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

Н. Я. Великите

ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

УДК 004.56 (075)

Рецензент:
доцент кафедры информационной безопасности
Института цифровых технологий ФГБОУ ВО «КГТУ»
А. Г. Жестовский

Великите, Н. Я.
Введение в специальность: учеб.-метод. пособие по изучению дисциплины для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 20 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Введение в специальность» для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем. В нем представлен тематический план изучения дисциплины, содержание дисциплины по её разделам и темам, темы практических занятий, указания к изучению каждой темы, рекомендации по выполнению практических заданий. Содержатся требования к текущей и промежуточной аттестации, определены условия получения положительной оценки.
Табл. 1, список лит. – 5 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры информационной безопасности ФГБОУ ВО «Калининградский государственный технический университет» 8 сентября 2022 г., протокол № 1

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией Института цифровых технологий, протокол от 5 июля 2023 г., № 8

УДК 004.56(075)

Оглавление

Введение

В результате освоения дисциплины ожидается, что студенты получат целостное представление о широкой сфере проблем обеспечения информационной безопасности в автоматизированных системах.

Дисциплина «Введение в специальность» является вводной для изучения всех последующих дисциплин в рамках специальности «Информационная безопасность автоматизированных систем».

Далее в учебно-методическом пособии по изучению дисциплины с практическими заданиями представлен тематический план, содержащий перечень изучаемых тем, обязательных 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 потребуется 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.

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

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

1. Тематический план

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции		
1.1	Раздел 1. Общие вопросы информационной безопасности	Тема 1. Введение. Термины и определения	3	2
1.2		Тема 2. Стандарты информационной безопасности	3	4
2.1	Раздел 2. Современное состояние обеспечения информационной безопасности в автоматизированных системах	Тема 3. Основные регуляторы в области ИБ. Обзор некоторых интернет-ресурсов в помощь к изучению вопросов информационной безопасности	2	4
2.2		Тема 4. Технологии информационной безопасности	4	4
2.3		Тема 5. Мировые тренды обеспечения информационной безопасности	3	6
2.4		Тема 6. Введение в специализацию. Безопасность открытых информационных систем	2	2
			17	**22**
		Практические занятия		
1.1	Раздел 1. Общие вопросы информационной безопасности	Практическое занятие 1. Парольная защита. Количественные оценки парольной защиты	5	2
1.2		Практическое занятие 2. Определение пароля архива	4	2
2.1	Раздел 2. Современное состояние обеспечения информационной безопасности в автоматизированных системах	Практическое занятие 3. Знакомство с обзорами по ИБ. Рассмотрение аналитики на современных порталах в области ИБ	4	2,85
2.2		Практическое занятие 4 Рассмотрение технологий ИБ по индивидуальному заданию преподавателя (СКУД, Техническая защита, Криптография)	4	3

№ п.п.	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
			17	**9,85**
		Рубежный (текущий) и итоговый контроль		
1.1	Раздел 1. Общие вопросы информационной безопасности	Выполнение тестовых заданий	2(РЭ)	2
2.1	Раздел 2. Современное состояние обеспечения информационной безопасности в автоматизированных системах	Выполнение тестовых заданий	0,15(КА)	2
		Итоговый контроль (зачёт)	-	-
			2(РЭ)+0,15(КА)	**4**
		Всего	**34+2(РЭ)+0,15(КА)**	**35,85**

2. Содержание дисциплины и указания к изучению

2.1 Раздел 1. Общие вопросы информационной безопасности

2.1.1 Тема 1.1 Введение. Термины и определения

Перечень изучаемых вопросов:

1. История развития теории и практики обеспечения информационной безопасности.
2. Содержание и структура понятия информационной безопасности.
3. Общая характеристика принципов, методов и механизмов обеспечения информационной безопасности.

Методические указания к изучению:

В данной теме мы рассмотрим предмет и задачи дисциплины. Рассмотрим специфику профиля специалиста по защите информации, рассмотрим дисциплины, осваиваемые студентами в течении 5,5 лет обучения. Дадим определение ИБ из Доктрины Информационной безопасности РФ, утверждённой Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Сделаем исторический экскурс по этапам развития методов и средств обеспечения безопасности информации. В вопросе «Содержание и структура понятия ИБ» рассмотрим три основных свойства информации: конфиденциальность, целостность, доступность [1, 2].

Особое внимание следует обратить на определения угроз и их классификацию. Дадим определение автоматизированной системы, несанкционированного доступа, угрозы, источникам угроз, уязвимости информации, политике безопасности, познакомимся с перечнем сокращений, широко применяемых в ИБ (НСД, АС, БД, СЗИ, ПЭМИН, ЦЗИ) и рассмотрим другие понятия, которые более подробно изложены в лекционном материале в виде презентаций в среде ЭИОС.

1. Практическое занятие «Парольная защита. Количественные оценки парольной защиты» содержит в себе информацию по рассмотрению подсистем идентификации и аутентификации.

Целью данного практического занятия является количественная оценка стойкости парольной защиты и реализации простейшего генератора паролей, обладающего требуемой стойкостью к взлому. Парольная аутентификация пользователя, как правило, – передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Защищённость пароля при его подборе зависит в общем случае от скорости проверки паролей и от размера полного множества возможных паролей, которое, в свою очередь, зависит от длины пароля и размера применяемого алфавита символов. Кроме того, на защищённость сильно влияет реализация парольной защиты. В методических указаниях, которые приведены в ЭИОС по дисциплине «Введение в специальность», приведены примеры определения времени перебора пароля, определение минимальной длины пароля и времени перебора всех паролей с параметрами. Также приведены задания для выполнения по вариантам. Требования к отчёту и защите приведены в разделе ЭИОС.

Если студент пропустил лекционный и практический материал, то он может воспользоваться информацией по теме лекции и практического занятия, которая приведена в разделе ЭИОС в виде презентации, а также самостоятельно изучить материал, который приведён в литературных источниках (см. ниже).

Литература:
[1, с. 5-26, 40-51],
[2, с. 9-25].

Контрольные вопросы:

1. Что является предметом изучения дисциплины?
2. Были ли в вашей практике случаи попыток НСД к информации, обрабатываемой в АС?
3. Поясните различие между понятиями «компьютерная безопасность и «информационная безопасность». Какое из понятий является более общим?
4. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?
5. Чем определяется стойкость подсистемы идентификации и аутентификации?
6. Перечислите минимальные требования к выбору пароля. Какой пароль является «плохим», а какой «хорошим»?
7. Назовите основные способы аутентификации. Какой из этих способов является, по вашему мнению, наиболее эффективным?
8. Дайте определение идентификации и аутентификации пользователей. В чём разница между этими понятиями?
9. Что такое авторизация?
10. Каковы основные принципы защиты от НСД? В чём суть каждого из них?

2.1.2 Тема 1.2 Стандарты информационной безопасности

Перечень изучаемых вопросов:

1. Роль стандартов ИБ.
2. Международные стандарты ИБ.
3. Отечественные стандарты безопасности информационных технологий.

Методические указания к изучению:

При изучении данной темы следует пользоваться системами «КонсультантПлюс» и «Гарант», чтобы иметь возможность пользоваться актуальным материалами в рамках законодательства и нормативно-правовой базы.

Главной задачей стандартов ИБ является создание основы для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Особое внимание в рамках этой темы уделим стандартам информационной безопасности в Интернете. Рассмотрены особенности стандартизации процесса обеспечения безопасности; коммерческой информации в сетях с протоколами передачи данных IP/TCP, SMTP, POP, SNMP, SSL, SET, IPSec, PKI.

Среди различных стандартов по безопасности ИТ следует выделить нормативные документы по критериям оценки защищённости средств вычислительной техники и АС и документы, регулирующие информационную безопасность [2].

Изучение данной темы более подробно происходит в рамках дисциплин на старших курсах. А в рамках данной темы мы познакомимся с понятиями: Коммерческая тайна, Государственная тайна, Обладатель информации, Гриф секретности, Степень секретности и др.

2. Практическое занятие «Определение пароля архива»

Файлы ZIP имеют достаточно сильный алгоритм шифрования. Пароль не сохраняется где-нибудь в архиве, защищённом паролем. Архиватор конвертирует (преобразовывает) пароль, который вы ввели в три 32-разрядных ключа шифрования, и затем использует их, чтобы зашифровать целый архив. Таким образом, если мы будем пробовать комбинации всех возможных ключей, то полная сложность атаки – 2^{96}. Однако этот алгоритм не столь силен, как DES, RSA, IDEA и подобные.

То, что многие криптосистемы не ограничивают минимальную длину пароля, из которого формируется ключ, как раз и приводит к успеху атак перебором не ключей, а паролей.

Программа Advanced ZIP Password Recovery (Продвинутое Восстановление Пароля ZIP, или просто AZPR) может использоваться, чтобы восстановить потерянный пароль для архива ZIP. В настоящее время не имеется никакого известного метода извлечь пароль из сжатого файла; так что единственные доступные методы – «решение в лоб» – **атака типа «полный перебор»** и **атака по словарю.**

Программа AZPR используется для восстановления забытых паролей ZIP-архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (brute force) и атака по словарю (dictionary-based attack).

Практическое задание 1:

1. Подготовьте зашифрованные файлы с шаблоном имени try_me.zip в четырех вариациях пароля: в имени все символы буквы, все числа, чередование букв символов, сначала буквы потом символы. В пароле не вводите больше 3-4 символов.
2. Используя программу для вскрытия паролей, произвести атаку на зашифрованный файл try_me. Область перебора – все печатаемые символы, длина пароля – от 1 до 4 символов. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.
3. При выполнении задания зафиксируйте скорость перебора в программе, сохранив файл статистики Advanced Archive Password Recovery.
4. Сравните полученные в программе результаты с ранее полученными при вычислении «вручную».
5. Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

Практическое задание 2:

Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic (…\archpr _port\archpr _port\ English.dic). Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

Сравнить затраченное время с методом прямого перебора.

Замечание: более подробно практические задания со скриншотами примера выполнения с данным программного продукта приведены в системе ЭИОС.

Содержание отчёта

Отчёт должен содержать результаты расчётов числовых характеристик пароля согласно варианту задания; скриншоты промежуточных шагов каждой лабораторной работы. Каждая фотография должна быть подписана и сопровождаться кратким пояснением.

К текстовому документу должны быть приложены результирующие файлы по каждой из работ:

1. *.txt по результатам проверки программы «Определение оптимальных характеристик пароля с использование генетического алгоритма».
2. *.txt с результатами перебора грубой силой, программой AZPR.
3. *.txt с результатами перебора по словарю, программой AZPR.

Литература*:*

[2, с. 76-97].

Контрольные вопросы:

1. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.

2. Сформулируйте основные положения Закона РФ «Об информации, информатизации и защите информации». Какие ещё российские законодательные акты вы знаете в этой области?

3. Изложите кратко основное содержание руководящих документов ФСТЭК России в области защиты от НСД СВТ и АС.

4. Что представляет из себя стандарт ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management» (Информационные технологии. Методы обеспечения безопасности)?

5. Назовите главную задачу стандартов информационной безопасности.

6. Что понимается под «Оранжевой книгой»?

7. Сколько критериев требований безопасности предложены в «Оранжевой книге»?

8. Сколько групп безопасности для оценки защищённости информационных систем рассматриваются в «Оранжевой книге»?

9. Какими государствами были разработаны Европейские критерии безопасности информационных технологий?

10. Какие задачи средств информационной безопасности рассматривают в «Европейских критериях»?

2.2 Раздел 2. Современное состояние обеспечения информационной безопасности в автоматизированных системах

2.2.1 Тема 2.1 Основные регуляторы в области ИБ. Обзор некоторых интернет-ресурсов в помощь к изучению вопросов информационной безопасности

Перечень изучаемых вопросов:

1. Основные ключевые регуляторы в области ИБ, их функции, зоны ответственности.

2. Значение использования современных интернет-ресурсов в области информационной безопасности.

Методические указания к изучению:

В данной теме рассмотрены некоторые основные регуляторы в области ИБ. Приведены зоны их ответственности и функции. Рассмотрены следующие регуляторы: ФСБ России, ФСТЭК России, Минкомсвязи России, Роскомнадзор. В нормативных ссылках в данном пособии представлены соответствующие ссылки на официальные сайты рассмотренных регуляторов.

В современных реалиях сложно переоценить значение интернет-ресурсов в области ИБ.

С помощью этих ресурсов для специалистов по информационной безопасности можно найти ответы на любые вопросы, обсудить профессиональные темы и обменяться ссылками с другими пользователями. Блоги – самый понятный ресурс, в рамках которого авторы делятся опытом, знаниями и быстрыми решениями задач. Руководства по языкам программирования, обзоры интересных проектов, можно найти информацию от программистов со всего мира. Можно найти отзыв на разное ПО и понять, для чего оно нужно.

В данном УМП приводится краткая характеристика и назначения соответствующих ресурсов. Более подробно по соответствующим ссылкам можно познакомиться с этими интернет-ресурсами, размещёнными в системе ЭИОС.

Хабр — это русскоязычный веб-сайт в формате системы тематических коллективных блогов с элементами новостного сайта, созданный для публикации новостей, аналитических статей, мыслей, связанных с информационными технологиями, бизнесом и Интернетом.

Навигатор безопасника — русскоязычный веб-сайт, созданный в помощь для директоров по ИБ, руководителей и начальников отдела или службы ИБ, которые ищут ответы на вопросы по созданию, управлению и совершенствованию процессов ИБ на предприятии.

Системный интегратор «Инфосистемы JET». Джет — русскоязычный веб-сайт, который продает свои услуги. Продает: ЦОД, вычислительные комплексы и СХД, сетевые решения, защита информационной безопасности, управление IT-услугами и IT-инфраструктурой, IT-аутсорсинг и техническая поддержка, разработка ПО, внедрение и сопровождение бизнес-приложений. Имеют отраслевые решения: специализированные решения и услуги для операторов связи, банки и финансовые организации, государственные организации и силовые структуры.

SecurityLab — русскоязычный веб-сайт, который имеет новостной блок, статьи, обзор программного обеспечения, блоги компаний и блоги людей в сфере информационной безопасности.

Информзащита — является российским системным интегратором в области информационной безопасности, которые оказывают услуги и предлагают эффективные комплексные решения по информационной безопасности.

Ростелеком — российский провайдер цифровых услуг и сервисов. Предоставляет услуги широкополосного доступа в Интернет, интерактивного телевидения, сотовой связи, местной и дальней телефонной связи и др. Занимает лидирующие позиции на российском рынке высокоскоростного доступа в Интернет, платного ТВ, хранения и обработки данных, а также кибербезопасности.

«Код ИБ»

Рекомендуется просмотреть соответствующие ресурсы и найти дополнительные источники веб-ресурсов, которые рассматривают проблемы информационной безопасности.

Литература:

1. Хабр [Электронный ресурс]: – веб-сайт. – режим доступа: https://habr.com/ru/.
2. Навигатор безопасника [Электронный ресурс]: – веб-сайт. – режим доступа: https://community.codeib.ru/.
3. Системный интегратор «Инфосистемы JET» [Электронный ресурс]: – веб-сайт. – режим доступа: https://jet.su/.
4. Информационный портал по безопасности [Электронный ресурс]: – веб-сайт. – режим доступа: https://www.securitylab.ru/.
5. Системный интегратор «Информзащита» [Электронный ресурс]: – веб-сайт. – режим доступа: https://www.infosec.ru/.
6. Ростелеком [Электронный ресурс]: – веб-сайт. – режим доступа: https://moscow.rt.ru.
7. КОД ИБ [Электронный ресурс]: – веб-сайт. – режим доступа: https://codeib.ru.
8. StaffCop [Электронный ресурс]: – веб-сайт. – режим доступа: https://www.staffcop.ru.
9. ФСТЭК России. [Электронный ресурс]: – веб-сайт. – режим доступа: https://fstec.ru/.
10. ФСБ России [Электронный ресурс]: – веб-сайт. – режим доступа: http://www.fsb.ru/.

3. Практическое занятие «Знакомство с обзорами по ИБ. Рассмотрение аналитики на современных порталах в области ИБ» содержит в себе информацию по аналитическим отчётам по ИБ в области актуальных киберугроз на текущий квартал соответствующего года, а также международные новости утечек информации, ежегодные аналитические отчеты и статистика по инцидентам за прошедшие годы.

Целью данного практического занятия является знакомство с актуальной аналитикой.

Аналитика безопасности – одно из важнейших направлений деятельности специалистов в области безопасности, в том числе информационной безопасности, поэтому в отчётах по направлению «Аналитика ИБ» есть данные, тенденции, выводы, которые необходимы в работе.

Аналитика безопасности содержит не только разделы «Аналитика ИБ» и данные про утечки информации, кибератаки, киберриски. Аналитика безопасности позволяет шире взглянуть на ситуацию, выйти за рамки повседневных проблем, понять, с какими проблемами безопасности специалисты и пользователи могут столкнуться завтра, какие задачи в области ИБ им придётся решать.

Сегодня аналитика ИБ требует системного подхода. В каждом представленном здесь отчёте описана методика, согласно которой отбирались и обрабатывались данные, ведь аналитика безопасности (аналитика ИБ) – это наука. Но аналитика безопасности – не просто сухие числа и графики, но и гипотезы, рассуждения, не позволяющие забыть, что безопасность – это ещё и искусство. Представленная в этом разделе аналитика ИБ отражает ключевые тенденции.

Аналитика ИБ – это новые исследования каждый месяц.

Практическое задание 1:

- ознакомиться с актуальной аналитикой отрасли информационной безопасности на портале компании «Инфовотч» https://www.infowatch.ru/analytics/analitika;
- подготовить обзор и информационное сообщение по индивидуальному заданию преподавателя с использованием ресурсов портала Инфовотч.

Практическое задание 2:

- ознакомиться с актуальной аналитикой отрасли информационной безопасности на портале компании Positive Technologies https://www.ptsecurity.com/ru-ru/research/analytics/;
- подготовить обзор и информационное сообщение по индивидуальному заданию преподавателя с использованием ресурсов портала Инфовотч.

Практическое задание 3:

ознакомиться с актуальной аналитикой отрасли информационной безопасности на портале компании «Код Безопасности» https://www.securitycode.ru/documents/analytics/.

- подготовить обзор и информационное сообщение по индивидуальному заданию преподавателя с использованием ресурсов портала «Код Безопасности».

Содержание отчёта

Отчёт должен содержать результаты обработки информации по индивидуальному заданию соответствующих порталов в области ИБ, оформленные в виде презентации и выложенные в ЭИОС.

Контрольные вопросы:

1. Какие основные методологические документы ФСТЭК России Вы знаете?
2. Какие руководящие документы ФСТЭК России, описывающие классификацию, Вы знаете?
3. Что такое реестры?
4. Какие виды деятельности ФСБ России Вы знаете?
5. Что такое критическая информационная инфраструктура (КИИ)?
6. Что относится к объектам КИИ?
7. Что относится к субъектам КИИ?

2.2.2 Тема 2.2 Технологии информационной безопасности

Перечень изучаемых вопросов:

1. Вирус. Антивирус. Песочницы. Общая информация. Стандартные методы антивирусной защиты. Антивирусное ПО.
2. Межсетевые экраны. Общая информация по программной и аппаратной технологии.
3. Инфраструктура открытых ключей (PKI).

Методические указания к изучению:

Целью этой темы является знакомство студентов с некоторыми технологиями, которые используются в современных системах защиты информации.

Рассмотрим компьютерные вирусы как специальный класс саморепродуцирующих программ. Рассмотрим средства антивирусной защиты. Антивирусная программа (антивирус) – любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифици-

рованных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Рассмотрим жизненный цикл вредоносной программы, среды обитания, отличительные свойства программных закладок, среда обитания, этапы программного противоборства, стандартные методы антивирусной защиты, виды антивирусных средств, простейшие организационные меры.

Ещё одной из технологий мы рассмотрим межсетевые экраны.

Межсетевой экран (МЭ) – это специализированный комплекс, называемый также брандмауэром или системой firewall.

Для большинства организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети.

Рассмотрим функции МЭ, проблемы безопасности МЭ, схемы сетевой защиты на базе МЭ.

Инфраструктура открытых ключей – это набор служб и сервисов для издания, хранения, обновления и отзыва цифрового сертификата открытого ключа подписи. Возникла в связи с необходимостью защищённого электронного документооборота как внутри компании, так и за её пределами и необходимостью удалённого доступа к ресурсам компании. Рассмотрим выгоды от внедрения системы.

Литература:
[1, с. 85-95, 72-77],
[2, с. 193-216, 98-120, 137-141],
[3, с. 1-62],
[4, с. 1-62].

Контрольные вопросы:

1. Дайте определение компьютерного вируса как саморепродуцирующей программы. Приведите примеры известных вам случаев заражения компьютерными вирусами.
2. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.
3. Охарактеризуйте известные вам основные классы антивирусных программ. В чём смысл комплексного применения нескольких программ?
4. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.
5. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?
6. Какие задачи призван решить МЭ?
7. Перечислите основных производителей МЭ.
8. Для чего используется категорирование межсетевых экранов?
9. Что такое удостоверяющий центр?
10. Hash-значение, что такое?
11. В чём смысл симметричного и асимметричного шифрования?
12. В чём преимущества и недостатки симметричного и асимметричного шифрования?
13. Как расшифровывается PKI?

4. Практическое занятие. «Рассмотрение технологий по индивидуальному заданию преподавателя» содержит в себе информацию по изученным на лекциях учебным вопросам и технологиям. Индивидуальные задания приведены в ЭИОС. На практическом занятии рассматривается пример.

Пример 1. Шифр Цезаря. Получим криптограмму с использованием шифра Цезаря с ключом d = 1 на базе английского алфавита, строчный регистр.

Исходное сообщение: information

Криптограмма: jogpsngujpo

Для русского языка с ключом d=10:

Исходное сообщение: информация

Криптограмма: тчюшьцйати

Используя шифр простой замены

Практическое задание 1: используя шифры простой замены и информацию из литературы [1], стр. 52-83, зашифровать любую комбинацию слов, например: «простая замена один из самых древних шифров», с помощью шифрования методом простой замены. В качестве тренировочных заданий выполнить шифрование и дешифрование с помощью виртуального тренажёра. Методические указания для работы с применением виртуального тренажёра приведены в ЭИОС.

Практическое задание 2: разбиться на группы по 4 человека и дешифровать сообщение соседней группы. Начальные условия для облегчения решения практического задания будут известны. В качестве тренировочных заданий выполнить шифрование и дешифрование с помощью виртуального тренажёра. Методические указания для работы с применением виртуального тренажёра приведены в ЭИОС.

Содержание отчёта

Отчёт будет содержать название работы, цель работы, последовательность действий для получения результата (шифрования, дешифрования), общие выводы, сделанные в процессе выполнения задания.

2.2.3 Тема 2.3 Мировые тренды обеспечения информационной безопасности

Перечень изучаемых вопросов:

1. Адаптивный. Поведенческий мониторинг.
2. Машинное обучение и возможности его применения в ИБ.
3. Безопасность IoT (Интернет вещей). Вызовы информационной безопасности.

Методические указания к изучению:

Целью этой темы является знакомство студентов с некоторыми трендами, тенденциями, которые позволяют повысить эффективную работу в области ИБ. Это связано с тем, что сейчас сменяется фокус обеспечения ИБ компаний с предотвращения атаки на её раннее обнаружение. В первом вопросе рассмотрим, с чем связано появление адаптивного мониторинга. Рассмотрим историческое развитие. Первый этап – реактивная обработка. Ручная реакция на инциденты. Второй этап – инструментальная обработка, которая содержит использование неспециализированных инструментов и технологий.

Третий этап – интегрированная система – включает в себя применение специализированных средств, частичная интеграция с различными системами. Четвёртый этап: Стратегическая интеграция – включает в себя тесную интеграцию с ИС компании. Пятый этап – динамический анализ – предполагает наличие АС, которая использует корреляционный анализ для обнаружения инцидентов ИБ и возможность анализа базы инцидентов. Шестой этап – продвинутая аналитика – подразумевает под собой раннее обнаружение атак различного рода при помощи исторического и поведенческого анализа.

Применение машинного обучения важно при активном применении DLP, которые уменьшают ошибки первого и второго рода путём адаптации правил. А также ускорение поиска необходимых данных в больших хранилищах, оптимизация настроек средств обеспечения безопасности.

В рамках факультатива более подробно можно будет ознакомиться с данной тематикой Интернета вещей в более широком объёме. Есть сложность с унификацией, так как существует большое количество разнообразных конечных устройств. Ещё одна из проблем – это использование обновлений и контроль за правильностью этих обновлений. Это перспективное направление Интернета вещей будет продолжать развиваться в части защиты конечных устройств, безопасности среды передачи данных и безопасности данных.

Данная тема не содержит практического задания. Скорее можно сказать, что углубленное изучение данных учебных вопросов может стать научно-исследовательской работой студентов на старших курсах и стать одной из тем при написании ВКР (дипломная работа).

2.2.4 Тема 2.4 Введение в специализацию. Безопасность открытых информационных систем

Перечень изучаемых вопросов:

1. Принципы и технология открытых систем.
2. Особенности и проблемы защиты информации в открытых информационных системах.

Методические указания к изучению:

Целью изучения данной темы является предварительное знакомство студентов специальности 10.05.03 Информационная безопасность автоматизированных систем с проблематикой специализации «Безопасность открытых информационных систем» и дисциплинами, на которых они будут изучать данные вопросы.

Практически к любой информационной системе предъявляются три основных требования: система должна обеспечивать функциональность; информационную безопасность; совместимость.

Область работ, посвящённых обеспечению совместимости, носит название принципов и технологии открытых систем.

Под основными свойствами открытости понимаются: переносимость и переиспользуемость программного обеспечения, данных и опыта людей; интероперабельность, т.е. возможность взаимодействия компонентов распределённой системы посредством обмена информацией и её совместного использования; масштабируемость как свойство сохранения работоспособности системы ИТ в условиях варьирования значений параметров, определяющих технические и ресурсные характеристики системы и/или поддерживающей среды.

Открытость систем достигается на основе стандартизации их поведения, наблюдаемого на границах систем или их интерфейсах. Таким образом, под открытыми системами можно понимать системы, обладающие стандартизованными интерфейсами, и решение проблемы открытости систем основывается на стандартизации интерфейсов систем и протоколов взаимодействия между их компонентами.

Методологическую основу концепции открытых систем составляют:

- концептуальный базис и принципы построения открытых систем,
- эталонная модель окружений открытых систем (RM OSE),
- эталонная модель взаимосвязи открытых систем (RM OSI),
- аппарат профилирования ИТ, предназначенный для конструирования открытых систем в пространстве стандартизованных решений,
- концепция тестирования конформности систем ИТ исходным стандартам и профилям,
- таксономия профилей.

Основными документами, определяющими методологическую основу концепции открытых систем, являются:

1) Технический отчет ISO/IEC TR 10000 Framework and taxonomy of International Standardized Profiles (Основы и таксономия международных стандартизованных профилей) в трёх частях [1, 2, 3], включая: Часть 1: General Principles and Documentation Framework (Общие принципы и основы документирования). Часть 2: Principles and Taxonomy for OSI Profiles (Принципы и таксономия профилей взаимосвязи открытых систем). Часть 3: Principles and Taxonomy for Open System Environment Profiles (Принципы и таксономия профилей окружений открытых систем).

2) Эталонная модель окружения (среды) открытых систем (RM OSE) - ISO/IEC DTR 14252, Portable Operating System Interface for Computer Environments - POSIX. (IEEE, P1003.0, Draft Guide to the POSIX Open System Environment).

3) Эталонная модель взаимосвязи открытых систем (RM OSI) - ISO 7498:1996, Information processing systems - Open Systems Interconnection - Basic Reference Model [ITU-T Rec. X.200].

Именно в этих документах установлены базовые понятия открытых систем, иерархическая модель пространства спецификаций ИТ (стандартов и профилей), а также строение и основное содержание этого пространства.

Профиль защиты информации. Очень важным моментом является эшелонированность системы, обеспечивающей информационную безопасность. От этого зависит надёжность всей системы. Тем не менее она оценивается по самому слабому звену. Самым слабым звеном чаще всего является человеческий фактор. Важно выделять его отдельно из всех угроз. Уже сейчас руководящими документами ФСТЭК России предполагаются две группы критериев безопасности: показатели защищённости средств вычислительной техники от несанкционированного доступа и критерии защищённости автоматизированных систем обработки данных. Таким образом осуществляются попытки гибко настроить систему безопасности на государственном уровне. Наше государство приходит к использованию узконаправленных рекомендаций – прообразам профилей защиты.

Можно построить множество профилей защиты информации, привязывая каждый из них к заранее оговорённым данным, ограничениям и требованиям. Но при разработке этих профилей должны учитываться принципы открытости.

Таким образом, стоит задача одновременно учитывать требования открытости и защиты и, в первую очередь, синтезировать модели открытой системы и защиты информации.

3. Требования к аттестации по дисциплине

3.1 Текущий и промежуточный контроль успеваемости

Оценивание поэтапного формирования результатов освоения дисциплины осуществляется в процессе текущего контроля, который представляет собой единый непрерывный процесс оценки знаний, умений, формирования и сформированности компетенций у обучающихся.

Текущий контроль предназначен для проверки хода и качества усвоения обучающимися учебного материала и стимулирования учебной работы студентов. Он может осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины. Текущий контроль предполагает постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Результаты контроля могут учитываться выставлением оценок в журнале учёта успеваемости.

Для текущего контроля успеваемости используются тестовые задания.

Положительная оценка («зачтено») по результатам контроля выставляется в соответствии с универсальной системой оценивания, приведённой в таблице 2. В случае получения оценки «не зачтено» студент должен пройти повторный контроль по данной теме в ходе последующих консультаций.

Примерный перечень тестовых вопросов приведён документе ФОС по дисциплине «Введение в специальность». Критерием оценивания выполнения тестирования является количество правильно выполненных тестовых заданий, свидетельствующих о полноте знаний теоретического материала в области дисциплины «Введение в специальность» по информационной безопасности. Критерий оценивания приведён в документе ФОС.

Таблица 1 – Система оценок и критерии выставления оценки при прохождении контроля (опроса)

Критерий	Система оценок			
	«не зачтено»	**«зачтено»**		
Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно корректно связывать между собой (только некоторые из них может связывать между собой)	Обладает минимальным набором знаний, необходимых для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект

Промежуточная аттестация по дисциплине «Введение в специальность» проводится в период зачётной недели. К оценочным средствам для промежуточной аттестации по дисциплине, проводимой в форме зачёта, относятся тестовые задания для текущего контроля успеваемости

Промежуточная аттестация в форме зачёта (выполнение тестовых заданий) проходит по результатам прохождения текущего контроля успеваемости в течение семестра.

3.2 Примерный перечень вопросов к самостоятельной проверке своих знаний по дисциплине:

1. Определите вероятность несанкционированного получения информации нарушителем, если в рассматриваемой автоматизированной системе (АС) возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающие АС.

2. Определите вероятность несанкционированного получения информации нарушителем, если каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дисплея и выдача её на печать.

3. В чём, по Вашему мнению, состоит опасность разработки и применения информационного оружия?

4. Какие меры международного характера необходимо было бы принять в целях предотвращения информационных войн?

5. Какие основные методы контроля доступа используются в современных автоматизированных системах?

6. Как реализовать методы контроля доступа и их возможности в АС ведения текущих счетов клиентов банка?

7. Дайте определение шифра и сформулируйте основные требования к нему.

8. Приведите пример совершенного шифра.

9. Перечислите основные требования, предъявляемые к хеш-функции, пригодной для использования при вычислении цифровой подписи документа.

10. Изложите принципиальную схему организации обмена документами, заверенными цифровой подписью.

11. Изложите принципиальную схему организации секретной связи с использованием системы шифрования с открытым ключом.

12. Разложите на простые сомножители число 391, которое является произведением двух близких по значению простых чисел.

13. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

14. Приведите примеры известных вам случаев заражения компьютеров вирусами.

15. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

16. Назовите основные виды технических каналов.

17. Дайте классификацию источников утечки информации.

18. Назовите методы и средства защиты информации от утечки по побочному электромагнитному каналу.

19. Охарактеризуйте основные способы предотвращения утечки информации по техническим каналам.

20. С чем связана необходимость организационно-правового обеспечения защиты информации?

21. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации.

22. Каковы должны быть функции центров защиты информации для наиболее полной реализации стоящих перед ними задач?

4 Список литературы

4.1 Основная литература:

1. Малюк, А. А. Введение в защиту информации в автоматизированных системах: учеб. пособие / А. А. Малюк; авт.: Пазизин, С.В., Погожин, Н.С. - 3-е изд. стер. - М.: Горячая линия - Телеком, 2005. - 147 с.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - М.: Издательский Дом «Форум»: ИНФРА-М, 2013. - 416 с.

3. Жестовский, Александр Георгиевич. Программно-аппаратные средства обеспечения информационной безопасности: лабораторный практикум для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / А. Г. Жестовский, В. В. Подтопельный; БГАРФ ФГБОУ ВО «КГТУ». - 2-е изд., перераб. и доп. - Калининград: Издательство БГАРФ. - Текст: непосредственный. Ч. 1: Защита компьютерной информации и компьютерных систем от вредоносных программ. - 2019.

4. Подтопельный, В. В. Программно-аппаратные средства защиты информации: учебное пособие / В.В. Подтопельный. – ФГБОУ ВО «КГТУ». – Калининград: Издательство КГТУ. - Электрон. версия печ. публикации. - Текст: электронный. Ч. 1: Поиск и удаление вредоносных объектов в информационных системах. - 2023.

4.2 Интернет-ресурсы:

1. http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/ - электронный каталог библиотеки БГАРФ.

2. http://elibrary.ru - электронная библиотека Elibrary.

3. http://rugost.com - электронный каталог ГОСТов.

4. https://fstec.ru/component/attachments/download/2018.

Заключение

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических заданий. Преподавателю, ведущему курс, рекомендуется на вводной лекции определить структуру курса, пояснить цели и задачи изучения дисциплины, сформулировать основные вопросы и требования к результатам освоения.

При рассмотрении темы важно выделить основные понятия и определения, желательна их визуализация. При подготовке и проведении занятий по данному курсу преподаватель должен руководствоваться как общими учебно-методическими принципами (научность, системность, доступность, последовательность, преемственность, наличие единой

внутренней логики курса, его связь с другими предметами), так и специфическими особенностями дисциплины. В подборе материала к занятиям следует руководствоваться рабочей программой учебной дисциплины, обращая внимание на компетенции, указанные в федеральном государственном образовательном стандарте высшего образования.

На первом занятии преподаватель обязан довести до обучающихся порядок работы в аудитории и нацелить их на проведение самостоятельной работы с учётом количества часов, отведённых на неё учебным планом. Рекомендуя литературу для самостоятельного изучения, преподаватель должен максимально использовать возможности, предлагаемые библиотекой академии, в том числе её электронными ресурсами.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления или процессов, научные выводы и практические рекомендации.

В конце лекции необходимо делать выводы и ставить задачи на самостоятельную работу. Практические занятия направлены на закрепление лекционного материала.

Самостоятельная работа студентов заключается в подготовке к практическим занятиям и выполнении заданий, выдаваемых преподавателем по каждому из разделов дисциплины. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с полученным заданием. Выполненные практические задания студенты выкладывают в соответствующий раздел в ЭИОС.

Локальный электронный методический материал

Наталья Яронимо Великите

ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

Редактор М. А. Дмитриева

Уч.-изд. л. 0,9. Печ. л. 1,2.

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