ дизассемблированного кода.

6. Использование нестандартных способов передачи управления.

Методы фактора внимания, сокрытие команд передачи управления и метод косвенной передачи, применяемой при противодействии.

Особенности динамического исследования. Метод чёрного ящика, маяков, step-trace.

Метод черного ящика:

1) Возможность отслеживания зависимостей на уровне бинарного кода(модификация отдельных байт в заголовках бинарного кода)

2) Исследование функционала криптозащиты:

1. Выявление марканта(случайная последовательность символов) в криптосистеме.

2. Зависимости марканта.

3. Выявление типа криптографического преобразования и т. д.

Метод маяков:

Маяки – это точки программы, действия которых ясны без знания контекста (вызовы динамических библиотек).

1) Все точки останова на все маяки.

2) Установка точки останова на обработки, соответствующие системным вызовам .

Метод step-trace 1-го этапа:

Используется для поиска функций безопасности с учетом внешних проявлений

Метод step-trace 2-го этапа:

Предполагает пошаговый проход от точки останова или маяка при step-trace 1-го этапа

Несмотря на то, что конкретные реализации данных типов защит, зачастую, значительно различаются, можно выделить несколько общих подходов, используемых как в первом, так и во втором типе. Данные подходы представлены ниже.

1. Использование триков (ловушек), с помощью которых можно выявить наличие отладчика в оперативной памяти, и, соответственно, прекратить работу, либо затруднить процесс отладки.

2. Определение наличия отладчика в оперативной памяти используя различные «дырки», допущенные при реализации отладчиков либо внедренные разработчиком отладчика принудительно.

Использование недокументированных команд и возможностей процессора.

Использование того, что некоторые отладчики при загрузке отлаживаемой программы не могут полностью эмулировать «чистую» среду ее запуска в ОС (например, обнуляют некоторые регистры, которые могут нести определенный смысл).

Рассмотрим более подробно реализации защит против отладчиков реального и защищенного режимов.

Особенностью отладчиков защищенного режима является возможность их полной изоляции от выполняемой программы. В связи с этим задача обнаружения отладчика в памяти стандартными средствами значительно усложняется.

Кроме этого, особенностью защищенного режима является введение специализированных отладочных регистров DR0 – DR7, предназначенных для отладочных целей (таких как установка точек останова на обращение к определенным адресам памяти и портам).

Наиболее предпочтительным способом защиты ПО от отладки и дизассемблирования является способ, основанный на шифровании кода программы на некотором секретном ключе. При этом предъявляется требование того, чтобы секретность ключа не могла быть нарушена путем исследования кода программы и дискового пространства ПК.

Методические указания к изучению:

Рассмотрите специфику методы противодействия дизассемблированию программного обеспечения, как статическому методу исследования.

Рассмотрите общие методы защиты программ от отладки и дизассемблирования

Литература:

1.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2.Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Приведите специфику методы противодействия дизассемблированию программного обеспечения, как статическому методу исследования.
2. Приведите общие методы защиты программ от отладки и дизассемблирования.

3.1.7 Тема 1.7 Идентификация и аутентификация с использованием технических устройств.

Перечень изучаемых вопросов:

Идентификация и аутентификация пользователей с использованием технических устройств.

Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

Методические указания к изучению:

Обратите внимание на использование технических устройств.

Обратите внимание на то каким образом производится идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

При идентификации/аутентификации пользователей с использованием физических устройств, в качестве пользовательского идентификатора используется некоторое техническое устройство, содержащее уникальный идентификационный номер, используемый для решения задач идентификации владельца, а в отдельных случаях и секретную аутентифицирующую информацию, ограничивающую доступ к устройству. Широко распространенными техническими устройствами, используемыми для решения задач идентификации/аутентификации являются:

- идентификаторы iButton (Touch Memory);
- бесконтактные радиочастотные карты proximity;
- пластиковые карты;
- ключи e-Token.

В качестве биометрических характеристик, которые могут быть использованы при аутентификации субъекта доступа, достаточно часто применяют следующие:

1. отпечатки пальцев;
2. геометрическая форма рук;
3. узор радужной оболочки и сетчатки глаз;
4. форма и размеры лица;
5. особенности голоса;
6. биомеханические характеристики почерка;
7. биомеханические характеристики «клавиатурного почерка».

Особенностью применения биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем И/АУ являются следующие:

1. Необходимость обучения биометрической системы для конкретных пользователей, зачастую, достаточно длительного.
2. Возможность ошибочных отказов и ошибочных подтверждений при аутентификации пользователей.
3. Необходимость использования специальных технических устройств для чтения биометрических характеристик, как правило, достаточно дорогостоящих (за исключением, быть может, аутентификации по клавиатурному подчерку).

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.
2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Охарактеризуйте идентификацию и аутентификацию пользователей с использованием технических устройств.
2. Охарактеризуйте идентификацию и аутентификацию с использованием индивидуальных биометрических характеристик пользователя

3.2. Раздел 2. Защита от разрушающих программных воздействий.

3.2.1. Тема 2.1 Защита от разрушающих программных воздействий.

3.2.2. Перечень изучаемых вопросов:

Модели взаимодействия прикладной программы и РПВ.

Компьютерные вирусы как класс РПВ. Защита от РПВ.

Изолированная программная среда.

Методические указания к изучению:

Рассмотреть модели взаимодействия прикладной программы и РПВ.

Рассмотреть компьютерные вирусы как класс РПВ. Защита от РПВ.

Рассмотреть изолированную программную среду.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Охарактеризуйте модели взаимодействия прикладной программы и РПВ.
2. Охарактеризуйте компьютерные вирусы как класс РПВ. Защита от РПВ
3. Поясните принципы построения изолированной программная среда.

3.2.2 Тема 2.2 Классификация компьютерных вирусов

Перечень изучаемых вопросов:

Типы вредоносных программ

Типы классификаций вирусных программ

Методические указания к изучению:

Рассмотреть различные типологии вирусных и вредоносных программ.

Исследовать методические документы ФСЭК с указанием типа вредоносных программ

Литература:

1.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2.Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Привести типы вредоносных программ
2. Привести типы классификаций вирусных программ

3.2.3 Тема 2.3 Программные закладки

Перечень изучаемых вопросов:

Программные закладки, пути их внедрения, методы их выявления.

Жизненный цикл вредоносных программ.

Структура компьютерных вирусов.

Методические указания к изучению:

Рассмотреть отличия программных закладок от вредоносных программ, пути их внедрения, методы их выявления.

Рассмотреть отличия жизненных циклов вредоносных программ.

Рассмотреть типовую структуру компьютерных вирусов.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Привести программные закладки, пути их внедрения, методы их выявления.
2. Привести жизненный цикл вредоносных программ.

3. Привести структура компьютерных вирусов.

3.2.4 Тема 2.4 Особенности функционирования троянских программ

Перечень изучаемых вопросов:

Особенности функционирования троянских программ.

Методики распознавания и извлечения вредоносных программ.

Классификация методов и средств борьбы с компьютерными вирусами.

Методические указания к изучению:

Рассмотреть особенности функционирования троянских программ в режимах ядро и пользовательском режиме.

Рассмотреть методики распознавания и извлечения вредоносных программ: сигнатурный, поведенческий, эвристический анализы.

Рассмотреть классификацию методов и средств борьбы с компьютерными вирусами; способы извлечения вирусов из ОС.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Привести особенности функционирования троянских программ.
2. Указать и охарактеризовать методики распознавания и извлечения вредоносных программ.
3. Привести классификацию методов и средств борьбы с компьютерными вирусами.

3.3. Раздел 3. Системы защиты информации

3.3.1 Тема 3.1 Особенности систем защиты информации

Перечень изучаемых вопросов:

Особенности организации и функционирования систем защиты информации (СЗИ).

Идентификация и аутентификация пользователей СЗИ.

Методические указания к изучению:

Особенности организации и функционирования систем защиты информации (СЗИ).

Идентификация и аутентификация пользователей СЗИ.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Особенности организации и функционирования систем защиты информации (СЗИ).

2. Идентификация и аутентификация пользователей СЗИ.

3.3.2 Тема 3.2 Контроль целостности

Перечень изучаемых вопросов:

Контроль целостности и системные вопросы защиты программ и данных

Использование СЗИ для контроля целостности.

Организация контроля.

Методические указания к изучению:

Определить специфику процедур контроля целостности и системные вопросы защиты программ и данных

Рассмотреть использование СЗИ для контроля целостности.

Обратить внимание на прядки организация контроля.

Функциональный контроль предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 6 загружены и функционируют. Функциональный контроль осуществляется перед входом пользователя в систему.

При функциональном контроле проверяется наличие в системе и работоспособность следующих компонентов:

- ядро;
- модуль входа в систему;

- криптоядро;
- модуль репликации;
- подсистема контроля целостности;
- подсистема аппаратной поддержки.
- В случае нарушении функциональной целостности:
- В журнале регистрируется факт нарушения. Это возможно при условии работоспособности ядра.

Администратор информируется об ошибочном завершении функционального контроля.

Вход в систему разрешается только пользователям, входящим в локальную группу администраторов компьютера.

Запуск функционального контроля инициирует модуль входа в систему. При обнаружении нарушений этот модуль управляет административным входом пользователя в систему. Кроме того, он информирует администратора об ошибках контроля.

Если нарушен и сам модуль входа в систему, то при входе пользователя в систему функциональный контроль проводит модуль репликации. Он проверяет, был ли выполнен функциональный контроль, и если нет — инициирует его выполнение.

Процесс инициализации КЦ представляет собой процесс формирования и сохранения списка объектов, подлежащих контролю подсистемой КЦ.

За формирование списка объектов файловой системы (ФС) отвечает приложение для операционных систем Microsoft Windows XP/2003/Vista/2008/7/2008R2 (x86/x64), Linux выполняющее следующие функции:

1. Формирование списка файлов для КЦ;
2. Вычисление контрольных сумм для файлов и секторов HDD, подлежащих КЦ;
3. Формирование объекта (файла), содержащего список объектов контроля и контрольные суммы.

Функции подсистемы обеспечения целостности:

– должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды, при этом:

– целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ,

– целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

– должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

– должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

– должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Каков контроль целостности программ и данных
2. Чем определяется специфика использования СЗИ для контроля целостности.

3.3.3 Тема 3.3 Подсистема управления доступом.

Перечень изучаемых вопросов:

Разграничение доступа.

Управление политикой безопасности.

Методические указания к изучению:

Рассмотреть разграничение доступа мандатного типа.

Рассмотреть разграничение доступа дискреционного типа.

Определить специфику управления политикой безопасности МБ, МБС, МО.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специально-

сти 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Привести правила разграничения доступа.
2. Описать механизм управления политикой безопасности МБ, МБС, МО

3.3.4 Тема 3.4 Подсистема регистрации

Перечень изучаемых вопросов:

Рассмотреть особенности подсистема регистрации и учета централизованного и децентрализованного типа.

Рассмотреть особенности Регистрация и учет событий защищаемой среды.

Методические указания к изучению:

Привести особенности подсистемы регистрации и учета.

Привести особенности регистрации и учет событий защищаемой среды.

Литература:

1.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2.Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Укажите особенности подсистемы регистрации и учета.
2. Приведите особенности Регистрация и учет событий защищаемой среды.

3.3.5 Тема 3.5 Криптографическая подсистема СЗИ.

Перечень изучаемых вопросов:

Особенности криптографических подсистем СЗИ.

Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.

Методические указания к изучению:

Рассмотреть виды криптографических подсистем СЗИ.

Рассмотреть шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Привести особенности криптографических подсистем СЗИ.
2. Привести шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах

3.3.6 Тема 3.6 Гарантирование уничтожение.

Перечень изучаемых вопросов:

Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ

Очистка (обнуление, обезличивание) внешних накопителей

Методические указания к изучению:

Рассмотреть процедуры обнуления, обезличивания освобождаемых областей оперативной памяти ЭВМ

Рассмотреть процедуры очистки (обнуление, обезличивание) внешних накопителей

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.
2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных си-

стем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Приведите способы очистки (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ.
2. Приведите способы очистки (обнуление, обезличивание) внешних накопителей.

3.3.7 Тема 3.7 Системы активного аудита и АПКШ

Перечень изучаемых вопросов:

Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.

Аппаратно-программные комплексы шифрования.

Аудит ИБ АИС.

Методические указания к изучению:

Рассмотрите программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях с использованием средств фильтрации и маршрутизации, аппаратно-программные комплексы шифрования.

Литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.
2. Подтопельный, В.В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» (в 4-х частях)/ В.В. Подтопельный – Калининград: Изд-во БГАРФ. – 2020. – 102 с.

Контрольные вопросы:

1. Укажите специфику программно-аппаратных средствх обеспечения информационной безопасности в вычислительных сетях.
2. Укажите специфику аппаратно-программные комплексы шифрования.
3. Приведите специфику аудит ИБ АИС.

4. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1. Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации:

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная либо балльно-рейтинговая..

Выбрана традиционная зачетно-экзаменационная методика оценивания знаний

Предусматриваются: зачет, экзамен, курсовой проект

4.2. Порядок применения рейтинговой системы (не предусматривается)

В рамках балльно-рейтинговой системы выставляется оценка за качество выполнения и защиту лабораторных и контрольных работ.

Таблица 1. Шкала оценок уровня усвоения материала обучающимся

Вид деятельности	Доля	Кол-во ед.	Макс. балл за ед.	Всего
Обязательные виды деятельности				
1-й семестр				
Посещаемость занятий	20 %	N1	=200/N1	200
Выполнение лаб. работ (защита)	40 %	2	200	400
Контрольная работа 1	40 %	1	400	400
Итого:	100%			1000
2-й семестр				
Посещаемость занятий	20 %	N2	=200/N2	200
Выполнение лаб. работ (защита)	40 %	2	200	400
Контрольная работа 2	40 %	1	400	400
Итого:	100%			1000
Всего				2000
Дополнительные задания (по выбору студента в каждом семестре)				
Подготовка реферата (видео-доклада)	20 %		200	200
Решение дополнительных задач контрольной работы	10 %		100	100
Выполнение задания в рамках НИРС	50 %		500	500

4.3 Условия получения положительной оценки

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой:

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя:

- материалы для проведения текущего контроля успеваемости – варианты заданий;
- перечень компетенций и их элементов, проверяемых на каждом мероприятии текущего контроля успеваемости;
- систему и критерии оценивания по каждому виду текущего контроля успеваемости
- описание процедуры оценивания.

Текущий контроль в форме опроса.

Текущий контроль осуществляется путем опроса по материалу, пройденному на предшествующих лекциях.

Оценивается:

- полнота усвоения пройденного материала,
- качество изложения пройденного материала (устно и письменно)

Таблица 2. Шкала оценок уровня усвоения материала обучающимся

Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не может ответить на вопросы по пройденному материалу или графически изобразить на доске	Отвечает сбивчиво, путается в определениях и обозначениях, нуждается в помощи других обучающихся	Допускает незначительные ошибки при изложении пройденного материала, не полностью представляет связи между разделами изучаемой дисциплины	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изученных разделов дисциплины

Таблица 3. Шкала оценок уровня освоения дисциплины по зачету

Оценка			
Неудовлетворитель-	Пороговый	Углубленный	Продвинутый

ный			
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Правильные ответы даны менее чем на 50% включительно. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи	Правильные ответы даны на 51-64% вопросов. Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи	Правильные ответы даны на 65-94% вопросов. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи	Правильные ответы даны на 95-100% вопросов. Ответы на поставленные в билете вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания предмета. Соблюдаются нормы литературной речи

Таблица 4. Шкала оценок уровня освоения дисциплины по экзамену.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические за-	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает по-	Твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, мо-	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически строй-

дания, задачи.	следовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.	жет правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий	но его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок

Таблица 5. Шкала оценок уровня освоения дисциплины по тесту

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Менее 50 % правильных ответов	50-70 % правильных ответов	71-90% правильных ответов	91-100 % правильных ответов

Таблица 6. Шкала оценок курсового проекта

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Работа носит реферативный характер, студент допускает существенные ошибки при защите, с больши-	Работа носит реферативный характер, допускает неточности, недостаточно правильные формулировки,	В работе углублены теоретические и практические знания, материал излагается грамотно и по существу, не допус-	В процессе выполнения работы приобретены навыки самостоятельного планирования и выполнения научно-

ми затруднениями отвечает на вопросы, оформление работы не соответствует правилам	нарушает последовательность в изложении при защите, оформление работы имеет незначительные отклонения от правил	кается существенных неточностей в ответе на вопрос, оформление работы соответствует правилам	исследовательской работы; получен опыт сбора и обработки исходного материала, анализа научно-технической литературы, материал излагается грамотно оформление работы соответствует правилам

Критерии оценивания для проведения итоговой аттестации

Итоговая аттестация обучающихся проводится **в форме зачета (8-й семестр) и экзамена (9-й семестр)**.

Допуск к итоговой аттестации возможен при:

- всех выполненных, сданных (проверенных, защищенных) лабораторных работах, наличии отчётов по ним;
- наличии показателей приемлемого уровня освоения материалов курса: более 50% посещений от общего числа требуемых по учебному плану.

Критерии оценивания:

- уровень усвоения материала, предусмотренного программой
- умение выполнять задания, предусмотренные программой
- уровень знакомства с дополнительной литературой
- уровень раскрытия причинно-следственных связей
- уровень раскрытия междисциплинарных связей
- стиль поведения (культура речи, манера общения, убежденность, готовность к дискуссии)
- качество ответа (полнота, правильность, аргументированность, его общая композиция, логичность)

4.4 Примерные вопросы к зачету/экзамену по дисциплине

4.4.1 Вопросы к зачету:

1. Надежность информации.
2. Интегральная информационная безопасность.
3. Основные этапы жизненного цикла информации.
4. Элементы информационной базы АСОД.
5. Уязвимость информации.
6. Типовые структурные компоненты АСОД.

7. Типы дестабилизирующих факторов.
8. Причины нарушения целостности информации.
9. Каналы несанкционированного получения информации без доступа нарушителя к элементам ЭВТ, АСОД.
10. Каналы несанкционированного получения информации с доступом нарушителя к элементам АСОД, но без их изменений.
11. Каналы несанкционированного получения информации с доступом нарушителя к элементам АСОД с их изменением.
12. Классификация угроз безопасности.
13. Основные методы защиты информации в вычислительных системах.
14. Общая схема идентификации и установления подлинности пользователя.
15. Метод проверки подлинности на основе простого пароля.
16. Метод проверки подлинности на основе динамически изменяющегося пароля.
17. Организация контроля информационной целостности.
18. Задачи решаемые аппаратными средствами защиты.
19. Классификация аппаратных средств защиты.
20. Классификация программных средств защиты.
21. Виды программных средств защиты.
22. Средства защиты данных.
23. Средства защиты от копирования.
24. Средства защиты информации о разрушения.
25. Концепция диспетчера доступа.

4.4.2 Вопросы к экзамену:

1. Методы управления безопасностью сетей.
2. Основные требования защиты сетей и возможные им угрозы.
3. Цели и задачи защиты информации в вычислительных сетях.
4. Перечень и содержание сервисов безопасности.
5. Стандарты сервисов безопасности.
6. Классификация видов услуг механизмов защиты.
7. Сущность методов распределения ключей при использовании механизмов цифровой подписи данных, передаваемых в сетях.
8. Основные положения концепции защиты информации в эталонной модели взаимодействия открытых сетей.
9. Назначение, задачи системы защиты СЗИ AURA.
10. Общее содержание функций подсистемы идентификации и аутентификации СЗИ AURA.
11. Общее содержание функций подсистемы разграничения доступа к ресурсам СЗИ AURA.
12. Общее содержание функций подсистемы контроля целостности СЗИ AURA.
13. Общее содержание функций подсистемы регистрации событий СЗИ

AURA.
14. Общее содержание функций подсистемы управления средствами защиты (администрирования) СЗИ AURA.
15. Назначение, задачи, классификация межсетевых экранов.
16. Назначение, задачи прокси-серверов.
17. Характеристика систем активного аудита.
18. Технологии и средства защиты процессов переработки информации в Интернете.
19. Основное содержание информационной безопасности в Интранете.
20. Назначение, состав и возможности системы защиты информации Dallas Lock.
21. Назначение, состав и возможности программно-аппаратного комплекса защиты информации Аккорд.
22. Назначение, состав и возможности программно-аппаратного комплекса защиты информации Соболь – PCI.
23. Назначение, состав и возможности программно-аппаратного комплекса защиты информации Страж NT.
24. Назначение, состав и возможности системы защиты Secret Disk.
25. Методы и средства нейтрализации угроз.
26. Основные нормативные правовые документы по информатизации и защите информации.
27. Основные специальные меры по технической защите информации, обрабатываемой средствами вычислительной техники. (Требования ФСТЭК).
28. Основные принципы защиты от НСД.
29. Основные способы и направления обеспечения защиты от НСД.
30. Основная структура и содержание монитора обращений.
31. Основные модели нарушителей в автоматизированных системах.
32. Порядок обеспечения защиты от НСД к ПК при его оставлении без завершения сеанса работы.
33. Классификация вирусов и методов защиты от них.
34. Классы и виды антивирусных программ.
35. Методы выявления программ-шпионов.
36. Укажите стандарты (ГОСТ Р) и РД, применяемые при эксплуатации СрЗИ.

4.4.3 Примерные темы курсовых проектов

1. Анализ методов и средств анализа защищенности беспроводных сетей.
2. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
3. Виброакустические средства современных систем обеспечения информационной безопасности.

4. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.

5. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.

6. Средства обеспечения информационной безопасности банков данных.

7. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).

8. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.

9. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.

10. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.

11. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.

12. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.

13. Инструментальные средства анализа рисков информационной безопасности.

14. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.

15. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).

16. Анализ рисков в области защиты информации

17. Управление рисками и международные стандарты

18. Технологии анализа рисков

19. Инструментальные средства анализа рисков

20. Аудит безопасности и анализ рисков

21. Анализ защищенности информационной системы

22. Обнаружение атак и управление рисками

23. Оценка серьезности сетевой атаки

24. Сигнатуры как основной механизм выявления атак

25. Анализ сетевого трафика и анализ контента.

26. IDS как средство управления рисками. Типовая и оптимальная архитектура системы выявления атак. Стандарты, определяющие правила взаимодействия между компонентами системы выявления атак.

CIDF. CVE - тезаурус уязвимостей. Пример использования. Рабочая группа IDWG.

5. ЗАКЛЮЧЕНИЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходят углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- *развивающая (*повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- *информационно-обучающая* (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- *ориентирующая и стимулирующая* (процессу обучения придается профессиональное ускорение);
- *воспитывающая* (формируются и развиваются профессиональные качества специалиста):
- *исследовательская* (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;

- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:

2. Выполнение письменных контрольных и курсовых работ;

3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:

4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

• индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;

• конспектирование лекций;

• получение консультаций для разъяснений по вопросам изучаемой дисциплины;

• подготовка ответов на вопросы тестов;

• подготовка к экзамену;

• выполнение контрольных, курсовых проектов и дипломных работ;

• подготовка научных докладов, рефератов, эссе;

• анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с *рабочей программой учебной дисциплины.* Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

• чтение текста (учебника, первоисточника, дополнительной литературы);

• составление плана текста;

• конспектирование текста;

• выписки из текста;

• работа со словарями и справочниками;

• исследовательская работа;

• использование аудио- и видеозаписи;

• работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

• работа с конспектом лекции (обработка текста);

• повторная работа над учебным материалом (учебника, первоисточ-

ника, дополнительной литературы, аудио- видеозаписей):

- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудио-видеотехники и компьютерных расчетных программ и электронных практикумов;
- подготовка курсовых проектов и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

6. ЛИТЕРАТУРА

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

1. Подтопельный, В. В. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие / В. В. Подтопельный. - Калининград : Изд-во БГАРФ, 2020. – Ч. 3. Поиск и извлечение вредоносных программ в программной среде.

Локальный электронный методический материал

Владислав Владимирович Подтопельный

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Редактор Г. А. Смирнова

Уч.-изд. л. 2,9. Печ. л. 2,6

Издательство федерального государственного бюджетного образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1

42