ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Кибербезопасность информационных систем»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ

К ВЫПОЛНЕНИЮ
КУРСОВЫХ РАБОТ ПО ДИСЦИПЛИНЕ

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Авторы
Короченцев Д.А.,
Гончаров Р.А.,
Болдырихин Н.В.

Ростов-на-Дону, 2018

Аннотация

Методические рекомендации и организационные требования к выполнению курсовых работ по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов очной формы обучения по направлению подготовки 10.05.01 «Компьютерная безопасность» представляют собой комплекс заданий и разъяснений, позволяющих студентам оптимальным образом организовать процесс выполнения курсовой работы.

Авторы

кандидат технических наук,
доцент кафедры «Кибербезопасность информационных систем»
Короченцев Д.А.

доцент, кандидат технических наук,
доцент кафедры «Техническая эксплуатация летательных аппаратов и наземного оборудования»
Гончаров Р.А.

доцент, кандидат технических наук,
доцент кафедры «Кибербезопасность информационных систем»
Болдырихин Н.В.

Оглавление

1. ВВЕДЕНИЕ

1.1. Цели освоения дисциплины «Организационное и правовое обеспечение информационной безопасности»

Дисциплина «Организационно-правовое обеспечение информационной безопасности» имеет целью раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

Данная дисциплина, как составная часть науки «Информационное право», является правовым фундаментом информационного общества, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов.

1.2. Задачи дисциплины «Организационное и правовое обеспечение информационной безопасности»:

1) изучение теоретических вопросов, основных понятий, определений и категорий, используемых в данной дисциплине, формирование базовых навыков по их применению;
2) формирование базовых знаний по основам построения систем информационной безопасности;
3) изучение предпосылок формирования правовых отношений в информационной сфере;
4) ознакомление с перечнем основных нормативных правовых документов, применяемых в области информационной безопасности;
5) подробное изучение отдельных нормативных правовых документов, применяемых в области информационной безопасности:
6) изучение программных средств, применяемых для проведения аудита информационной безопасности;
7) применение полученных знаний на практике для проведения аудита информационной безопасности на предприятии.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения.

В соответствии с ГОС ВПО в результате изучения дисциплины студенты должны:

– Овладеть способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства получить представление о теории конечных автоматов;

– Овладеть способностью использовать нормативные правовые документы в своей профессиональной деятельности;

– Овладеть способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам

обеспечения информационной безопасности компьютерных систем;

– Овладеть способностью проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;

– Овладеть способностью участвовать в разработке проектной документации;

– Овладеть способностью обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения.

2. ТЕМЫ КУРСОВЫХ РАБОТ

Курсовая работа выполняется по темам дисциплины в соответствии с вариантом. Номер варианта соответствует номеру в журнале группы.

1. **Предметная область информационной безопасности.** Понятие информационной безопасности, понятие и классификация, виды угроз. Характеристика средств и методов защиты информации от случайных угроз, от угроз несанкционированного вмешательства. Криптографические методы защиты информации и межсетевые экраны. [10,14,36,38,40,42,48,49,80,83]
2. **Основные методы атак на информацию и способы защиты от компьютерных злоумышленников.** Системы и технологии информационной безопасности, определение угроз и управление рисками. Понятие криптосистемы, построение антивирусной защиты и работа брандмауэров. [2,5,10,17,18,30,32,33,41,50,84]
3. **Способы и методы защиты информационных ресурсов.** Основные понятия защиты информации и информационной безопасности. Классификация и содержание, источники и предпосылки появления возможных угроз информации. Основные направления защиты от информационного оружия (воздействия), сервисы сетевой безопасности. [7,13,21,23-25,28,42,44,52,82,84]
4. **Защита интересов личности, общества и государства при обмене данными в сети Интернет.** Особенности интересов государства в информационной сфере. Проблемы правового регулирования защищенности этих интересов при обмене данными в сети Интернет. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности. [1,3,64,66,68,70,76,78,82,84]
5. **Построение системы активного отражения атак в корпоративных сетях.** Описание информационных технологий и модель угроз. Средства защиты периметра сети, межсетевые экраны. Системы обнаружения вторжений, их классификация по уровням информационной системы. Подходы к автоматическому отражению атак и предотвращению вторжений. [4,9,23-25,34,48,49,60,67,71,78]
6. **Концепция защиты информации, записанной на энергонезависимых электронных носителях от несанкционированного копирования и распространения.** Виды и характеристики современных средств защиты. Устойчивость к взлому. Лицензирование. Системы защиты энергонезависимых электронных носителей.[6,7,19,34,37,45,47,51,53,54,57]
7. **Функции, задачи и особенности службы безопасности организации.** Принципы организации службы безопасности организации. Типовая структура службы безопасности. Задачи и функционал службы безопасности организации [8,27,30,32,33,34,42,69,73,83]
8. **Защита информации от несанкционированного доступа.** Средства обеспечения информационной безопасности. Возможные каналы утечки информации. Защита данных с помощью шифрования. Обзор видов технических устройств, защищающих системы, и принцип их действия. Программно-аппаратный комплекс средств защиты.[27,35,36,39,43,45,47,56-67,71]
9. **Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.** Порядок формирования режима государственной тайны. Основные регуляторы в области защиты сведений, составляющих государственную тайну. Порядок допуска организаций к проведению работ. Ответственность за нарушения порядка обращения со сведениями, составляющими государственную тайну.[5,20,34,36,37,56-67,76,77,81,84]

10. Виды тайн, законодательно закрепленные в Российской Федерации. Понятие тайны, виды тайн. Отличительные особенности обращения с различными видами тайн. Ответственность за нарушения режима безопасности при обработке сведений, составляющих один из видов тайн.[3,31,36,37,68,69,75-79]

11. Концептуальные основы защиты информации к автоматизированных системах. Порядок разработки и построения автоматизированных систем. Защищенные автоматизированные системы. Организация хранения информации. Классификация вирусов, пути их проникновения и проявление в работе компьютера.[3,5,11,13-16,21,22-25,29,42,55,62,63,74]

12. Проблемы защиты информации в интернете. Сравнительная характеристика способов защиты информации от вирусов и несанкционированного доступа. Методы атак на защищаемую информацию и ресурсы. [1,3,64,66,68,70,76,78,82]

13. Законодательные основы компьютерной безопасности. Неправомерный доступ к информации, хранящейся на компьютере. Создание, использование и распространение вредоносных программ. [3,5,31,34,36,68,69,71,75-79,83,84]

14. Ответственность за правонарушения и преступления в области защиты информации и информационной безопасности. Место и роль в современном обществе информационных технологий. Определение компьютерного преступления в соответствии с действующим уголовным законодательством Российской Федерации. Ответственность за правонарушения в сфере информационных технологий.[3,7,8,34,36,39,54,71,72,75-79,84-86]

15. Информация: сбор, защита, анализ. Методика информационно-аналитической работы, ее содержание. Работа с источниками информации. Способы ее оценки, обеспечение безопасности и защиты. Элементы системы безопасности. Методы и средства обеспечения информационной безопасности организации. [3,5,31,34,36,68,69,71,75-79,83,84-86]

16. Стандарты информационной безопасности. Отличительные особенности стандартизации автоматизированных, компьютерных, телекоммуникационных систем. Сравнительный анализ отечественных и зарубежных стандартов в рассматриваемых областях.[6,8,17-19,30-33,36,41,44,68,69]

17. Защита информации в системах реального времени. Проблемы защиты информации в компьютерных системах. Принципы защиты информации. Методы решения проблем защиты электронной информации. [3,5,11,13-16,21,22-25,29,42,55,62,63,74]

18. Классификация сбоев в системах телекоммуникаций. Определение и анализ причин нарушения нормального функционирования систем телекоммуникаций. Пошаговая методика построения системы защиты информации. Физическая защита данных. [3,5,11,13-16,21,22-25,29,42,55,62,63,74]

19. Концепция безопасности и система защиты информации. Понятие и состав научно-методологических основ обеспечения информационной безопасности. Основные положения теории систем. Содержание принципов организации комплексной системы защиты информации, предъявляемые к ней требования и порядок работ при создании. [3,5,31,34,36,68,69,71,75-79,83,84]

20. Требования к защите информации от несанкционированного доступа. Анализ научно-методологических основ обеспечения информационной безопасности и формирование требований к функциям безопасности, реализуемым системой. Компоненты системы защиты информации в компьютерных системах. [27,35,36,39,43,45,47,56-67,71]

21. Определение возможных угроз и уязвимостей защиты информации в системе электронных платежей. Анализ технологий обработки информации.

Построение системы защиты информации, порядок контроля за ее состоянием, определение и анализ угроз. Техническая защита банковских операций. [27,35,36,39,43,45,47,56-67,71]

22. Виды и источники угроз информационной безопасности. Классы каналов несанкционированного получения информации. Виды угроз информационным системам. Причины нарушения целостности информации. Потенциально возможные действия злоумышленника (модель нарушителя). [3,5,31,34,36,68,69,71,75-79,83,84-86]

23. Защита информации в телефонных сетях. Виды угроз в телефонных сетях. Потенциально возможные злоумышленные действия. Факторы, влияющие на требуемый уровень защиты информации. Методы и средства обеспечения безопасности в каналах телефонной связи. Рекомендации по увеличению уровня защищенности. [1,3,64,66,68,70,76,78,82]

24. Защита персонального компьютера от несанкционированного доступа к информации в базах данных. Архитектура защиты Access. Система безопасности SQL Server. Пользователи базы данных. Ограничение доступа пользователей к данным. [3,5,11,13-16,21,22-25,29,42,55,62,63,74]

25. Понятие безопасности информационной системы и угроз, которым она подвержена. Пути несанкционированного доступа к информации. Причины возникновения каналов утечки. Методы обеспечения безопасности информации. Кодирование, шифрование и защита данных. [2,5,10,17,18,30,32,33,41]

26. Обеспечение безопасности данных в современных СУБД (Microsoft Access, MS SQL Server, Oracle 7). Особенности юридической защиты авторских прав на базы данных. [3,5,11,13-16,21,22-25,29,42,55,62,63,74]

27. Характеристика развития средств и методов защиты информации, а также основных этапов их развития. Анализ структуры систем, применяемых в общемировой практике обеспечения информационной безопасности. [2,5,10,17,18,30,32,33,41]

28. Проблемы информационной безопасности, цели применения радиоэлектронного шпионажа. Способы перехвата информации, передаваемой по радиоэлектронным каналам связи. Методы ее защиты на энергетическом уровне. Виды помех, используемых для защиты информации. [3,7,21,22-27,35,36,39,44,47,56-67,71].

3. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ ПО ВЫПОЛНЕНИЮ И ОФОРМЛЕНИЮ КУРСОВОЙ РАБОТЫ

Требования по выполнению и оформлению курсовой работы приведены в документе «Правила оформления и требования к содержанию курсовых проектов (работ) и выпускных квалификационных работ» ДГТУ, введенного приказом от 30.12.2015 г. № 227, расположенном на сайте университета во вкладке:

Образование/Методическое обеспечение/Документы (http://cme.dstu.edu.ru/index.php?action=pages&id=104).

Тема курсовой работы (её объем – от 30 до 40 машинописных страниц без учета приложений) соответствует одной из представленных тем курсовых работ (алгоритм выбора темы курсовой работы приведен в разделе 2 настоящих Методических рекомендаций).

На основе курсовой работы готовится выступление по рассматриваемой проблеме на 5-7 минут.

В общем случае структура курсовой работы включает в себя: титульный лист, содержание, введение, разделы основной части, заключение, список использованных источников и приложения (при наличии).

На титульном листе указываются:

1) полное наименование учебного заведения,
2) факультет,
3) кафедра,
4) учебная дисциплина,
5) тема работы,
6) курс,
7) группа,
8) фамилия, имя, отчество студента и руководителя работы,
9) название города, в котором находится учебное заведение,
10) год написания работы.

В среднем поле дается заглавие курсовой работы, которое проводится без слова "тема" и в кавычки не заключается. Далее, ближе к правому краю титульного листа, указываются фамилия, инициалы студента, написавшего курсовую работу, а также его курс и группа. Ниже или слева указываются фамилия и инициалы преподавателя - руководителя работы. В нижнем поле указывается год написания курсовой работы.

После титульного листа помещают раздел **«СОДЕРЖАНИЕ»**, в котором приводятся все заголовки работы и указываются страницы, с которых они начинаются. Заголовки разделов должны точно повторять заголовки в тексте. Сокращать их или давать в другой формулировке и последовательности **нельзя**.

Все заголовки начинаются с прописной буквы без точки на конце. Последнее слово каждого заголовка соединяют многоточием / ..... / с соответствующим ему номером страницы в правом столбце оглавления. Заголовки одинаковых ступеней рубрикации необходимо располагать друг под другом. Заголовки каждой последующей ступени смещают на три-пять знаков вправо по отношению к заголовкам предыдущей ступени.

В разделе **«ВВЕДЕНИЕ»** аргументируется актуальность выбранной темы, указываются цели и задачи исследования. В нем также отражается методика исследования и структура работы. Актуальность предполагает оценку своевременности и социальной значимости выбранной темы, обзор литературы по теме отражает знакомство автора курсовой работы с имеющимися источниками, умение их систематизировать,

критически рассматривать, выделять существенное, определять главное.

Основная часть работы предполагает освещение материала в соответствии с планом. Обзор литературы начинается с ознакомления с первоисточниками: исторические, ***законодательные и нормативные акты***, статистические сборники. После этого можно приступить к изучению монографий, научно-исследовательской литературы, затрагивающих данную проблему. Взгляды наиболее видных ученых должны быть кратко проанализированы и сопоставлены. Основной текст желательно разбивать на главы и параграфы. Содержание глав этой части должно точно соответствовать теме работы и полностью ее раскрывать. Эти главы должны показать умение исследователя сжато, логично и аргументировано излагать материал, обобщать, анализировать, делать логические выводы.

В разделе **«ЗАКЛЮЧЕНИЕ»** излагаются основные выводы и рекомендации по теме исследования. Предполагается последовательное, логически стройное изложение обобщенных выводов по рассматриваемой теме.

Раздел **«СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ»** оформляется в соответствии с ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления».

Ссылка на использованный литературный источник в тексте может быть представлена как сноска либо посредством указания его номера в квадратных скобках после изложения источника. Этот номер должен соответствовать порядковому номеру из раздела «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ», например, [13].

В работах используются следующие способы построения библиографических списков: по алфавиту фамилий, авторов или заглавий; по тематике; по видам изданий; по характеру содержания; списки смешанного построения.

Литература в списке указывается в алфавитном порядке (более распространенный вариант). После указания фамилии и инициалов автора указывается название литературного источника, место издания (пишется сокращенно, например, Москва - М., Санкт - Петербург - СПб ит.д.), название издательства (например, Мир), год издания (например, 2015), можно указать страницы (например, с. 54-67). Страницы можно указывать прямо в тексте, после указания номера, под которым литературный источник находится в списке литературы (например, 7) номер литературного источника, (с. 67- 89). Номер литературного источника указывается после каждого нового отрывка текста из другого литературного источника.

В списке использованных источников должно быть не менее 12 различных источников.

В разделе **«ПРИЛОЖЕНИЯ»** помещают вспомогательные или дополнительные материалы, которые загромождают текст основной части работы (таблицы, карты, графики, неопубликованные документы, переписка и т.д.). Каждое приложение должно начинаться с нового листа, страницы с указанием в правом верхнем углу слова "Приложение" и иметь тематический заголовок. При наличии в работе более одного приложения они нумеруются арабскими цифрами, без знака "№", например, "Приложение 1". Нумерация страниц, на которых даются приложения, должна быть сквозной и продолжать общую нумерацию страниц основного текста. Связь основного текста с приложениями осуществляется через ссылки, которые употребляются со словом "смотри", оно обычно сокращается и заключается вместе с шифром в круглые скобки - (см. прил. 1).

Все страницы работы, включая содержание и список использованных источников, нумеруются по порядку с титульного листа (на нем цифра не ставится) до последней страницы без пропусков и повторений. Введение, заключение, новые главы, список использованных источников должны начинаться с нового листа. Подбор лите-

ратуры производится студентом из предложенного преподавателем списка литературы, допускается использование дополнительной литературы.

Разделы «СОДЕРЖАНИЕ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ», «ПРИЛОЖЕНИЯ» не имеют номеров, оформляются полужирным шрифтом Times New Roman, размером 14 pt и начинаются с новой страницы.

Текст курсовой работы необходимо набирать на компьютере на одной стороне листа. Размер левого поля 20 мм, правого – 10 мм, верхнего – 20 мм, нижнего – 20 мм. Шрифт – Times New Roman, размер – 14, межстрочный интервал – 1,5. Фразы, начинающиеся с новой строки, печатаются с абзацным отступом от начала строки.

Курсовая работа, выполненная небрежно, неразборчиво, без соблюдения требований по оформлению, возвращается студенту без проверки с указанием причин возврата на титульном листе.

4. ЗАЩИТА КУРСОВЫХ РАБОТ

Защита курсовой работы является обязательной формой проверки выполнения работы. Защита производится на научном семинаре при непосредственном участии руководителя, в присутствии студентов. Результаты наиболее интересных курсовых работ (проектов) могут быть доложены на научных конференциях.

Публичная защита стимулирует научный интерес, творчество, ответственность студентов.

При выполнении и защите курсовой работы студент должен продемонстрировать:

- владение соответствующим понятийным и терминологическим аппаратом;
- знакомство с основной литературой;
- умение выделить проблему и определить методы её решения;
- умение последовательно изложить существо рассматриваемых вопросов.

Защита курсовой работы студентом предусматривает доклад по выбранной тематике не более 5-7 минут, ответы на вопросы оппонентов. Вопросы задаются присутствующими на защите преподавателями и студентами. Результаты защиты курсовой работы, оцениваются дифференцированной отметкой по пятибалльной системе. Оценка курсовой работы записывается в ведомость, которая представляется в деканатах факультета.

После выставления оценки руководителем курсовой работы составляется рецензия.

Студент, не представивший в установленный срок курсовую работу или не защитивший ее по неуважительной причине, считается имеющим академическую задолженность.

Курсовые работы, представляющие теоретический и практический интерес, следует представлять на конкурс в студенческие научные общества, конференции, отмечать приказом по университету.

Выполненные работы после их защиты хранятся на кафедре, в конце текущего года составляется опись в соответствии с которой курсовые работы сдаются в архив.

Итоги выполнения курсовых работ (проектов) ежегодно обсуждаются на кафедрах и по мере необходимости на Ученых советах факультетов, а в отдельных случаях и на заседаниях Ученого Совета университета.

5. ДОПУСК К ЗАЩИТЕ И КРИТЕРИИ ОЦЕНКИ КУРСОВОЙ РАБОТЫ

Для формального допуска к защите курсовой работы студенту (слушателю) достаточно сдать один экземпляр готовой курсовой работы на кафедру за 7 дней до официального срока защиты. Курсовая работа должна быть подписана самим студентом и проверена и завизирована руководителем. ***Для подтверждения оригинальности текста – не менее 70%, подшивается отчет о проверке текста курсовой работы в системе «Антиплагиат»***. Руководитель ставит число, когда была проверена работа, свою фамилию и инициалы, резолюцию (рекомендуется или не рекомендуется к защите данная работа) и рекомендуемую оценку.

На защите запрещено чтение текста курсовой работы.

1. Отметке ***«отлично»*** соответствует курсовая работа, в которой:

А) соблюдены все требования, предъявляемые к оформлению текстовой части и содержанию;

Б) при защите которой автору удалось полно и качественно довести содержание работы членам комиссии и коллегам, выгодно устно и визуально представить работу;

В) полно ответить на все поступившие вопросы, касающиеся проблематике, рассмотренной в курсовой работе.

2. Отметке ***«хорошо»*** соответствует работа, в которой допущены:

А) незначительные ошибки в оформлении (например, неправильно оформлены библиографические ссылки);

Б) незначительные ошибки в содержании работы;

В) недочеты в презентации работы (на пример, студенту не удалось за отведенное время представить результаты работы комиссии);

Г) ошибки при ответах на вопросы, возникшие в процессе защиты.

3. Отметке ***«удовлетворительно»*** соответствует работа, в которой не выполнены требования для получения отметки «хорошо» и при защите которой студент (слушатель) не смог представить полученные результаты (запутался в собственных результатах и выводах) или не смог ответить на ряд вопросов членов комиссии.

4. Отметке ***«неудовлетворительно»*** соответствует работа с одним или несколькими из ниже приведенных серьезных замечаний:

А) имеют место грубые ошибки содержательного плана;

Б) курсовая работа формально не соответствует описанным выше требованиям;

В) во время презентации работы студент (слушатель) продемонстрировал слабое владение предметом, не ориентируется в собственном исследовании;

Г) не было получено ответов на большинство вопросов заданных студенту (слушателю) членами комиссии.

СПИСОК ЛИТЕРАТУРЫ

1. Information Security. Информационная безопасность. Электронный журнал, http://www.itsec.ru
2. Афанасьев А.Л., Веденьев Л.Т., Воронцов А. А., Газизова Э.Р. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебное пособие для вузов. — Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. — М.: Горячая линия-Телеком, 2012. — 552 с.
3. Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации М.: Издательский Центр РИОР: ООО "Научно-издательский центр ИНФРА-М", 2017.
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.
5. Безбогов, А.А. Безопасность операционных систем : учебное пособие / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. – М.: "Издательство Машиностроение-1", 2007. – 220 с.
6. Галатенко В.А. Стандарты информационной безопасности Москва: Национальный открытый Университет "ИНТУИТ", 2016.
7. Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов на Дону: Феникс, 2010. – 324 с.
8. Городов О.А. Информационное право: учебник / О. А. Городов. – М.: Проспект, 2009. – 242 с.
9. ГОСТ 19781-90. Обеспечение систем обработки информации программное. Термины и определения.
10. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
11. ГОСТ 28195-89. Оценка качества программных средств. Общие положения.
12. ГОСТ 28806-90. Качество программных средств. Термины и определения.
13. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения
14. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
15. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
16. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем.
17. ГОСТ ISO 9000-2011. Системы менеджмента качества. Основные положения и словарь.
18. ГОСТ ISO 9001-2011. Системы менеджмента качества. Требования.
19. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
20. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
21. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
22. ГОСТ Р 51318.22-2006. Совместимость технических средств электромагнитная. Оборудование информационных технологий. Радиопомехи индустриальные. Нор-

мы и методы испытаний (взамен ГОСТ 29216-91).

23. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения

24. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

25. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.

26. ГОСТ Р 53112-2008. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.

27. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

28. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.

29. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.

30. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

31. ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

32. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

33. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

34. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений/
В. Г. Грибунин, В.В. Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

35. Казарин О.В., Забабурин А.С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для вузов. СПб.: Питер, 2018.

36. Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности/Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.

37. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. М.: Горячая линия – Телеком, 2012. — 140 с.

38. Консультант Плюс http://www.consultant.ru/

39. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации: Учебное пособие для студентов высших учебных заведений. - М.: Академия, 2006. - 256 с.

40. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11.02.2014 года.

41. Нестеров С.А. Основы информационной безопасности: Учебное пособие. — 3-е изд., стер. — СПб.: Издательство «Лань», 2017. — 324 с.

42. Никифоров С.Н. Защита информации. Защита от внешних вторжений. СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, 2017.

43. Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282

44. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М.: Горячая линия - Телеком, 2006. - 544 с.

45. Панов А.С. Реверсинг и защита программ от взлома – БХВ-Петербург, 2006. – 243 с.

46. Пирогов В.Ю. Ассемблер и дизассемблирование БХВ-Петербург, 2006. - 466 стр.

47. Проскурин В.Г. Защита программ и данных: Учебное пособие. – 2-е изд., стер. — М. Издательский центр «Академия», 2012.

48. Профиль защиты систем обнаружения вторжений уровня сети четвертого-шестого классов защиты ИТ.СОВ.С4-5.ПЗ. Утвержден ФСТЭК России 03.02.2012 года.

49. Профиль защиты систем обнаружения вторжений уровня узла четвертого-шестого классов защиты ИТ.СОВ.У4-6.ПЗ. Утвержден ФСТЭК России 03.02.2012 года.

50. Профиль защиты средств антивирусной защиты типа «А» четвертого класса защиты. Утвержден ФСТЭК России 14.06.2012 года.

51. Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.Н4.ПЗ. Утвержден ФСТЭК 01.12.2014 года.

52. Р 50.1.053-2005. Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации.

53. Р 50.1.056-2005. Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.

54. Расторгуев С.П. Основы информационной безопасности: учеб.пособ. для студ.вузов / С.П. Расторгуев. - М: Академия, 2009. - 192с.

55. РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения.

56. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

57. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992

58. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утвержден решением председателя Гостехкомиссии России от 30.03.1992 года.

59. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992 г.

60. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30.03.1992 года.

61. Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню

контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. № 114

62. Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 04.06. 1999 N 114.

63. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

64. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992 года.

65. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

66. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992

67. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 25.07.1997 года.

68. Сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. http://rkn.gov.ru

69. Сайт ФСТЭК http://fstec.ru

70. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18.02.2013 N 21.

71. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: уч. пособие для студентов ВУЗ – М. Издательский центр «Академия», 2008

72. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. Москва: ФГБОУ ВО «РЭУ им. Г. В.Плеханова», 2017. – 207 с.

73. Титов А.А. Инженерно-техническая защита информации: Учебное пособие: Томск, ТГУСИР, 2010. – 197 с.

74. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17.

75. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

76. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

77. Федеральный закон от 02 июля 1993 г. № 5481-1-ФЗ «О государственной тайне».

78. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ

«Об информации, информационных технологиях и о защите и информации».

79. Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

80. Федотова Е. Л. Информационные технологии и системы: учеб. пособие для вузов / Е. Л. Федотова. – М.: ФОРУМ: ИНФРА-М, 2013. – 351 с.

81. Цирлов В.Л. Основы информационной безопасности: краткий курс/ В.Л. Цирлов. – Ростов-на-Дону: Феникс, 2008.

82. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. - М.: ИД «ФОРУМ»: ИНФРА-М, 2011. - 416 с.

83. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2010. — 544 с.

84. "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ (ред. от 23.04.2018, с изм. от 25.04.2018).

85. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ (ред. от 23.04.2018).

86. "Трудовой кодекс Российской Федерации" от 30.12.2001 № 197-ФЗ (ред. от 05.02.2018).