МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«11» 04 2023 г.

Защита информационных процессов в компьютерных системах

Методические указания по выполнению самостоятельной работы
для студентов направления подготовки 10.03.01
«Информационная безопасность»

Курск 2023

УДК 004

Составители: ст.преп. Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры «Вычислительная техника» А.В. Киселев

Защита информационных процессов в компьютерных системах: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. - Курск, 2023. - 20с.: Библиогр.: с. 20.

Содержатся сведения о темах для самостоятельного изучения по дисциплине «Защита информационных процессов в компьютерных системах», необходимые для успешного освоения дисциплины. Указывается порядок выполнения самостоятельной работы всех предусмотренных учебным планом видов, приводятся рекомендации по оформлению результатов работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

Введение

Самостоятельная работа - это индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, но по его заданиям и под его контролем.

Самостоятельная работа студентов включает:

- изучение лекционного материала по конспекту с использованием рекомендованной литературы;
- отработку изучаемого материала по печатным и электронным источникам, конспектам лекций;
- подготовку к выполнению лабораторных работ;
- выполнение отчетов по лабораторным работам и подготовку к их защите;
- индивидуальные задания (решение задач, подготовка сообщений, докладов, исследовательские работы и т.п.);
- работу над творческими заданиями;
- подготовку кратких сообщений, докладов, рефератов, самостоятельное составление задач по изучаемой теме (по указанию преподавателя).

Назначение самостоятельной работы студентов.

- ***Овладение знаниями***, что достигается:

чтением текста (учебника, первоисточника, дополнительной литературы), составлением плана текста, графическим структурированием текста, конспектированием текста, выписками из текста, работой со словарями и справочниками, поиском информации в сети Интернет и т.п.;

- ***закрепление знаний,*** что достигается:

работой с конспектом лекций, обработкой текста, повторной работой над учебным материалом (учебником, первоисточником, дополнительнойлитературой), составлением плана, составлением таблиц для систематизации учебного материала, ответами на контрольные вопросы, заполнением рабочей тетради, аналитической обработкой текста (аннотирование, рецензирование, реферирование, конспект-анализ и др), составлением библиографии и т.п.;

- ***формирование навыков и умений***, что достигается:

решением задач и упражнений по образцу, решением вариативных задач, выполнением схем, выполнением расчетов, решением ситуационных задач, подготовкой к дискуссиям, проектированием и моделированием

разных видов и компонентов профессиональной деятельности, математическим описанием опытно экспериментальной работой и т.п.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от поставленной цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Текущий контроль качества выполнения самостоятельной работы может осуществляться с помощью:

- контрольного опроса;
- собеседования;
- автоматизированного программированного контроля (машинного контроля, тестирования с применением ЭВМ).

Содержание самостоятельной работы

№	Наименование раздела учебной дисциплины	Задание	Алгоритм выполнения задания	Форма представления выполненного задания
1.	Проблемы информационной безопасности сетей	Подготовить реферат по определенной теме. Тематика рефератов указана в Приложении 1	1. Найти информацию по любому из источников или с помощью сети Интернет по выбранной теме (Приложение 1) 2. Оформить реферат	Реферат, оформленный в соответствии с Приложением 4
2.	Политика безопасности	Создать компьютерную презентацию	Используя УМК по дисциплине найти информацию о методах доступа к сети, их характеристиках, принципах работы**;** Проанализировать информацию и оформить презентацию согласно требованиям к презентации, указанным в Приложении 2	Ссылка на презентацию
		Составить сводную таблицу основных компонентов политики безопасности в организации;	1. Задание 2. Источники: УМК по дисциплине	Ссылка на файл
3.	Технологии аутентификации	Выполнение индивидуального задания из Приложения 3	Используя УМК по дисциплине найти информацию выбранной теме и выполнить пункты задания	Ссылка на текстовый файл

4.	Технологии межсетевых экранов	Выполнение индивидуальн ого задания из Приложения 3	Используя УМК по дисциплине найти информацию выбранной теме и выполнить пункты задания	Ссылка на текстовый файл
5.	Технологии защиты от вирусов	Создание презента ции «Технологии защиты от вирусов»	Используя УМК по дисциплине найти информацию по технологиям защиты от вирусов	Ссылка на презентацию
		Выполнить сравнительный анализ относительно уровня угроз компьютерных вирусов	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл
		Составьте сводную таблицу методов обнаружения компьютерных вирусов	Источники: УМК по дисциплине	Сводная таблица, оформленная в тетради или ссылка на файл
6.	Технологии анализа защищенности и обнаружения сетевых атак	Создание презентации «Технологии анализа защищенности и обнаружения сетевых атак»	Используя УМК по дисциплине найти информацию по технологиям анализа защищенности и обнаружения сетевых атак	Ссылка на презентацию
		Выполнить сравнительный анализ методов обнаружения атак	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл
7.	Требования к системам защиты информации	Составить сводную таблицу систем обнаружения атак и защиты информации	Источники: УМК по дисциплине	Сводная таблица, оформленная в тетради или ссылка на файл
8.	Аудит безопасности информационных	Создание презентации «Аудит в	Используя УМК по дисциплине найти информацию по	Ссылка на презентацию

	систем	информационн ой безопасность компьютерны х сетей»	методикам аудита в информационной безопасность компьютерных сетей	
		Выполнение индивидуальн ого задания из Приложения 3	Используя УМК по дисциплине найти информацию выбранной теме и выполнить пункты задания	Ссылка на текстовый файл
9	Разработка и защита Web-сайтов	Выполнить сравнительный анализ методов и средств защиты веб-сервисов от потенциальных атак	Источники: УМК по дисциплине	Сравнительная таблица, оформленная в тетради или ссылка на файл

Приложение 1

Темы рефератов

№ п/п	Название темы
1	Основы сетевой безопасности.
2	Сеть как объект защиты.
3	Уязвимость компонентов распределенных АС.
4	Рабочие станции,
5	Серверы и коммуникационное оборудование,
6	Каналы связи.
7	Виды угроз информационной безопасности.
8	Классификация угроз информационной безопасности в КС: Естественные угрозы,Искусственные угрозы, Основные непреднамеренные искусственные угрозы,
9	Основные преднамеренные искусственные угрозы,
10	Классификация каналов проникновения в систему и утечки информации,
11	Неформальная модель киберпреступника,
12	Европейская конвенция о киберпреступности.
13	Идентификатор беспроводной локальной сети (SSID),
14	Аутентификация,
15	Комплексная система обеспечения безопасности беспроводных сетей,
16	WPA/WPA2 (Wi-Fi Protected Access, защищенныйдоступ Wi-Fi),
17	Стандарт IEEE 802.1x/EAP, EAP-MD5, EAP-TLS,
18	Развертывание беспроводных виртуальных сетей,
19	Системы обнаружения вторжения в беспроводных сетях,
20	Унифицированные решения.

Текст реферата необходимо набирать в текстовом процессоре с соблюдением следующих правил:

1. Формат документа А4.
2. Ориентация: книжная.
3. Поля: верхнее — 2 см, нижнее — 2 см, левое — 2,5 см, правое — 1 см.
4. Выравнивание текста по ширине.

5. Выравнивание заголовков либо по центру, либо по левому краю (единообразно для всей работы).

6. Установка переносов автоматическая.

7. Абзацный отступ — 1,5 см.

8. Интервал одинарный.

9. Интервал после заголовка до подзаголовка — 12 пт., до текста — 18 пт.

10. Шрифт для заголовков и подзаголовков Arial —14 пт.,

11. Шрифт для текста Times New Roman — 12 пт.

12. Начертание: для заголовка и подзаголовка — полужирный, для текста — обычный.

13. Нумерация страниц вставляется в нижний колонтитул без черточек и точек, размер шрифта 12 пт., начинается со второго листа.

14. Оформление оглавления автоматическое, располагается перед введением.

15. Переход на новую страницу необходимо делать с помощью комбинации клавиш Ctrl + Enter.

16. Нумерованные и многоуровневые списки оформляются с точкой после каждой цифры.

17. Использование маркированных списков с помощью символов:

▪ (квадратик);

• (кружочек);

- (дефис).

18. Стиль маркеров единообразный для всей работы.

19. Список использованных источников (книги, статьи, Интернет-ресурс) не менее

Требования по содержанию реферата:

1. реферат должен содержать достоверные и актуальные сведения на достаточном научном уровне;
2. реферат, кроме текста, может дополнительно содержать: качественные цветные иллюстрации, фрагменты программ, исполняемые модули, фрагменты информационных систем, презентации и другие материалы качественно дополняющие основную часть реферата.

Приложение 2

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ПРЕЗЕНТАЦИИ

Электронная презентация — электронный документ, представляющий набор слайдов, предназначенный для демонстрации проделанной работы.

Целью любой презентации является визуальное представление замысла автора, максимально удобное для восприятия. Электронная презентация должна показать то, что трудно объяснить на словах.

Задачи презентации:

- привлечение внимания аудитории;
- предоставление необходимой информации, достаточной для восприятия результатов проделанной работы без пояснений;
- предоставление информации в максимально комфортном виде;
- акцентирование внимания на наиболее существенных информационных разделах.

Схема презентации:

1. Титульный слайд
2. Введение (содержание)
3. Основная часть
4. Заключение
5. Список использованных источников

Требования к оформлению слайдов:

Средний расчет времени, необходимого на презентацию ведется исходя из количества слайдов. Обычно на один слайд необходимо не более двух-трех минут.

- Необходимо использовать максимальное пространство экрана (слайда) - например, растянув рисунки. По возможности используйте верхние ¾площади экрана (слайда), т.к. с последних рядов нижняя часть экрана обычно не видна.
- Дизайн должен быть простым и лаконичным.
- Каждый слайд должен иметь заголовок.
- Слайды могут быть пронумерованы с указанием общего количества слайдов в презентации.
- Завершать презентацию следует кратким резюме, содержащим ее основные положения, важные данные, прозвучавшие в докладе, и т. д.

Оформление заголовков:

Назначение заголовка — однозначное информирование аудитории о содержании слайда. Сделать это можно, по меньшей мере, тремя способами:

озвучив тему слайда, лаконично изложив самую значимую информацию слайда или сформулировав основной вопрос слайда. В заголовке нужно указать основную мысль слайда. Из одного слайда можно вынести много смыслов и тезис в заголовке делается для того, чтобы слушатель понял, что именно он должен понять. Все заголовки должны быть выполнены в едином стиле (цвет, шрифт,размер, начертание).

- Текст слайда для заголовков должен быть размером 24 — 36 пунктов.
- Точку в конце заголовков не ставить. А между предложениями ставить.
- Не писать длинные заголовки.
- Слайды не могут иметь одинаковые заголовки. Если хочется назвать одинаково — желательно писать в конце (1), (2), (3) или Продолжение 1, Продолжение 2.

Выбор шрифтов:

Для оформления презентации следует использовать стандартные, широко распространенные пропорциональные шрифты, такие как Arial, Tahoma, Verdana, Times New Roman, Georgia и др.

Кроме того, большинство дизайнерских шрифтов, используемых обычно для набора крупных заголовков в печатных изданиях, оформления фирменного стиля, упаковок и т. д., в рамках презентации смотрятся слишком броско, отвлекают внимание от ее содержания, а порой и просто вызывают раздражение аудитории.

В одной презентации допускается использовать не более 2 – 3 различных шрифтов, хотя в большинстве случаев вполне достаточно и одного. Размер шрифта для информационного текста 18 – 22 пункта.

Цветовая гамма, текстовое наполнение:

Для презентации изначально необходимо подобрать цветовую гамму: обычно это три—пять цветов, среди которых есть как теплые, так и холодные. Очевидно, любой из этих цветов должен отлично читаться на выбранном ранее фоне; малейшее подозрение на то, что цвет шрифта хотя бы немного сливается с фоном — и что-то одно из этого подлежит немедленной замене: не вынуждайте тех, для кого делается презентация, портить зрение. Назначив каждому из текстовых элементов свой цвет, например: крупным заголовкам — красный, мелким за- головкам — зеленый, подрисуночным

подписям — оранжевый и т. п., нужно следовать такой схеме на всех слайдах.

Ни в коем случае не стоит стараться разместить на одном слайде как можно больше текста. Так как мелкий текст плохо воспринимается.

Использование рисунков, диаграмм, схем:

Обязательно иллюстрируйте презентацию рисунками, фотографиями, наглядными схемами, графиками и диаграммами. Яркие картинки привлекают внимание куда эффективнее, чем сплошной текст или. Изображению всегда следует придавать как можно больший раз- мер; если это возможно, иллюстрации стоит распределить по нескольким слайдам, нежели размещать их на одном но в уменьшенном виде. Подписи вполне допустимо располагать не над и не под изображением, а сбоку, если оно, например, имеет вертикальную ориентацию. Не следует перегружать слайд графическими объектами.

Приложение 3

Индивидуальные задания

РАБОТА No 1.

Тестовые испытания программных средств защиты. Индивидуальные задачи:

1.Механизм идентификации и аутентификации субъектов доступа;

2.Механизм контроля доступа субъектов к информационным ресурсам;

3.Механизм регистрации учета событий.

РАБОТА No 2.

Тестовые испытания программных средств защиты. Индивидуальные задачи:1.Механизм очистки памяти;

2.Механизм обеспечения целостности; 3.Механизм управления потоками информации.

РАБОТА No 3. Тестовые испытания программных средств защиты.

Индивидуальные задачи:

1. Механизм обеспечения безопасности информации при взаимодействии сетям и общего пользования;
2. Механизм шифрования (преобразования) информации; 3.Механизм контроля и аудита безопасности.

РАБОТА No 4. Тестовые испытания программных средств защиты.

Индивидуальные задачи:

1. Механизм архивирования и дублирования критичной информации;
2. Механизм формирования и проверки подлинности ЭЦП (при их использовании);3.Механизм восстановления средств защиты информации.

РАБОТА No 5.

Тестовые испытания программных средств защиты. Индивидуальные задачи:

1. Механизм сигнализации попыток нарушения защиты;

2. Механизм обнаружения «злонамеренного кода»;
3. Механизм антивирусной защиты;
4. Механизм управления сертификатами (при использовании PKI системы).

РАБОТА No 6. Защита от утечек по каналу ПЭМИН, по акустическом у и виброакустическому каналам.

Индивидуальные задачи:

1. Измерение ПЭМИ рабочих станций (АРМ) пользователей, серверов, устройств вывода (ввода) информации, коммуникационного оборудования и кабельных соединений;
2. Измерение наводок информационных сигналов на вспомогательные средства, имеющие выход за пределы контролируемой зоны;
3. Измерение наводок информационных сигналов на кабельное и коммуникационноеоборудование.

РАБОТА No 7. Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам.

Индивидуальные задачи:

1. Измерение звукоизоляции выделенных помещений;
2. Измерение виброизоляции выделенных помещений;
3. Измерение электроакустических преобразований вспомогательных технических средств;

РАБОТА No 8. Анализ сетевой топологии установленных сервисов. Индивидуальные задачи:

1.Определение сетевой топологии системы;

2.Определение внутренней доменной структуры сети.

РАБОТА No 9.

Анализ сетевой топологии установленных сервисов. Индивидуальные задачи:

1.Определение информации о конфигурации топологии системы;

2. Определение текущей логической структуры корпоративной сети.

РАБОТА No 10. Сетевое сканирование. Индивидуальные задачи:

1.Сканирование TCP-портов функцией connect;

2.Сканирование с использованием ICMP echo-пакетов;

3.SYN-сканирование TCP-портов.

РАБОТА No 11. Сетевое сканирование. Индивидуальные задачи:

1. FIN-сканирование TCP -портов;
2. Сканирование с использованием фрагментации;
3. Обратное IDENT-сканирование.

РАБОТА No 12. Сетевое сканирование. Индивидуальные задачи:

1.FTP bounce-сканирование;

2.UPD-сканирование;

3.Определение списка открытых и закрытых портов.

РАБОТА No 13. Сетевое сканирование. Индивидуальные задачи:

1.Определение списка имеющихся средств межсетевого экранирования;

2.Определение признаков работы сервисов по нестандартным портам;

3.Определение типов используемых операционных систем.

РАБОТА No 14. Анализ трафика и сбор критичной информации программами пассивного анализа.

Индивидуальные задачи:

1. Получение информации об используемых аутентификационных протоколах, процедурахдоступа;

2. Обнаружение в открытом трафике передаваемых регистрационных имен,

3. Идентификаторы и пароли пользователей, определение текстовых паролей, пароли на доступ вудаленные системы;

4. Проверка паролей, используемых при аутентификации службами SMB, POP3, IMAP, Telnet,HTTP, FTP.

РАБОТА No 15. Анализ трафика и сбор критичной информации программами пассивного анализа.

Индивидуальные задачи:

1. Определение почтовых ящиков на общедоступных почтовых серверах;

2. Анализ почтового трафика на предмет выявления писем, отвечающих определеннымпризнакам;

3. Диагностика проблем при сетевом обмене хостов.

РАБОТА No 16. Анализ трафика и сбор критичной информации программами пассивного анализа.

Индивидуальные задачи:

1.Проверочная рассылка электронной почты со служебными заголовками;

2.Определение свойств реализации стека TCP;

3. Определение маршрутов хождения пакетов;

4. Тестированиеп равильности настроек систем контроля трафика.

РАБОТА No 17. Обнаружение уязвимостей по сигнатурам.

Индивидуальные задачи:

1. Определение слабых мест в защите сервисов: FTP, TFTP, SSH, Finger, HTTP, IMAPSMTP, NetBIOS/SMB, RPC;

2. Выявление слабых мест сетевых информационных служб (NIS);

3. Проверка на возможность IP-спуфинга;
4. Проверка маршрутизации из источника rlogin, rsh и telnet.

РАБОТА No 18. Обнаружение уязвимостей по сигнатурам.
Индивидуальные задачи:
1.Проверка IP-переадресации (forwarding);
2.Проверка сетевых масок и временных меток (timestamp) ICMP;
3.Проверка инкапсуляции пакета MBONE;
4.Проверка инкапсуляции APPLETALK IP, IPX, X.25, FR.

РАБОТА No 19. Обнаружение уязвимостей по сигнатурам.
Индивидуальные задачи:
1.Проверка резервированных разрядов и паритет-протоколов;
2.Проверка специализированных фильтров;
3. Проверка фильтров с возможностью нулевой длины TCP и IP;
4. Проверка на передачу сверх нормативных пакетов.

РАБОТА No 20. Обнаружение уязвимостей по сигнатурам
Индивидуальные задачи:
1.Проверкаопций post-EOL дляTCPи IP;
2. Проверка наличия в Web-сервисах уязвимых сценариев, на базе BasicScript, JavaScript,Perl и ActiveXo;
3. Проверка программного обеспечения на закрытие всех известных уязвимостей данной платформы.

Контрольные вопросы для самоконтроля

Тема 1. Проблемы информационной безопасности сетей.

1. Классификация угроз информационной безопасности автоматизированных систем.
2. Назначение и структура стека протоколов TCP/IP. Характеристика протокола TCP/IP с точки зрения информационной безопасности.
2. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: подслушивание (sniffing), подмена доверенного субъекта (IP – spoofing), посредничество в обмене незашифрованными ключами (Man-in-the-Middle).
4. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: перехват сеанса (Sessionhijacking), отказ в обслуживании (DenialofService, DoS), парольная атака полного перебора (bruteforceattack).
5. Основные цели и характерные особенности сетевых атак. Виды сетевых атак: угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием.
6. Основные характеристики спама и методы борьбы с ним.
7. Виды интернет- мошенничества: фишинг и фарминг и методы борьбы с ними.
8. Угрозы и уязвимости проводных корпоративных сетей.
9. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: вещание радиомаяка, обнаружение WLAN, подслушивание, ложные точки доступа в сеть.
10. Особенности построения и актуальность защиты беспроводных сетей. Виды сетевых атак: отказ в обслуживании, атаки типа “ человек в середине”, атака подмены ARP-записей, анонимный доступ в Интернет.
11. Способы обеспечения информационной безопасности компьютерных сетей. Фрагментарный и комплексный подходы.
12. Пути решения проблем защиты информации в сети Интернет. Информационная безопасность электронного бизнеса.

Тема 2. Политика безопасности.

13. Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности.
14. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности.

15.Основные этапы разработки политики безопасности.

Тема 3. Технологии аутентификации.

16. Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе паролей.

17. Аутентификация на основе PIN-кода.

18. Строгая аутентификация. Примеры протоколов аутентификации.

19. Биометрическая аутентификация пользователя.

20. Электронные системы идентификации и аутентификации.

21. Комбинированные системы идентификации и аутентификации.

Тема 4. Технологии межсетевых экранов.

22. Основные функции и дополнительные возможности межсетевых экранов. Политика работы МЭ.

23. Особенности функционирования межсетевых экранов на уровнях модели OSI. Варианты исполнения МЭ.

24. Основные схемы подключения межсетевых экранов.

Тема 5. Технологии защиты от вирусов.

25. Понятие компьютерного вируса. Классификация вирусов.

26. Специализированные утилиты для борьбы с вредоносным ПО: антишпионы, антируткиты и антикейлоггеры.

27. Троянские программы. Виды троянских программ.

28. Компьютерные черви. Виды компьютерных червей.

29. Методы борьбы с вирусами: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”

30. Методы борьбы с вирусами: обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ, метод резидентных мониторов.

31. Антивирусные программы: утилита Dr. WebCurelt, программа Dr. Web., антивирус AviraAntiVirPersonal, антивирус Avast! HomeEdition.

32. Популярные пакеты антивирусной защиты: пакеты компании ESET(ESETNOD32 Antivirus, ESETNOD32 SmartSecurity), пакеты “Лаборатории Касперского” (Антивирус Касперского, KasperskyInternetSecurity, KasperskyMobileSecurity).

Тема 6. Технологии анализа защищенности и обнаружения сетевых атак.

33 . Концепция адаптивного управления безопасностью.

34. Средства анализа защищенности и общие требования к ним.

35. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак.

36. Обзор современных средств обнаружения атак. Продуктыкомпании Internet Security Systems. Продукты компании CiscoSystems.

Тема 7. Требования к системам защиты информации.

37. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Показатели защищенности межсетевых экранов.

38. Классы защищенности автоматизированных систем.

39.Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Защита конфиденциальной информации в АС и на рабочих местах пользователей ПК.

40.Требования к защите информации в локальных вычислительных сетях и при межсетевом взаимодействии. Требования к защите информации при работе с системами управления базами данных.

41.Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

Тема 8. Аудит безопасности информационных систем.

42. Понятие аудита безопасности информационных систем и цели его проведения. Стандарты, используемые при проведении аудита.

43. Основные этапы проведения аудита безопасности информационных систем .

44. Анализ рисков и управление рисками. Методы оценки рисков и уровня защиты информационных систем.

45. Обзор программных продуктов для анализа и управления рисками: GRAMM, RiskWath, COBRA, ПО компании MethodWare, ПО “Аван Гард”.

Тема 9. Разработка и защита Web – сайтов.

46. Защита информации сайта от несанкционированного доступа с помощью аутентификации.

47. Защита контента сайта от несанкционированного копирования.

48. Методы защиты сайта от DDos – атак.

Список литературы

1) Пролубников, А. В. Сети передачи данных : учебное пособие : в 2 частях / А. В. Пролубников. – Омск : Омский государственный университет им. Ф.М. Достоевского, 2020. – Ч. 1. – 116 с. – URL: https://biblioclub.ru/index.php?page=book&id=614062 . – Режим доступа: по подписке. – Текст : электронный.

2) Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.– URL: https://biblioclub.ru/index.php?page=book&id=429035. –Режим доступа: по подписке. – Текст : электронный.

3) Васяева, Н. С. Проектирование локальных вычислительных сетей: учебное пособие для курсового проектирования / Н. С. Васяева, Е. С. Васяева. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 94 с.– URL: https://biblioclub.ru/index.php?page=book&id=560566. – Режим доступа: по подписке. – Текст : электронный.

4) Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. – Минск : РИПО, 2019. – 180 с.– URL: https://biblioclub.ru/index.php?page=book&id=599948. – Режим доступа: по подписке. – Текст : электронный.

5) Сети и системы телекоммуникаций: учебное электронное издание / В. А. Погонин, А. А. Третьяков, И. А. Елизаров, В. Н. Назаров. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 197 с.– URL: https://biblioclub.ru/index.php?page=book&id=570531 . – Режим доступа : по подписке. – Текст : электронный.

6) Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с.– URL: https://biblioclub.ru/index.php?page=book&id=429032. – Режим доступа: по подписке. – Текст : электронный.