Комплект методических указаний по выполнению практических работ по дисциплине Безопасность информационных систем

Перечень практических (лабораторных) работ

№ работы	Название работы (в соответствии с рабочей программой)	Объём часов на выполнение работы	Страница
1.	Анализ Доктрины информационной безопасности Российской Федерации	2	3
2.	Информация как объект защиты (семинар)	2	4 - 5
3.	Введение в информационную безопасность (итоговое занятие по разделу 1)	2	6 – 11
4.	Методы и средства защиты информации (семинар)	2	12 – 13
5.	Средства и способы обеспечения информационной безопасности (Контрольная работа)	2	14 – 15
6.	Анализ защищенности объекта защиты информации	2	16 – 17
7.	Построение модели потенциального нарушителя ИС	2	18 – 19
8.	Итоговое занятие	2	20

Практическая работа №1

Название работы: Анализ Доктрины информационной безопасности Российской Федерации.
Цель работы: Ознакомиться с нормативным документом, который представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.
Исходные данные (задание):

1. Прочитайте и проанализируйте Доктрину ИБ РФ.
2. Постройте схему органов государственной власти и самоуправления, отвечающих за информационную безопасность.
3. Определите функциональные обязанности органов государственной власти и самоуправления, отвечающих за информационную безопасность.
4. Определите положения государственной политики в области обеспечения ИБ.
5. Выделите первоочередные мероприятия по обеспечению ИБ, дайте им оценку.

Порядок выполнения:

1. Познакомиться с теоретическим материалом
2. Сделать краткий конспект теоретического материала в рабочих тетрадях (основные понятия, определения)
3. В тетрадях для практических работ выполнить самостоятельную работу.
4. Сдать преподавателю тетради для практических работ.

Литература:

1. Доктрина информационной безопасности, утверждена президентом РФ 9 сентября 2000 г.

Практическая работа №2

Название работы: Информация как объект защиты (семинар)
Цель работы: Приобрести навыки и разобраться в терминологии информационной безопасности.
Исходные данные (вопросы к семинару):

1. Дайте определение следующим терминам:
   1.1 информационная безопасность;
   1.2 защита информации;
   1.3 угроза безопасности информации;
   1.4 атака;
   1.5 злоумышленник;
   1.6 политика безопасности;
   1.7 конфиденциальность информации;
   1.8 целостность информации;
   1.9 доступность информации;

1.10 идентификатор;
1.11 пароль;
1.12 ключ;
1.13 учетная запись пользователя;
1.14 идентификация;
1.15 аутентификация;
1.16 снифер;
1.17 спуфер;
1.18 сканирование портов;
1.19 отказ от обслуживания;
1.20 утечка;
1.21 разглашение.

2. Меры по защите информации: предупреждение, выявление, обнаружение угроз, пре сечение и локализация угроз, ликвидация последствий угроз.
3. Основные составляющие информационной безопасности: доступность, целостность и конфиденциальность информации.
4. Цели защиты информации. Направления работы для достижения целей защиты информации.
5. Уровни обеспечения информационной безопасности: законодательный, административный, процедурный и программно-технический.
6. Принципы построения Политики безопасности.
7. Угрозы доступности. Примеры угроз доступности.
8. Угрозы целостности и конфиденциальности. Примеры угроз целостности и конфиденциальности.
9. Парольные системы. Способы аутентификации. Угрозы безопасности парольных систем. Разглашение, утечка, несанкционированный доступ к информации.
10. Виды атак на защищаемые ресурсы.

сечение и локализация угроз, ликвидация последствий угроз.

Порядок выполнения:

1. Семинар проходит в виде открытой дискуссии и обсуждения вышеуказанных вопросов.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.
4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru
6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.

7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.

8. Положение о лицензировании деятельности по технической защите конфиденциальной информации

9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.

10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.

11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.

12. Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.

Практическая работа №3

Название работы: Введение в информационную безопасность (итоговое занятие по разделу 1)

Цель работы: Текущий контроль знаний по изученному материалу.

Исходные данные (задание):

1. Вставьте пропущенное слово.
   «Под информационной безопасностью будем понимать защищенность информации и …….. от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»
   а) поддерживающей инфраструктуры
   б) человека
   в) конфиденциальных данных
2. Защита информации – это …
   а) комплекс мероприятий, направленных на обеспечение информационной безопасности
   б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов
   в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям
   г) все определения корректны
3. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:

а) обнаружение угроз
б) пресечения и локализация угроз
в) ликвидация угроз

4. Возможность за приемлемое время получить требуемую информационную услугу называется:
   а) доступностью информации
   б) целостностью информации
   в) предоставлением информации
5. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:
   а) доступностью информации
   б) целостностью информации
   в) предоставлением информации
   г) конфиденциальностью информации
6. Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации
   а) доступность информации
   б) целостность информации
   в) предоставление информации
   г) конфиденциальность информации
7. Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:
   а) законодательного уровня
   б) административного уровня
   в) процедурного уровня
   г) программно-технического уровня
   д) программно-аппаратного уровня
8. Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?
   а) ISO
   б) ITU
   в) ANSI
   г) NIST
   д) NASA
   е) SWIFT
   ж) GISA
9. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:
   а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
   б) Федеральная служба безопасности Российской Федерации

в) Служба внешней разведки Российской Федерации

10. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:
    а) политикой безопасности
    б) методами защиты информации
    в) ограничением доступа к информации
    учетными записями пользователей
11. Потенциальная возможность определенным образом нарушить информационную безопасность – это ….
    а) угроза
    б) атака
    в) взлом
12. Источниками угрозы называют …
    а) потенциальных злоумышленников
    б) компьютерные вирусы
    в) глобальную сеть Интернет
13. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …
    а) окном безопасности
    б) окном опасности
    в) скользящим окном
    г) окном угрозы
14. Ошибки программного обеспечения с точки зрения информационной безопасности являются:
    а) уязвимым местом
    б) окном опасности
    в) окном безопасности
    г) источником угрозы
15. Ошибки администрирования системы с точки зрения информационной безопасности являются:
    а) уязвимым местом
    б) окном опасности
    в) окном безопасности
    г) источником угрозы
16. Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:
    а) уязвимым местом
    б) окном опасности
    в) окном безопасности
    г) источником угрозы
17. Некоторая уникальная информация, позволяющая различать пользователей называется:
    а) идентификатор (логин)
    б) пароль
    в) учетная запись

г) ключ

18. Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:
    а) идентификатор (логин)
    б) пароль
    в) учетная запись
    г) ключ
19. Совокупность идентификатора и пароля пользователя называется:
    а) логин пользователя
    б) учетная запись пользователя
    в) ключ пользователя
20. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:
    а) идентификацией пользователя
    б) аутентификацией пользователя
    в) опознанием пользователя
    г) созданием учетной записи пользователя
21. Проверка принадлежности пользователю предъявленного им идентификатора является:
    а) идентификацией пользователя
    б) аутентификацией пользователя
    в) регистрацией пользователя
    г) созданием учетной записи пользователя
22. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:
    а) утечкой
    б) разглашением
    в) взломом
23. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:
    а) утечкой
    б) разглашением
    в) взломом
24. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называется:
    а) утечкой
    б) разглашением
    в) взломом
25. Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:
    а) «Отказ от обслуживания» (Denial of Service - DoS)
    б) срыв стека

в) внедрение на компьютер деструктивных программ
г) перехват передаваемой по сети информации (Sniffing)
д) спуфинг
е) сканирование портов

26. Атака, целью которой является трафик локальной сети, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

27. Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

28. Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

Порядок выполнения:

1. В тетрадях для практических работ выполнить тест.
2. Сдать преподавателю тетради для практических работ.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.
4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru

6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.

7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.

8. Положение о лицензировании деятельности по технической защите конфиденциальной информации

9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.

10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.

11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.

Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.

Практическая работа №4

Название работы: Методы и средства защиты информации (семинар).

Цель работы: Приобрести навыки и разобраться в терминологии информационной безопасности.

Исходные данные (задание):

1. Дайте определение следующим терминам:
   - 1.1 собственник информации;
   - 1.2 владелец информации;
   - 1.3 пользователь, распоряжение;
   - 1.4 гриф секретности;
   - 1.5 дезинформация;
   - 1.6 легендирование;
   - 1.7 клевета.
2. Стратегия национальной безопасности Российской Федерации: особенности, цели, составляющие национальных интересов России в информационной сфере.
3. Доктрина информационной безопасности Российской Федерации: назначение документа, источники угроз информационной безопасности Российской Федерации, общие методы обеспечения информационной безопасности РФ.
4. Нормативно-правовое регулирование защиты информации: направления защиты
5. Виды конфиденциальной информации

Порядок выполнения:

1. Семинар проходит в виде открытой дискуссии и обсуждения вышеуказанных вопросов.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.
4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru
6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.
7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.
8. Положение о лицензировании деятельности по технической защите конфиденциальной информации
9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.
10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.
11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.

Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.

Практическая работа № 5

Название работы: Средства и способы обеспечения информационной безопасности (Контрольная работа)

Цель работы: Текущий контроль полученных знаний и умений.

Исходные данные (задание):

1. Приведите основные методы и приемы защиты обеспечения информационной безопасности в разных информационных пространствах.

Таблица 1. Виды информационного пространства для организации защиты информации по вариантам

Порядок выполнения:

1. В тетрадях для практических работ выполнить самостоятельную работу или решить номера, которые указаны в работе.
2. Сдать преподавателю тетради для практических работ.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.
4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru
6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.
7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.
8. Положение о лицензировании деятельности по технической защите конфиденциальной информации
9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.
10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.
11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.
Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.

Практическая работа №6

Название работы: Анализ защищенности объекта защиты информации

Цель работы: Формирование умений и навыков определения угроз и защищённости объектов информации.

Исходные данные (задание):

Для выбранного определенного объекта защиты информации (номер варианта соответствует номеру студента по списку) необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1 виды угроз;
2 характер происхождения угроз;
3 классы каналов несанкционированного получения информации;
4 источники появления угроз;
5 причины нарушения целостности информации;

Наименование объекта защиты информации:

а) Одиночно стоящий компьютер в бухгалтерии.
б) Сервер в бухгалтерии.
в) Почтовый сервер.
г) Веб-сервер.

д) Компьютерная сеть материальной группы.

е) Одноранговая локальная сеть без выхода в Интернет.

ж) Одноранговая локальная сеть с выходом в Интернет.

з) Сеть с выделенным сервером без выхода в Интернет.

и) Сеть с выделенным сервером с выхода в Интернет.

к) Телефонная база данных (содержащая и информацию ограниченного пользования) в

твердой копии и на электронных носителях.

л) Телефонная сеть.

м) Средства телекоммуникации (радиотелефоны, мобильные телефоны).

н) Банковские операции (внесение денег на счет и снятие).

о) Операции с банковскими пластиковыми карточками.

п) Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.

р) Компьютер, хранящий конфиденциальную информацию о разработках предприятия.

с) Материалы для служебного пользования на твердых носителях и на электронных носителях в производстве.

т) Материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии.

у) Материалы для служебного пользования на твердых носителях в архиве.

ф) Материалы для служебного пользования на твердых носителях и на электронных носителях в налоговой инспекции.

х) Комната для переговоров по сделкам на охраняемой территории.

ц) Комната для переговоров по сделкам на неохраняемой территории.

ч) Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).

ш) Судебные материалы (твердая копия и на электронных носителях).

щ) Паспортный стол РОВД (твердая копия и на электронных носителях).

Порядок выполнения:

1. Познакомиться с теоретическим материалом
2. В тетрадях для практических работ выполнить самостоятельную работу или решить номера, которые указаны в работе.
3. Сдать преподавателю тетради для практических работ.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.

4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru
6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.
7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.
8. Положение о лицензировании деятельности по технической защите конфиденциальной информации
9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.
10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.
11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.
12. Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.

Практическая работа №7

Название работы: Построение модели потенциального нарушителя ИС.

Цель работы: Формирование умений и навыков определения угроз ИС.

Исходные данные (задание):

1. Определите возможных нарушителей объекта защиты информации. Классифицируйте их в соответствии с двумя группами: внешние нарушители и внутренние нарушители.
2. Заполните на основе собственных полученных данных Таблицу «Типы угроз и возможные внутренние нарушители объекта».
3. Приведите список персонала АСОИ и соответствующую степень риска от каждого из них.

Порядок выполнения:

1. Познакомиться с теоретическим материалом
2. В тетрадях для практических работ выполнить самостоятельную работу.
3. Сдать преподавателю тетради для практических работ.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.

4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru
6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.
7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.
8. Положение о лицензировании деятельности по технической защите конфиденциальной информации
9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.
10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.
11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.
Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.

Практическая работа № 8

Название работы: Итоговое занятие

Цель работы: Промежуточная аттестация по дисциплине.

Исходные данные (задание):

Представление преподавателю для проверки тетрадь конспектов с темами СРС.

Литература:

1. ГОСТ Р50922-2006 “Защита информации. Основные термины и определения” от 27 декабря 2006 г.
2. 2 ГОСТ Р50.1.056-2005 “Техническая защита информации. Основные термины и определения” от 29 декабря 2005 г.
3. 3 ГОСТ Р51275-2006 “Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения” от 27.12.2006 г.
4. Доктрина информационной безопасности Российской Федерации от 09.09.2000 г.
5. Официальный сайт ФСТЭК России http://www.fstec.ru
6. Положение о Федеральной Службе Безопасности и ее структуры от 11.08.2003 г.
7. Положение о Федеральной службе технического и экспортного контроля от 16.08.2008 г.
8. Положение о лицензировании деятельности по технической защите конфиденциальной информации
9. Постановление Правительства Российской Федерации № 45 “Об организации лицензирования отдельных видов деятельности” от 26.01.2006 г.

10. Федеральный закон №128 “О лицензировании отдельных видов деятельности” от 08.08.2001 г.

11. Федеральный закон № 149-ФЗ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г.

Федеральный закон № 5485-I “О государственной тайне” от 21.07.93 г.