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

А. Г. Жестовский

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по выполнению лабораторных работ
для студентов специальности
10.05.03 – Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

Рецензент:
заведующий кафедрой информационной безопасности
Института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»,
кандидат физико-математических наук, доцент
Н. Я. Великите

Жестовский, А. Г.

Основы информационной безопасности: учебно-методическое пособие по выполнению лабораторных работ для студентов специальности 10.05.03 – Информационная безопасность автоматизированных систем / А. Г. Жестовский. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 32 с.

В учебно-методическом пособии необходимый теоретический и справочный материал для выполнения лабораторных работ.

Содержит общие методические указания для выполнения задач, а также теоретические сведения о системах защиты информации. Теоретический материал закрепляется выполнением лабораторных работ, которые содержат элементы исследовательской деятельности.

Список литературы – 13 наименований

Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» 10.05.03 – Информационная безопасность автоматизированных систем.

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры ИБ ФГБОУ ВО «Калининградский государственный технический университет» 30.06.2023, протокол № 11.

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 05.07.2023, протокол № 8.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

На сегодняшний день автоматизированные системы являются основой обеспечения практически любых бизнес-процессов, как в коммерческих, так и в государственных организациях. Вместе с тем повсеместное использование автоматизированных систем для хранения, обработки и передачи информации приводит к обострению проблем, связанных с их защитой. Подтверждением этому служит тот факт, что за последние несколько лет, как в России, так и в ведущих зарубежных странах имеет место тенденция увеличения числа информационных атак, приводящих к значительным финансовым и материальным потерям.

Считается, что одной из наиболее опасных угроз является утечка хранящейся и обрабатываемой внутри автоматизированных систем конфиденциальной информации. Как правило, источниками таких угроз являются недобросовестные или ущемлённые в том или ином аспекте сотрудники компаний, которые своими действиями стремятся нанести организации финансовый или материальный ущерб. Всё это заставляет более пристально рассмотреть, как возможные каналы утечки конфиденциальной информации, так и ознакомиться со спектром технических решений, позволяющих предотвратить утечку данных.

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями. Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя, таким образом, информационные технологии.

Субъекты производственно-хозяйственных отношений вступают друг с другом в информационные отношения (отношения по поводу получения, хранения, обработки, распределения и использования информации) для выполнения своих производственно-хозяйственных и экономических задач. Поэтому обеспечение информационной безопасности - это гарантия удовлетворения законных прав и интересов субъектов информационных отношений. В дальнейшем субъектами информационных отношений будем называть государство (в целом или отдельные его органы и организации), общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельных граждан (физические лица).

Существует множество причин и мотивов, по которым одни люди хотят шпионить за другими. Имея немного денег и старание, злоумышленники могут организовать ряд каналов утечки сведений, используя собственную изобрета-

тельность и (или) халатность владельца информации. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Для построения системы надежной защиты информации необходимо выявить все возможные угрозы безопасности, оценить их последствия, определить необходимые меры и средства защиты, оценить их эффективность. Оценка рисков производится квалифицированными специалистами с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящих потенциальную угрозу в разряд реально опасных и, следовательно, требующих принятия дополнительных мер обеспечения безопасности.

Анализ системы защиты информации, моделирование вероятных угроз позволяет определить необходимые меры защиты. При построении системы защиты информации необходимо строго соблюдать пропорцию между стоимостью системы защиты и степенью ценности информации. И только располагая сведениями о рынке открытых отечественных и зарубежных технических средств несанкционированного съема информации, возможно определить необходимые меры и способы защиты информации. Это одна из самых сложных задач в проектировании системы защиты коммерческих секретов.

Все возможные способы защиты информации сводятся к нескольким основным методикам:

- воспрепятствование непосредственному проникновению к источнику информации с помощью инженерных конструкций технических средств охраны;
- скрытие достоверной информации;
- предоставление ложной информации.

Самыми распространенными способами несанкционированного получения конфиденциальной информации являются:

- прослушивание помещений с помощью технических средств;
- наблюдение (в т. ч. фотографирование и видеосъемка);
- перехват информации с использованием средств радиомониторинга информативных побочных излучений технических средств;
- хищение носителей информации и производственных отходов;
- чтение остаточной информации в запоминающих устройствах системы после выполнения санкционированного запроса, копирование носителей информации;
- несанкционированное использование терминалов зарегистрированных пользователей с помощью хищения паролей;

- внесение изменений, дезинформация, физические и программные методы разрушения (уничтожения) информации.

Современная концепция защиты информации, циркулирующей в помещениях или технических системах коммерческого объекта, требует не периодического, а постоянного контроля в зоне расположения объекта. Защита информации включает в себя целый комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами. Она должна решать такие задачи, как:

- предотвращение доступа злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;

- защита носителей информации от уничтожения в результате различных воздействий;

- предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической защиты информации.

Противоправные действия осуществляются с использованием всех достижений современной микроэлектроники: приемников, передатчиков, усилителей, ретрансляторов, магнитофонов, телекамер, компьютеров и т.п.

С помощью данных средств подслушивают, подсматривают, перехватывают и записывают сообщения, нередко искажают и уничтожают чужую информацию. Современные электронные приборы позволяют проконтролировать практически все используемые каналы сбора, обработки и передачи информации - акустический канал, телефон, радио, компьютер и т.д.

Для того чтобы сформулировать главную цель защиты данных, необходимо определить потенциально существующие возможности нарушения безопасности хранимых, обрабатываемых и передаваемых данных. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно используют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения информационной безопасности.

Понятия «информационная защита» и «защита информации» отнюдь не одно и то же. Информация может быть не только объектом защиты, но и источником угроз для человека и человечества. В защите нуждаются и информационные отношения, т. е. права, свободы и обязанности граждан и юридических лиц в вопросах обладания и распоряжения информацией.

Человечество стало развивать и использовать различные направления информационной защиты еще задолго до того, как его передовые умы задумались о смысле и свойствах информации. В каждом направлении защиты имеет-

ся своя терминология, разрабатываются методы и средства, научная школа и учебные программы для подготовки специалистов. Следователь по компьютерным преступлениям, сотрудник подразделения по защите государственной тайны, сетевой администратор – все это специальности, имеющие непосредственное отношение к защите информации. Однако представители этих специальностей говорят на различных профессиональных языках, используют в своей профессиональной деятельности разные средства и методы и часто с трудом понимают друг друга.

В конце каждой лабораторной работы приведены вопросы для самопроверки. Ответы на некоторые из них достаточно просты.

Необходимость практической подготовки специалистов по защите информации в рамках лабораторных практикумов становится очевидной. Данные методические указания предназначены для подготовки студентов, обучающихся по направлению 10.05.03 - "Информационная безопасность автоматизированных систем", а также будет полезно для курсантов морских специальностей.

Учебно-методическое пособие построено в соответствии с темами теоретического модуля дисциплины «Основы информационной безопасности».

ТЕХНИКА БЕЗОПАСНОСТИ ПРИ ВЫПОЛНЕНИИ ЛАБОРАТОРНЫХ РАБОТ

1. К работе с приборами и персональным компьютером допускаются лица, ознакомленные с его устройством, принципом работы, и методическим пособием.

2. Вход в лабораторию осуществляется только по разрешению преподавателя.

3. На первом занятии преподаватель проводит инструктаж по технике безопасности и напоминает студентам о бережном отношении к лаборатории и о материальной ответственности каждого из них за сохранность оборудования и обстановки лаборатории.

4. При ознакомлении с рабочим местом проверить наличие комплектности оборудования и соединительных проводов (в случае отсутствия, какого-либо элемента, необходимо немедленно сообщить об этом преподавателю).

5. Если во время проведения работы замечены какие-либо неисправности оборудования, необходимо немедленно сообщить об этом преподавателю.

6. После окончания лабораторной работы рабочее место привести в порядок.

ЛАБОРАТОРНАЯ РАБОТА № 1

ЗАКОНОДАТЕЛЬСТВО РФ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель занятия – закрепление теоретических знаний в области правового обеспечения информационной безопасности.

1. Учебные вопросы

1. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.
2. Федеральные законы в области информации и информационной безопасности.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Правовые режимы защиты информации.
5. Правовые вопросы защиты информации с использованием технических средств.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы, используя рекомендованную литературу, а также конспект лекций.

При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся положений Конституции РФ, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического

занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.
2. Какие существуют подходы к определению понятия «информация».
3. В чем заключается двуединство документированной информации с правовой точки зрения.
4. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
5. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
6. Назовите основные виды конфиденциальной информации.
7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
8. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
9. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
10. Назовите основные цели государства в области обеспечения информационной безопасности.
11. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
12. Какой закон определяет понятие «официальный документ»?
13. Какой закон определяет понятие «электронный документ»?
14. В тексте какого закона приведена классификация средств защиты информации?
15. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
16. Назовите основные положения Доктрины информационной безопасности РФ.
17. Назовите составляющие правового института государственной тайны.
18. В каких случаях нельзя относить информацию к государственной тайне?
19. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?

20. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.

21. Дайте определение системы защиты государственной тайны и укажите ее составляющие.

22. Что в соответствии с законодательством РФ представляет собой засекречивание информации.

23. Перечислите основные принципы засекречивания информации.

24. Что понимается под профессиональной тайной?

25. Какие виды профессиональных тайн вам известны?

26. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?

27. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?

28. Что представляет собой электронная цифровая подпись?

29. Каковы основные особенности правового режима электронного документа?

30. Назовите основные ограничения на использование электронных документов?

Литература

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А. Клейменов. – Москва: Академия, 2008. – 330 с.

2. Сычев Ю. Н. Основы информационной безопасности [Электронный ресурс]: учеб.-практ. пособие / Ю. Н. Сычев. – Электрон. текстовые дан. – Москва: ЕАОИ, 2010. – 328 с

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ.

4. О связи: Федеральный закон от 07.07.2003 г. № 126-ФЗ.

5. Об электронной цифровой подписи: Федеральный закон от 10.01.2002 г. № 1-ФЗ.

6. О коммерческой тайне: Федеральный закон от 29.07.2004 г. № 98-ФЗ.

7. О персональных данных: Федеральный закон от 27.07.2006 г. № 152-ФЗ.

8. О лицензировании отдельных видов деятельности: Федеральный закон от 08.08.2001 г. № 128-ФЗ.

9. Об утверждении перечня сведений конфиденциального характера: Указ Президента Российской Федерации от 06.03.1997 г. № 188.

10. О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена: Указ Президента Российской Федерации от 12 мая 2004 года № 611 (в редакции Указов Президента Российской Федерации от 22.03.2005 № 329 и от 03.03.2006 г. № 175).

11. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233.

ЛАБОРАТОРНАЯ РАБОТА № 2

ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации.

1. Учебные вопросы

1. Организационная структура системы государственного лицензирования в области защиты информации.
2. Общий порядок проведения лицензирования в области защиты информации.
3. Контроль за деятельностью лицензиатов.
4. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций.

При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию. Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы государственного лицензирования в области защиты информации, порядка лицензирования и контроля лицензиатов, изучения видов деятельности предприятий в области защиты информации, подлежащих лицензированию, лично отрабатывают контрольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.
5. Права и обязанности лицензиатов.
6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Назовите случаи приостановления или прекращения действия лицензии.
8. В каких случаях предприятию отказывают в выдаче лицензии?
9. Какие документы предоставляются для получения лицензии?
10. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
11. Какие средства относятся к шифровальным?
12. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
13. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.
14. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

15. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

16. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Литература

1. О лицензировании отдельных видов деятельности: Федеральный закон от 08.08.2001 г. № 128-ФЗ.

2. О государственном лицензировании деятельности в области защиты информации: Утв. решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60).

3. О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны: Постановление Правительства Российской Федерации от 15 апреля 1995 г. №333.

4. Об организации лицензирования отдельных видов деятельности: Постановление Правительства Российской Федерации от 26 января 2006 г. №45.

5. О лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах: Постановление Правительства Российской Федерации от 22 октября 2007 г. №689.

6. О лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами: Постановление Правительства Российской Федерации от 29 декабря 2007 г. №957.

7. О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации: Постановление Правительства Российской Федерации от 31 августа 2006 г. №532.

ЛАБОРАТОРНАЯ РАБОТА № 3

СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств защиты информации по требованиям безопасности информации.

1. Учебные вопросы

1. Система сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Виды и схемы сертификации средств защиты информации.
4. Функции ФСТЭК в области сертификации средств защиты информации.
5. Функции органов сертификации средств защиты информации.
6. Функции испытательных лабораторий (центров).
7. Функции заявителей.
8. Порядок проведения сертификации и контроля.
9. Перечень средств защиты информации, подлежащих сертификации.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций. При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации средств защиты информации, порядка сертификации и контроля, лично отрабатывают контрольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Назовите виды и схемы сертификации средств защиты информации.
4. Каковы функции ФСТЭК в области сертификации средств защиты информации?
5. Каковы функции органов сертификации средств защиты информации?
6. Каковы функции испытательных лабораторий (центров).
7. Каковы функции заявителей?
8. Общий порядок проведения сертификации средств защиты информации.
9. Виды контроля в области сертификации средств защиты информации.
10. Чем определяются сроки проведения сертификационных испытаний?
11. На какой срок выдается сертификат?
12. Назовите причины приостановления или аннулирования действия сертификата.

Литература

1. Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации».
2. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. приказом Государственной технической комиссии при Президенте РФ от 27 октября 1995 г. N 199).

ЛАБОРАТОРНАЯ РАБОТА № 4

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств криптографической защиты информации.

1. Учебные вопросы

1. Система сертификации средств криптографической защиты информации.
2. Виды и схемы сертификации средств криптографической защиты информации.
3. Функции органов, лабораторий и заявителей в системе сертификации криптографической защиты информации.
4. Особенности подготовки и проведения сертификации криптографических средств защиты информации.
5. Контроль и надзор за проведением сертификации криптографических средств защиты информации и стабильностью характеристик сертифицированной продукции.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций. При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации средств криптографической защиты информации, особенностей подготовки, проведения сертификации средств криптографической защиты информации и контроля за сертифици-

рованной продукцией, лично отрабатывают контрольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Организационная структура системы сертификации средств криптографической защиты информации.
2. Назовите виды и схемы сертификации средств криптографической защиты информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств криптографической защиты информации?
4. Особенности порядка подготовки и проведения сертификации средств криптографической защиты информации.
5. Виды контроля в области сертификации средств криптографической защиты информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Какие средства относятся к шифровальным?
9. Что относится к закрытым телекоммуникационным системам и комплексам?

Литература

1. Система сертификации средств криптографической защиты информации. № РОСС RU.0001.030001 от 15 ноября 1993 г.
2. Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации».
3. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. приказом Государственной технической комиссии при Президенте РФ от 27 октября 1995 г. № 199).

ЛАБОРАТОРНАЯ РАБОТА № 5

СЕРТИФИКАЦИИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СВЯЗИ

Цель занятия – закрепление теоретических знаний по вопросам сертификации средств вычислительной техники и связи.

1. Учебные вопросы

1. Система сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
2. Виды и схемы сертификации средств вычислительной техники и связи.
3. Особенности подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций. При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информа-

ции, особенностей подготовки, проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации, лично отрабатывают контрольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.
8. Назовите показатели защищенности.
9. Сколько классов защищенности существует?
10. Сформулируйте требования к показателям защищенности.

Литература

1. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: Утв. решение председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

ЛАБОРАТОРНАЯ РАБОТА № 6

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.

1. Учебные вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации объектов информатизации по требованиям безопасности информации.
3. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации.
4. Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации.
5. Порядок проведения аттестации и контроля.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций. При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы аттестации объектов информатизации по требованиям безопасности информации, функций органов аттестации и заявителей, особенностей подготовки, проведения аттестации объектов информатизации по требованиям безопасности информации и контроля, лично отрабатывают кон-

трольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Организационная структура системы объектов информатизации по требованиям безопасности информации.
3. Виды аттестации объектов информатизации по требованиям безопасности информации.
4. Какие объекты информатизации подлежат обязательной аттестации?
5. Каковы функции ФСТЭК в области аттестации объектов информатизации по требованиям безопасности информации?
6. Каковы функции органов по аттестации?
7. Каковы функции заявителей в области аттестации объектов информатизации по требованиям безопасности информации?
8. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
9. На основе каких сведений разрабатывается программа аттестационных испытаний?
10. Порядок проведения аттестационных испытаний.
11. Какая документация представляется органу по аттестации?
12. Что такое технический паспорт объекта информатизации и какие сведения о объекте он включает в себя?
13. В чем состоит содержание специального исследования аттестуемого объекта информатизации?
14. Цель и содержание специальных обследований и проверок.
15. Проведение измерения и оценка уровней защищенности.
16. Какие измерения дополнительно проводятся при использовании на объекте информатизации систем активной защиты?
17. Содержание заключения аттестационной проверки объекта информатизации.
18. Содержание протокола аттестационных испытаний объекта информатизации.
19. Содержание аттестата соответствия на объект информатизации.
20. Ответственность за выполнение установленных условий функционирования аттестованного объекта информатизации.

Литература

1. Положение по аттестации объектов информатизации по требованиям безопасности информации: Утв. председателем Государственной технической комиссии Российской Федерации при Президенте Российской Федерации от 25 ноября 1994 г.

2. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации: Утв. председателем Государственной технической комиссии Российской Федерации при Президенте Российской Федерации, 1994.

ЛАБОРАТОРНАЯ РАБОТА № 7

АТТЕСТАЦИЯ ПОМЕЩЕНИЙ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний по вопросам аттестации помещений по требованиям безопасности информации.

1. Учебные вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Особенности проведения аттестации помещений по требованиям безопасности информации.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций. При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы аттестации объектов информатизации по требованиям безопасности информации, функций органов аттестации и заявителей, особенностей подготовки, проведения аттестации помещений по требованиям безопасности информации и контроля, лично отрабатывают контрольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Какие помещения подлежат обязательной аттестации?
4. Порядок проведения аттестации помещений по требованиям безопасности информации.
5. Какая документация представляется органу по аттестации?
6. Содержание заключения аттестационной проверки помещения.
7. Содержание протокола аттестационных испытаний помещения.
8. Содержание аттестата соответствия на объект информатизации.

Литература

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утв. председателем Государственной технической комиссии Российской Федерации при Президенте Российской Федерации от 25 ноября 1994 г.
2. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации: Утв. председателем Государственной технической комиссии Российской Федерации при Президенте Российской Федерации, 1994.

ЛАБОРАТОРНАЯ РАБОТА № 8

МЕТОДИКА ИСПЫТАНИЙ ОБЪЕКТОВ ИНФОРМАТИКИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний о условиях, порядке и объеме проведения испытаний объектов.

1. Учебные вопросы

1. Объекты испытаний.
2. Цели и задачи проверок и испытаний.
3. Условия и порядок проведения испытаний.
4. Методы испытаний.
5. Испытания объектов на соответствие организационно-техническим требованиям по защите информации.
6. Испытания объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН.
7. Испытания объектов на соответствие требованиям по защите информации от несанкционированного доступа (НСД).
8. Проверка правильности применения криптографических средств защиты информации.
9. Испытания объекта на соответствие требованиям по защите информации от утечки по акустическим каналам.
10. Проверка выполнения требований по защите информации от утечки за счет встроенных технических средств.
11. Оценка результатов испытаний и оформление отчетных материалов.

2. Методические указания студентам по подготовке и проведению лабораторной работы

2.1. При подготовке к занятию

В период подготовки к лабораторной работе студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и учебные материалы лекции, используя рекомендованную литературу, а также конспект лекций. При подготовке к лабораторной работе студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся условий, порядка и объема проведения испытаний объектов, лично отрабатывают контрольные вопросы лабораторной работы. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Перечислите объекты испытаний.
2. Назовите цели и задачи испытаний и проверок.
3. Каковы условия проведения испытаний?
4. Порядок проведения испытаний.
5. Перечислите общие методы испытаний.
6. В чем состоит суть испытаний объектов на соответствие организационно-техническим требованиям по защите информации?
7. Методы испытаний объектов на соответствие организационно-техническим требованиям по защите информации.
8. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН?
9. Виды испытаний объектов на соответствие требованиям по защите информации от утечки за счет ПЭМИН средств вычислительной техники (СВТ).
10. Методы испытаний объектов на соответствие требованиям по защите информации от утечки за счет ПЭМИН СВТ.
11. Виды испытаний объектов на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные цепи и оборудование.
12. Методы испытаний объектов на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные цепи и оборудование.
13. Виды испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания.
14. Методы испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания.

15. Виды испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи.

16. Методы испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи.

17. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от НСД.

18. Виды испытаний объектов на соответствие требованиям по защите информации от НСД.

19. Методы испытаний объектов на соответствие требованиям по защите информации от НСД.

20. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по акустическим каналам.

21. В чем состоит суть проверки выполнения требований по защите информации от утечки за счет встроенных технических средств.

22. В чем состоит суть проверки правильности применения криптографических средств защиты информации.

23. Каким образом осуществляется оценка результатов испытаний и оформление отчетных материалов?

Литература

1. Типовая методика испытаний объектов информатики по требованиям безопасности информации (аттестация АС): Утв. председателем Государственной технической комиссии Российской Федерации при Президенте Российской Федерации от 25 ноября 1994 г.

ЛИТЕРАТУРА

1. Васильков А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков, И. А. Васильков. — Москва: ФОРУМ: ИНФРА-М, 2013. – 368 с.

2. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. — Санкт-Петербург : СПбНИУИТМО, 2014. – 173 с.

3. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.]. — Москва : Радио и связь, 2000. — 192 с.

4. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. — Москва: Горячая линия — Телеком, 2001. — 148 с.

5. Мельников В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. — Москва : Финансы и статистика, 2003. — 368 с.

6. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах / Н. А. Гайдамакин. — Екатеринбург : Изд-во Урал. ун-та, 2003. — 328 с.

7. Зегжда Д. П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. — Москва : Горячая линяя — Телеком, 2000. — 452 с.

8. Расторгуев С. П. Информационные войны / С. П. Расторгуев. — Москва: «Финансы и статистика», 1998. — 415 с.

9. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. — 6-е изд. — М.: Академия, 2012.

10. Астахова, А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД: учеб. пособие / А. В. Астахова. — СПб.: Троицкий мост, 2014..

11. Чеботарева, А. А. Информационное право: учеб. пособие / А.А. Чеботарева. — М.: Юридический институт МИИТа, 2014.

12. Груздева, Л. М. Информационные технологии в профессиональной деятельности : метод. указания по выполнению практических работ / Л. М. Груздева, С.Л. Лобачев, А. А. Чеботарева. — М. : Юридический институт МИИТа, 2015.

13. Карпов, В. И Основы теории обеспечения безопасности личности, общества и государства : учеб. пособие / В.И. Карпов, О. Н. Новокшанов, Д. Б. Павлов. — М.: Юридический институт МИИТа, 2010.

ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

1. http://www.inside-zi.ru — сайт журнала «Защита информации»
2. http://www.inside-zi.ru — сайт журнала «Инсайд»
3. http://www.xakep.ru — сайт журнала «Хакер»
4. http://garant.ru — Гарант: законодательство РФ
5. http://www.consultant.ru — Консультант +: законодательство РФ
6. http://fstec.ru/ — официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)
7. http://www.scrf.gov.ru/ — официальный сайт Совета безопасности Российской Федерации
8. http://fsb.ru — официальный сайт Федеральной службы безопасности Российской Федерации (ФСБ России)

Локальный электронный методический материал

Александр Георгиевич Жестовский

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор Г. А. Смирнова

Уч.-изд. л. __. Печ. л. __

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