Каталоги угроз и контрмер IT Baseline

Каталоги угроз и контрмер, используемые в Германском стандарте IT Baseline Protection Manual

Каталог угроз

Содержит следующие группы угроз:

T1. Угрозы в связи с форс-мажорными обстоятельствами.

T2. Угрозы на организационном уровне.

T3. Угрозы, связанные с ошибками людей.

T4. Угрозы, связанные с техникой.

T5. Угрозы, возникающие на предпроектном этапе.

Ниже перечислены угрозы, входящие в каждую из групп. Детальное описание угроз на английском языке можно посмотреть по адресу http://www.bsi.bund.de/gshb/english/t/t1000.htm.

T 1. Угрозы в связи с форс-мажорными обстоятельствами

T1.1. Потеря персонала.

T1.2. Отказ информационной системы.

T1.3. Молния.

T1.4. Пожар.

T1.5. Затопление.

T1.6. Возгорание кабеля.

T1.7. Недопустимая температура и влажность.

T1.8. Пыль, загрязнение.

T1.9. Потеря данных из-за воздействия интенсивных магнитных полей.

T1.10. Отказ сети на большой территории.

T1.11. Катастрофы в окружающей среде.

T1.12. Проблемы, вызванные неординарными общественными событиями.

T1.13. Шторм.

T2. Угрозы на организационном уровне

T2.1. Отсутствие или недостатки регламентирующих документов.

T2.2. Недостаточное знание требований регламентирующих документов.

T2.3. Недостаточно совместимые или неподходящие ресурсы.

T2.4. Недостатки контроля и измерения уровня безопасности в информационной технологии.

T2.5. Недостатки в обслуживании.

T2.6. Несоответствие помещений требованиям в области безопасности.

T2.7. Превышение полномочий.

T2.8. Нерегламентированное использование ресурсов.

T2.9. Недостатки в процедурах отслеживания изменений в информационной технологии.

T2.10. Несоответствие среды передачи данных предъявляемым требованиям.

T2.11. Недостаточный горизонт планирования.

T2.12. Недостатки в документировании коммуникаций.

T2.13. Недостаточная защищенность от действий дистрибьюторов.

Т2.14. Ухудшение использования информационных технологий из-за плохих условий на рабочих местах.

Т2.15. Возможность несанкционированного доступа к конфиденциальным данным в ОС UNIX.

Т2.16. Несанкционированное (недокументированное) изменение пользователей портативной ЭВМ.

Т2.17. Неправильная маркировка носителей данных.

Т2.18. Неверная доставка носителей данных.

Т2.19. Некорректная система управления криптографическими ключами.

Т2.20. Неподходящее обеспечение расходными материалами факсов.

Т2.21. Ненадлежащая организация изменения пользователей.

Т2.22. Отсутствие должной оценки результатов аудита данных.

Т2.23. Подключение ПК под DOS в сеть, содержащую серверы.

Т2.24. Несанкционированный доступ к конфиденциальным данным в сети.

Т2.25. Уменьшение скорости обмена, вызванное вспомогательными функциями взаимодействия одноуровневых объектов.

Т2.26. Недостаточное тестирование ПО.

Т2.27. Неправильная документация.

Т2.28. Нарушение авторского права.

Т2.29. Несанкционированное тестирование программ на этапе эксплуатации ИС.

Т2.30. Неправильное планирование доменной структуры.

Т2.31. Некорректная защита систем под управлением ОС Windows NT.

Т2.32. Неподходящая пропускная способность телекоммуникационных линий.

Т2.33. Размещение Novell Netware Servers в опасном окружении.

Т2.34. Отсутствие или некорректная настройка механизмов безопасности Novell Netware.

Т2.35. Отсутствие аудита ОС Windows 95.

Т2.36. Неправильные ограничения пользовательской среды.

Т2.37. Неконтролируемое использование коммуникационных линий.

Т2.38. Недостаточное или неправильное использование штатных механизмов защиты базы данных.

Т2.39. Сложность DBMS.

Т2.40. Сложность доступа к базам данных.

Т2.41. Неверная организация обмена данных пользователей с базой данных.

Т2.42. Сложность NDS.

Т2.43. Миграция с ОС Novell 3.x на ОС Novell версии 4 и 5.

Т2.44. Несовместимые активные и пассивные сетевые компоненты.

Т2.45. Концептуальные ошибки проектирования сети.

Т2.46. Превышение максимально допустимой длины кабеля.

Т2.47. Передача данных по коммуникациям, не соответствующим требованиям безопасности.

Т2.48. Неадекватное использование информации и документов при работе в домашних условиях.

Т2.49. Недостаточное или неверное обучение телеобработке.

Т2.50. Задержки, вызванные временными сбоями при удаленной работе.

Т2.51. Плохая интеграция удаленных рабочих мест в информационную технологию.

Т2.52. Более длинные временные периоды реакции системы в случае неверного выбора архитектуры системы.

Т2.53. Неполные инструкции относительно замены аппаратно-программных средств на удаленных рабочих местах.

Т2.54. Несанкционированный доступ к данным через скрытые элементы данных.

Т2.55. Неконтролируемое использование электронной почты.

Т2.56. Ненадлежащее описание файлов.

Т2.57. Неправильное хранение носителей информации в случае аварий.

Т2.58. ОС Novell Netware и «проблема 2000».

Т2.59. Работа с незарегистрированными компонентами.

Т2.60. Недостаточная детализация стратегии сети и системы управления сетевыми ресурсами.

Т2.61. Неразрешенная совокупность личных данных.

Т2.62. Неподходящая обработка инцидентов в области безопасности.

Т2.63. Бесконтрольное использование факсов.

Т2.64. Недостатки или отсутствие правил для RAS.

Т2.65. Сложность конфигурации сервера SAMBA

Т2.66. Недостатки или неадекватность системы управления в области безопасности.

Т2.67. Недостатки администрирования прав доступа.

Т3. Угрозы, связанные с ошибками людей

Т3.1. Нарушение конфиденциальности/целостности данных в результате ошибок пользователей.

Т3.2. Разрушение оборудования или данных в результате небрежности.

Т3.3. Несоблюдение правил поддержания режима ИБ.

Т3.4. Несанкционированные подключения кабелей.

Т3.5. Повреждения кабелей из-за небрежности.

Т3.6. Опасности, связанные с увольнением или выведением персонала за штат.

Т3.7. Сбои АТС и ошибки оператора.

Т3.8. Запрещенные действия в информационной системе.

Т3.9. Запрещенные действия системного администратора.

Т3.10. Некорректный перенос файловой системы ОС UNIX.

Т3.11. Некорректная конфигурации сервера электронной почты sendmail.

Т3.12. Потери носителей с данных при их перевозке (перемещении).

Т3.13. Передача неправильных или нежелательных данных.

Т3.14. Неправильное (с юридической позиции) оформление факса.

Т3.15. Неправильное использование автоответчиков.

Т3.16. Неправильное администрирование сайта и прав доступа.

Т3.17. Смена пользователей ПК, не соответствующая внутренним правилам.

Т3.18. Совместное использование информационных ресурсов и оборудования.

Т3.19. Хранение паролей в ОС Windows 95 в открытом виде.

Т3.20. Неумышленное предоставление доступа для чтения.

Т3.21. Использование ключей с нарушениями правил.

Т3.22. Модификация системного реестра.

Т3.23. Нарушение правил администрирования DBMS.

Т3.24. Небрежность манипуляций с данными.

Т3.25. Небрежность при стирании (уничтожении) информации.

Т3.26. Небрежность при совместном использовании файловой системы.

Т3.27. Неверная синхронизация времени.

Т3.28. Неправильные конфигурации активных сетевых компонентов.

Т3.29. Недостатки системы сегментации.

Т3.30. Использование удаленных рабочих станций для личных нужд.

Т3.31. Хаотичность в организации данных.

Т3.32. Нарушение законодательства в использовании криптографии.

Т3.33. Неправильное использование криптомодулей.

Т3.34. Неудачная конфигурация системы управления.

Т3.35. Отключение сервера во время работы.

Т3.36. Неверное истолкование событий.

Т3.37. Непродуктивные исследования.

Т3.38. Ошибки в конфигурации и операциях.

Т3.39. Неправильное администрирование RAS.

Т3.40. Несоответствие используемых процедур аутентификации требованиям, предъявляемым к удаленным рабочим местам.

Т3.41. Неправильное использование сервисов удаленного доступа.

Т3.42. Опасные конфигурации RAS-клиентов.

Т3.43. Нарушение инструкций использования паролей.

Т3.44. Небрежности в обработке информации.

Т3.45. Некорректно работающая система идентификации партнеров.

Т3.46. Ошибки в конфигурации сервера Lotus Notes.

Т3.47. Ошибки в конфигурации доступа браузера к Lotus Notes.

Т4. Угрозы, связанные с техникой

Т4.1. Разрушения системы электроснабжения.

Т4.2. Отказы внутренних сетей электроснабжения.

Т4.3. Недействительность имеющихся гарантий.

Т4.4. Ухудшение состояния линий из-за воздействия окружающей среды.

Т4.5. Перекрестные подключения.

Т4.6. Броски напряжения в системе электроснабжения.

Т4.7. Дефекты кабелей информационных сетей.

Т4.8. Обнаруженные уязвимости ПО.

Т4.9. Разрушение внутренних источников электропитания.

Т4.10. Сложности доступа к сетевым ресурсам.

Т4.11. Недостатки аутентификации между NIS-сервером и NIS-клиентом.

Т4.12. Недостатки аутентификации между серверами и клиентами.

Т4.13. Потеря хранимых данных.

Т4.14. Отсутствие специальной бумаги для факсов.

Т4.15. Отправка сообщения по факсу неправильному получателю из-за неверной коммутации.

Т4.16. Неполучение сообщения, отправленного по факсу, из-за ошибки передачи.

Т4.17. Дефект факсимильного аппарата.

Т4.18. Разрядка аккумулятора или неправильное электропитание в автоответчиках.

Т4.19. Потери информации из-за старения (ухудшения качества) носителя данных.

Т4.20. Потери данных из-за старения (ухудшения качества) носителя данных.

Т4.21. Неправильное экранирование от транзитных потоков.

Т4.22. Уязвимости ПО или ошибки.

Т4.23. Уязвимости системы распознавания CD-ROM.

Т4.24. Преобразования имени файла при резервном копировании данных в ОС Windows 95.

Т4.25. Все еще активные подключения.

Т4.26. Отказ базы данных.

Т4.27. Несанкционированный доступ через ODBC.

Т4.28. Потери данных в базе данных.

Т4.29. Потери данных в базе данных, вызванные недостатком емкости диска.

Т4.30. Потеря целостности базы данных.

Т4.31. Отказ или сбой компонентов сети.

Т4.32. Отказ при отправке сообщений.

Т4.33. Отсутствие процедуры идентификации или ненадлежащее ее качество.

Т4.34. Отказ криптомодулей.

Т4.35. Некорректность криптоалгоритма.

Т4.36. Ошибки при кодировании данных.

Т4.37. Неполучение (несвоевременная доставка) электронной почты или квитанций.

Т4.38. Отказы компонентов системы управления сетью или информационной системой.

Т4.39. Концептуальные ошибки ПО.

Т4.40. Некорректная настройка RAS-клиента операционной среды.

Т4.41. Недостатки в мобильной сети связи.

Т4.42. Отказ мобильного телефона.

Т4.43. Недокументированные возможности.

Т5. Угрозы, возникающие на предпроектном этапе

Т5.1. Разрушение оборудования или вспомогательной инфраструктуры информационной системы.

Т5.2. Манипуляция данными или ПО.

Т5.3. Нарушения системы контроля доступа в помещениях.

Т5.4. Воровство.

Т5.5. Вандализм.

Т5.6. Нападения.

Т5.7. Перехват в линиях связи.

Т5.8. Манипуляции линиями связи.

Т5.9. Неавторизованное использование информационной системы.

Т5.10. Злоупотребления, связанные с удаленным доступом.

Т5.11. Несанкционированный доступ к конфиденциальным данным, сохраненным в процессе инсталляции офисной АТС.

Т5.12. Перехват телефонных звонков и передаваемых данных.

Т5.13. Подслушивание.

Т5.14. Пользование телефоном для личных нужд.

Т5.15. «Любознательные» сотрудники.

Т5.16. Угрозы, исходящие от персонала (штатных сотрудников) в процессе обслуживания/администрирования информационной системы.

Т5.17. Угрозы, исходящие от посторонних специалистов, привлекаемых для обслуживания элементов информационной системы.

Т5.18. Подбор паролей.

Т5.19. Злоупотребления правами пользователей.

Т5.20. Злоупотребления правами администратора.

Т5.21. Вредоносное ПО. «Троянские» кони.

Т5.22. Воровство мобильных элементов информационной системы.

Т5.23. Враждебные апплеты и вирусы.

Т5.24. Закладки.

T5.25. Маскарад.

T5.26. Подслушивание и перехват сообщений.

T5.27. Отказ от авторства сообщения.

T5.28. Недоступность сервисов.

T5.29. Несанкционированное копирование носителей данных.

T5.30. Несанкционированное использование факсимильных машин.

T5.31. Несанкционированный просмотр поступающих по факсу сообщений.

T5.32. Информация, остающаяся в факсимильных машинах.

T5.33. Использование факсимильных машин для доставки поддельных писем.

T5.34. Преднамеренное перепрограммирование факсимильных машин.

T5.35. Манипуляции с поступающими по факсу сообщениями.

T5.36. Перезагрузка автоответчиков.

T5.37. Определение кодов доступа.

T5.38. Неправильные употребления отдаленного запроса.

T5.39. Проникновение в информационную систему через системы связи.

T5.40. Ненадлежащий контроль помещений, в которых установлены компьютеры, оборудованные микрофонами.

T5.41. Некорректное использование программ под управлением ОС UNIX, использующих протокол uucp.

T5.42. Враждебное использование методов социальной инженерии.

T5.43. Макровирусы.

T5.44. Злоупотребление доступом к отдаленным портам для получения чужих данных.

T5.45. Подбор пароля в ОС Windows.

T5.46. Маскарад в АРМ под управлением ОС Windows.

T5.47. Уничтожение почтового сервера.

T5.48. Атака IP Spoofing.

T5.49. Злоупотребления с маршрутизацией данных.

T5.50. Злоупотребления с протоколом ICMP.

T5.51. Злоупотребления с протоколом маршрутизации.

T5.52. Злоупотребления правами администратора в системах под Windows NT.

T5.53. Неправильное использование защитных кабинетов.

T5.54. Преднамеренные действия, приводящие к аварийному завершению.

T5.55. Вход в обход системы аутентификации.

T5.56. Ненадлежащий учет пользователей, имеющих свободный доступ к сетевым ресурсам.

T5.57. Несанкционированный запуск сканеров сети.

T5.58. Взлом ОС Novell Netware.

T5.59. Злоупотребление правами администратора в сетях Novell Netware 3.x.

T5.60. Рекомендации по обходу системы.

T5.61. Злоупотребления, связанные с удаленным управлением маршрутизатором.

T5.62. Злоупотребления, связанные с удаленным управлением ресурсами информационной системы.

T5.63. Манипуляции через D-канал ISDN.

T5.64. Манипуляции данными или программным обеспечением базы данных.

T5.65. Отказ в обслуживании базы данных.

T5.66. Неразрешенные подключения в ЛВС информационной системы.

T5.67. Несанкционированное управление сетевыми ресурсами.

T5.68. Несанкционированный доступ к активному сетевому оборудованию.

T5.69. Риск воровства на домашнем рабочем месте.

T5.70. Манипуляции, выполняемые родственниками или посетителями.

T5.71. Несанкционированный доступ к конфиденциальной информации определенных категорий пользователей.

T5.72. Неразрешенное использование почтовых услуг.

T5.73. Маскарад отправителя.

T5.74. Манипуляции файлами рассылки и псевдонимами.

T5.75. Перегрузка при получении письма по электронной почте.

T5.76. Вредоносное ПО в почте.

T, 5.77. Несанкционированное ознакомление с электронной почтой.

T5.78. Атака DNS spoofing.

T5.79. Несанкционированное приобретение прав администратора под Windows NT.

T5.80. Атака Hoaxes.

T5.81. Неразрешенное использование криптомодулей.

T5.82. Манипуляции криптомодулями.

T5.83. Компрометация криптографических ключей.

T5.84. Подделка удостоверений.

T5.85. Потеря целостности информации, которая должна быть защищена.

T5.86. Манипуляции параметрами управления.

T5.87. Атака Web spoofing.

T5.88. Неправильное использование активного контента.

T5.89. Захват сетевых подключений.

T5.90. Манипуляции списками рассылки и адресными книгами.

T5.91. Отключение механизма защиты доступа RAS.

T5.92. Использование клиента RAS в качестве сервера.

T5.93. Разрешение третьим лицам использовать RAS-компоненты.

T5.94. Неправильное употребление компонентов оборудования.

T5.95. Подслушивание конфиденциальных переговоров по мобильным телефонам.

T5.96. Вмешательство с использованием мобильных телефонов.

T5.97. Неразрешенная передача данных по мобильным телефонам.

T5.98. Перехват телефонных звонков с мобильных телефонов.

T5.99. Перехват трафика мобильных телефонов.

T5.100. Злоупотребление активным контентом для доступа к Lotus Notes.

T5.101. Взлом Lotus Notes.

T5.102. Саботаж.

Каталог контрмер

Каталог, доступный по адресу http://www.bsi.bund.de/gshb/english/menue.htm. содержит следующие группы контрмер для обеспечения безопасности:

- поддерживающей инфраструктуры;
- на организационном уровне;
- на кадровом уровне;
- программного обеспечения и вычислительной техники;
- коммуникаций;
- непрерывности бизнеса.

Далее перечисляются контрмеры, входящие в каждую из групп. Детальное описание контрмер на английском языке можно найти на сайте http://www.bsi.bund.de/gshb/english/s/s1000.htm.

S1. Обеспечение безопасности на уровне поддерживающей инфраструктуры

S1.1. Соответствие стандартам и отраслевым спецификациям элементов инфраструктуры.

S1.2. Система контроля со стороны правительства над производителями и дистрибьюторами электроэнергии, телефонными сетями, газо- и водоснабжением.

S1.3. Периодические проверки поддерживающей инфраструктуры (электропитания, климатических систем и т.д.) на соответствие предъявляемым к ним (на текущий момент) требованиям.

S1.4. Грозо- и молниезащита.

S1.5. Гальваническая развязка с внешними сетями.

S1.6. Соответствие помещений требованиям стандартов в области пожарной безопасности.

S1.7. Автоматические (дистанционные) системы пожаротушения.

S1.8. Использование отделочных материалов, соответствующих требованиям в области пожарной безопасности.

S1.9. Использование силовых и информационных кабелей с пожароустойчивой изоляцией.

S1.10. Наличие запасных выходов для персонала.

S1.11. Наличие планов коммуникаций, относящихся к инфраструктуре (электро-, газо- и водоснабжению).

S1.12. Организация защиты воздухозаборников, климатического оборудования, распределительных щитов.

S1.13. Организация защиты зданий и прилегающей территории от внешних факторов: затопления, автомобильного движения и т.п.

S1.14. Автоматизация дренажных работ. В некоторых помещениях (в подвалах, подверженных частым затоплениям) необходимо установить насосы, включающиеся автоматически в случае возникновения угрозы затопления.

S1.15. Контроль доступа. Окна и двери должны быть закрыты в отсутствие людей.

S1.16. Схемы размещения. Распределение персонала по комнатам следует производить с учетом требований минимизации перемещения людей. Подразделения, не связанные технологически, должны быть по возможности изолированы.

S1.17. Наличие эффективного контроля на входе в помещение.

S1.18. Наличие приборов (датчиков) охранной и пожарной сигнализации.

S1.19. Комплекс мер защиты от проникновения посторонних в помещения.

S1.20. Разделение кабелей с разными требованиями в области защиты (с разными физическими и механическими свойствами).

S1.21. Соответствие мест прокладки кабелей необходимым требованиям.

S1.22. Физическая защита мест прокладки кабелей.

S1.23. Отсутствие открытых неиспользуемых дверей.

S1.24. Отсутствие близко расположенных трубопроводов (тепло- и водоснабжения).

S1.25. Защита от высокого напряжения.

S1.26. Защита силовых проводов от обрывов и повреждений.

S1.27. Климатическое оборудование.

S1.28. Использование UPS.

S1.29. Правильное расположение элементов информационной системы.

S1.30. Обеспечение сохранности регистрационной информации о входящих/ исходящих сообщениях.

S1.31. Удаленная индикация сбоев (неисправностей) оборудования.

S1.32. Корректная настройка консолей, устройств передачи данных, принтеров.

S1.33. Обеспечение сохранности переносных (мобильных) ПК при использовании их вне территории организации.

S1.34. Обеспечение сохранности переносных (мобильных) ПК при использовании их в качестве офисных ПК.

S1.35. Организация хранения временно не используемых переносных (мобильных) ПК.

S1.36. Организация хранения носителей данных с записанными на них резервными копиями и другими данными.

S1.37. Меры безопасности при эксплуатации факсов.

S1.38. Меры безопасности при эксплуатации модемов.

S1.39. Защита данных в линиях связи.

S1.40. Обеспечение сохранности кабелей.

S1.41. Защита от ПЭМИН.

S1.42. Обеспечение безопасности сервисов Novell.

S1.43. Обеспечение безопасности маршрутизации ISDN.

S1.44. Меры безопасности при организации рабочих мест в домашних условиях.

S1.45. Организация надежного хранения важных данных и документов.

S1.46. Использование техники, предотвращающей кражи.

S1.47. Локализация пожароопасных мест.

S1.48. Противопожарная сигнализация.

S1.49. Формализация технических и административных требований к организации рабочих мест и других элементов информационной системы.

S1.50. Защита от курения на рабочих местах.

S1.51. Уменьшение возможных последствий пожара.

S1.52. Уменьшение избыточности технологической инфраструктуры.

S1.53. Видеонаблюдение.

S1.54. Раннее обнаружение пожара.

S1.55. Защита периметра.

S1.56. Альтернативные источники электропитания.

S1.57. Документирование инфраструктуры и планы здания.

S1.58. Технические и организационные требования к помещениям для размещения серверов.

S2. Обеспечение безопасности на организационном уровне

S2.1. Распределение должностных обязанностей в сфере IT.

S2.2. Управление ресурсами.

S2.3. Контроль за средой передачи данных.

S2.4. Планирование мероприятий в области ремонта и поддержки.

S2.5. Разделение ответственности и функций.

S2.6. Регламентация доступа к информационным ресурсам.

S2.7. Регламентация привилегий различных групп пользователей.

S2.8. Регламентация правил доступа к приложениям и данным.

S2.9. Запрещение использования ПО, не входящего в список официально разрешенного.

S2.10. Список разрешенного ПО и его владельцев.

S2.11. Правила использования паролей.

S2.12. Служба поддержки для пользователей.

S2.13. Правильное расположение информационных ресурсов, требующих защиты.

S2.14. Управление доступом к ключам от помещений.

S2.15. Инспекция пожарной безопасности.

S2.16. Сопровождение посетителей.

S2.17. Правила доступа на территорию посторонних.

S2.58. Ограничение времени сообщения.

S2.59. Приобретение подходящего модема.

S2.60. Администрирование модемов с учетом требований ИБ.

S2.61. Документирование процедур пользования модемами.

S2.62. Разрешенное к применению ПО и процедуры санкционирования его применения.

S2.63. Права доступа.

S2.64. Просмотр log-файлов.

S2.65. Проверка эффективности разграничения пользователей в информационной системе.

S2.66. Приобретение только сертифицированных элементов.

S2.67. Стратегии для одноранговых сетей.

S2.68. Применение процедур контроля безопасности в одноранговых сетях.

S2.69. Стандарты на рабочие станции.

S2.70. Использование МЭ.

S2.71. Политика ИБ для МЭ.

S2.72. Требования к МЭ.

S2.73. Выбор подходящего МЭ.

S2.74. Выбор подходящего пакетного фильтра.

S2.75. Выбор подходящего шлюза.

S2.76. Определение правил фильтрации.

S2.77. Конфигурация компонентов, соответствующая требованиям безопасности.

S2.78. Правила работы с МЭ.

S2.79. Определение ответственных за использование стандартного ПО.

S2.80. Каталоги используемого стандартного ПО.

S2.81. Выбор подходящего стандартного ПО.

S2.82. Разработка плана тестирования стандартного ПО.

S2.83. Тестирование стандартного ПО.

S2.84. Разработка инструкций по инсталляции стандартного ПО

S2.85. Санкционирование установки стандартного ПО.

S2.86. Гарантии совместимости стандартного ПО.

S2.87. Инсталляция и конфигурирование стандартного ПО.

S2.88. Управление лицензированием и контроль за версиями ПО.

S2.89. Деинсталляция стандартного ПО.

S2.90. Контроль поставок ПО.

S2.91. Определение стратегии безопасности для клиент-серверных приложений Windows NT.

S2.92. Выбор способов контроля безопасности для клиент-серверных приложений Windows NT.

S2.93. Планирование конфигурации сети на основе ОС Windows NT.

S2.94. Совместное использование директорий в сетях под управлением ОС Windows NT.

S2.95. Обеспечение должной защиты шкафов.

S2.96. Блокирование шкафов с важными ресурсами.

S2.97. Корректные процедуры для электронных замков.

S2.98. Безопасность при инсталляции Novell Netware servers.

S2.99. Штатные механизмы безопасности Novell Netware servers.

S2.100. Обеспечение ИБ при использовании Novell Netware servers.

S2.101. Проверка Novell Netware servers.

S2.102. Активизация удаленных консолей.

S2.103. Профили пользователей в ОС Windows 95.

S2.104. Руководство пользователя по безопасности для ОС Windows 95.

S2.105. Расширение учрежденческой АТС.

S2.106. Выбор подходящих ISDN-плат.

S2.107. Документирование конфигурации ISDN-плат.

S2.108. Удаленная поддержка ISDN gateways.

S2.109. Назначение прав при удаленном доступе.

S2.110. Руководство по работе с log-файлами.

S2.111. Сохранность руководств.

S2.112. Соблюдение правил обмена файлами и данными между рабочими станциями и получателями.

S2.113. Документирование процедурных вопросов, связанных с использованием телекоммуникаций.

S2.114. Потоки информации вовне и извне.

S2.115. Поддержка удаленного доступа.

S2.116. Использование телекоммуникаций.

S2.117. Управление доступом к телекоммуникациям.

S2.118. Политика безопасности при использовании e-mail.

S2.119. Инструкции по использованию e-mail.

S2.120. Конфигурирование почтового сервера.

S2.121. Регулярное уничтожение писем e-mail.

S2.122. Стандартизация адресов e-mail.

S2.123. Выбор провайдера.

S2.124. Выбор подходящей СУБД.

S2.125. Инсталляция и конфигурирование СУБД.
S2.126. Разработка концепции безопасности для СУБД.
S2.127. Интерфейс.
S2.128. Управление доступом к СУБД (организационные аспекты).
S2.129. Управление доступом к информации в СУБД.
S2.130. Гарантии целостности СУБД.
S2.131. Разделение задач администрирования и поддержания СУБД.
S2.132. Конфигурирование доступа пользователей и групп пользователей.
S2.133. Контроль за log-файлами.
S2.134. Руководства по использованию СУБД.
S2.135. Безопасность обмена данными с СУБД.
S2.136. Правила безопасности для вычислительной среды рабочих станций.
S2.137. Процедуры резервного копирования.
S2.138. Структурирование данных при хранении.
S2.139. Обзор сетевой инфраструктуры.
S2.140. Анализ сетевой инфраструктуры.
S2.141. Концепция развития сетевой инфраструктуры.
S2.142. Разработка планов развития сетевой инфраструктуры.
S2.143. Система управления сетевыми протоколами.
S2.144. Выбор протокола управления сетевыми ресурсами.
S2.145. Средства управления сетью.
S2.146. Обеспечение ИБ системы управления сетью.
S2.147. Вопросы ИБ при миграции на старшие версии Novell.
S2.148. Конфигурирование Novell Netware 4.x networks.
S2.149. Обеспечение безопасности Netware 4.x networks.
S2.150. Аудит сетей Novell Netware 4.x.
S2.151. Разработка концепции NDS.
S2.152. Разработка концепции синхронизации времени.
S2.153. Документирование на Novell Netware 4.x networks.
S2.154. Концепция защиты от вирусов.
S2.155. Идентификация уязвимостей для вирусов.
S2.156. Выбор подходящей стратегии антивирусной защиты.
S2.157. Выбор подходящей антивирусной программы.
S2.158. Обработка сообщений о заражении вирусами.
S2.158. Обновление антивирусных программ.
S2.160. Управление антивирусными программами.
S2.161. Разработка концепции использования криптографии.
S2.162. Необходимость использования криптографических продуктов.
S2.163. Факторы, влияющие на выбор криптографических продуктов.
S2.164. Выбор адекватных процедур криптографической защиты.
S2.165. Выбор подходящих криптографических продуктов.
S2.166. Организационные аспекты использования криптографии.
S2.167. Обеспечение безопасности при уничтожении носителей информации.

S2.168. Системный анализ информационной системы, предшествующий выбору системы управления.

S2.169. Разработка стратегических целей системы управления.

S2.170. Требования к системе управления.

S2.171. Выбор продуктов для использования в системе управления.

S2.172. Разработка концепции использования WWW.

S2.173. Определение стратегии безопасности для WWW.

S2.174. Вопросы безопасности, связанные с сервером WWW.

S2.175. Настройки сервера WWW.

S2.176. Выбор Internet-провайдера.

S2.177. Обеспечение безопасности при переездах.

S2.178. Руководство по использованию факса.

S2.179. Процедуры управления факс-сервером.

S2.180. Настройки fax/mail-серверов.

S2.181. Выбор подходящего факс-сервера.

S2.182. Регулярный пересмотр критериев безопасности.

S2.183. Анализ аспектов безопасности, связанных с удаленным доступом.

S2.184. Разработка концепции безопасности удаленного доступа.

S2.185. Выбор архитектуры удаленного доступа.

S2.186. Выбор продукта, обеспечивающего безопасность удаленного доступа.

S2.187. Определение настроек продукта, обеспечивающего безопасность удаленного доступа.

S2.188. Правила использования мобильной связи.

S2.189. Блокирование мобильных телефонов в случае их утраты.

S2.190. Настройки пула мобильных телефонов.

S2.191. Процедуры, обеспечивающие ИБ (организационные аспекты).

S2.192. Политика безопасности и ее изменение.

S2.193. Организационная структура в области ИБ.

S2.194. Описание существующей информационной системы.

S2.195. Разработка (модернизация) концепции ИБ.

S2.196. Синхронизация этапов концепции ИБ и этапов развития системы.

S2.197. Концепция обучения в области ИБ.

S2.198. Проведение обучения персонала.

S2.199. Поддержание режима ИБ.

S2.200. Подготовка докладов в области ИБ.

S2.201. Документирование процедур и процессов в области ИБ.

S2.202. Подготовка руководства по обеспечению ИБ (организационные аспекты).

S2.203. Подготовка взаимосвязанных документов в области ИБ.

S2.204. Предотвращение несанкционированного доступа в сетях.

S2.205. Обмен персональными данными.

S2.206. Планирование использования Lotus Notes.

S2.207. Руководство по безопасности Lotus Notes.

S2.208. Планирование доменной структуры и иерархии сертификатов Lotus Notes.

S2.209. Планирование использования Lotus Notes в системе Intranet.

S2.210. Планирование использования Lotus Notes в системе Intranet с доступом через браузер.

S2.211. Планирование использования Lotus Notes в демилитаризованной зоне.

S2.212. Организационные аспекты, связанные с уборкой помещений и техники.

S2.213. Поддержка технической инфраструктуры.

S2.214. Концепция операций в информационной технологии.

S2.215. Меры по коррекции ошибок.

S2.216. Санкционирование процедур для отдельных компонентов информационной технологии.

S2.217. Классификация информационных ресурсов.

S2.218. Процедуры контроля обмена данными в информационной системе.

S2.219. Постоянное документирование изменений в информационной системе.

S2.220. Руководство по управлению доступом.

S2.221. Управление изменениями.

S2.222. Регулярная проверка параметров режима ИБ.

S2.223. Аспекты безопасности при использовании стандартного ПО.

S2.224. Защита от вредоносного ПО.

S2.225. Назначение ответственных за информационные ресурсы и отдельные компоненты информационной системы.

S2.226. Использование специалистов по временным трудовым договорам и специалистов сторонних организаций по договорам.

S3. Обеспечение безопасности на кадровом уровне

S3.1. Система обучения нового (поступающего на работу) персонала.

S3.2. Обязательства персонала в части следования законам и внутренним инструкциям.

S3.3. Проверка знаний сотрудников по исполнению своих обязанностей.

S3.4. Обучение перед использованием приложений.

S3.5. Обучение измерению параметров режима ИБ.

S3.6. Процедуры в отношении заканчивающих работу в компании.

S3.7. Пункты контракта в отношении личных проблем.

S3.8. Предотвращение конфликтов в коллективе.

S3.9. Эргономика рабочих помещений.

S3.10. Выбор надежного администратора безопасности и его замена.

S3.11. Обучение по вопросам эксплуатации средств защиты.

S3.12. Информирование персонала о возможностях местной АТС и о предупредительных сигналах.

S3.13. Уменьшение численности персонала, имеющего доступ к АТС и ее настройкам.

S3.14. Информирование персонала о процедурах корректного обмена данными с посторонними.

S3.15. Информирование персонала о процедурах корректного использования факсов.

S3.16. Информирование персонала о корректном использовании автоответчика.

S3.17. Информирование персонала о корректном использовании модема.

S3.18. Выключение ПК при уходе.

S3.19. Инструкции относительно корректного (безопасного) соединения взаимодействующих систем.

S3.20. Инструкции по защите служебных помещений от доступа посторонних.

S3.21. Обучение вопросам безопасности при использовании телекоммуникаций.

S3.22. Вопросы замены телекоммуникационного оборудования.

S3.23. Основы криптографической защиты.

S3.24. Обучение администраторов архитектуре Lotus Notes.

S3.25. Обучение пользователей механизмам безопасности Lotus Notes.

S3.26. Инструктаж персонала по вопросам безопасного использования (конфигурирования) элементов информационной технологии.

S4. Защита программного обеспечения и вычислительной техники

S4.1. Парольная защита.

S4.2. Использование экранных заставок для блокировки доступа.

S4.3. Периодическое использование антивирусных средств.

S4.4. Блокирование дисковода.

S4.5. Протоколирование действий администратора учрежденческой АТС.

S4.6. Аудит конфигурации учрежденческой АТС.

S4.7. Замена паролей.

S4.8. Защита консоли оператора учрежденческой АТС.

S4.9. Использование механизмов безопасности X Windows.

S4.10. Парольная защита терминалов учрежденческой АТС.

S4.11. Экранирование интерфейсов учрежденческой АТС.

S4.12. Удаление неиспользуемого оборудования.

S4.13. Выбор идентификаторов.

S4.14. Парольная защита в ОС UNIX.

S4.15. Безопасность при входе в систему.

S4.16. Ограничение доступа к терминалам.

S4.17. Блокирование доступа к неиспользуемым устройствам и терминалам.

S4.18. Административные и технические средства контроля работы пользователей.

S4.19. Ограничения на атрибуты файлов и директорий в UNIX (правила администрирования).

S4.20. Ограничения на атрибуты файлов и директорий в UNIX (правила для пользователей).

S4.21. Предотвращение незаконного использования прав администратора.

S4.22. Предотвращение потери конфиденциальных и важных данных в UNIX.

S4.23. Обеспечение безопасности EXE-файлов.

S4.24. Обеспечение управления системой.

S4.25. Использование log-файлов в ОС UNIX.

S4.26. Проверка режима безопасности в ОС UNIX.

S4.27. Парольная защита в портативных ПК.

S4.28. Смена системного ПО в случае изменения пользователя портативного ПК.

S4.29. Криптографическая защита в портативных ПК.

S4.30. Использование штатных средств безопасности прикладного ПО.

S4.31. Обеспечение электропитания при мобильном использовании портативного ПК.

S4.32. Уничтожение информации до и после использования средств хранения данных.

S4.33. Антивирусный контроль при передаче данных.

S4.34. Использование криптографии, контрольных сумм, ЭЦП.

S4.35. Проверка правильности перенаправления потоков данных.

S4.36. Блокирование учетной информации, передаваемой по факсу.

S4.37. Блокирование номера отправителя факса.

S4.38. Удаление сервисов, не являющихся необходимыми.

S4.39. Отключение автоответчиков на период длительного отсутствия.

S4.40. Предотвращение несанкционированного использования микрофонов.

S4.41. Использование подходящих программных продуктов для защиты информации.

S4.42. Инструментарий для обеспечения безопасности при работе приложений.

S4.43. Факсы с системой защиты от изменения установок.

S4.44. Проверка входящих файлов на отсутствие макровирусов.

S4.45. Обеспечение безопасности среды при взаимодействии объектов с равными правами.

S4.46 Использование паролей в ОС Windows 95.

S4.47. Ведение журналов при работе МЭ.

S4.48. Парольная защита в ОС Windows NT.

S4.49. Обеспечение защиты от загрузки с дискеты в ОС Windows NT.

S4.50. Системное администрирование в ОС Windows NT.

S4.51. Профили пользователей и ограничения в ОС Windows NT.

S4.52. Защита оборудования, функционирующего под управлением ОС Windows NT.

S4.53. Ограничения на доступ к файлам и директориям под управлением ОС Windows NT.

S4.54. Документирование событий в ОС Windows NT.

S4.55. Инсталляция ОС Windows NT в соответствии с требованиями безопасности.

S4.56. Уничтожение информации в ОС Windows NT и ОС Windows 95.

S4.57. Отключение возможности использования CD-ROM.

S4.58. Совместное использование файлов в ОС Windows 95.

S4.59. Отключение неиспользуемых функций ISDN.

S4.60. Отключение ненужных функций маршрутизации ISDN.

S4.61. Использование штатных механизмов безопасности компонентов ISDN.

S4.62. Использование фильтров.

S4.63. Выполнение требований в области информационной безопасности.

S4.64. Проверка данных перед отправкой и уничтожением.

S4.65. Предварительное тестирование оборудования и данных.

S4.66. Novell Netware - проверка решения «проблемы 2000».

S4.67. Блокирование и удаление регистрации пользователей баз данных, которым она более не требуется.

S4.68. Управление базой данных.

S4.69. Регулярная проверка состояния безопасности в СУБД.

S4.70. Мониторинг состояния базы данных.

S4.71. Ограничение на использование связей, имеющихся в СУБД.

S4.72. Криптографическая защита СУБД. S4.73. Спецификация на ограничение.

S4.74. Сети с ПК под управлением ОС Windows 95.

S4.75. Защита регистра в ПК под управлением ОС Windows NT.

S4.76. Версии ОС Windows NT с повышенным уровнем безопасности.

S4.77. Защита администратора в сетях на основе ОС Windows NT.

S4.78. Безопасность при модернизации.

S4.79. Механизмы безопасности при локальном администрировании.

S4.80. Механизмы безопасности при удаленном администрировании.

S4.81. Аудит журналов (log-файлов) с записями о сетевой активности.

S4.82. Вопросы безопасности при конфигурировании активного сетевого оборудования.

S4.83. Обновление компонентов сетевой инфраструктуры и ПО.

S4.84. Использование механизмов безопасности BIOS.

S4.85. Интерфейс модулей криптозащиты.

S4.86. Безопасность при разделении ролей персонала и конфигурировании криптомодулей.

S4.87. Физическая безопасность криптографических устройств.

S4.88. Требования к операционным системам, в которых устанавливаются криптомодули.

S4.89. Безопасность излучения (уровней полей) приборов.

S4.90. Использование криптографической защиты на разных уровнях модели ISO/OSI.

S4.91. Безопасность при инсталляции системы управления.

S4.92. Безопасность выполнения операций в системе управления.

S4.93. Регулярная проверка целостности.

S4.94. Защита WWW-файлов.

S4.95. Минимизация действий в информационной системе.

S4.96. Отключение DNS.

S4.97. Один сервис на один сервер.

S4.98. Ограничение потоков информации путем использования пакетных фильтров.

S4.99. Защиты от изменения информации.

S4.100. Межсетевые экраны и защита информационных ресурсов.

S4.101. Межсетевые экраны и криптография.

S4.102. Обеспечение уровня безопасности C2 для Novell 4.11.

S4.103. Сервер DHCP (Dynamic Host Configuration Protocol) под Novell Netware 4.x.

S4.104. Сервисы LDAP для NDS.

S4.105. Первоначальные измерения после инсталляции UNIX.

S4.106. Активация системных log-файлов.

S4.107. Сервисная поддержка производителя.

S4.108. Управление сервисом DNS под Novell NetWare 4.11.

S4.109. Переустановка ПО на рабочих станциях.

S4.110. Безопасность при инсталляции службы удаленного доступа.

S4.111. Безопасная конфигурация службы удаленного доступа.

S4.112. Безопасная работа с использованием службы удаленного доступа.

S4.113. Использование сервера аутентификации внутри службы удаленного доступа.

S4.114. Безопасность при использовании мобильных телефонов.

S4.115. Безопасность электропитания в мобильных телефонах.

S4.116. Безопасность при инсталляции Lotus Notes.

S4.117. Безопасность при конфигурировании сервера Lotus Notes.

S4.118. Конфигурирование сервера Lotus Notes.

S4.119. Ограничения по доступу к серверу Lotus Notes.

S4.120. Конфигурирование доступа к управляющим спискам базы данных Lotus Notes.

S4.121. Конфигурирование прав доступа к Lotus Notes Name и Address Book.

S4.122. Конфигурирование браузера доступа к Lotus Notes.

S4.123. Конфигурирование SSL в браузере доступа к Lotus Notes.

S4.124. Конфигурирование механизма аутентификации при доступе к Lotus Notes.

S4.125. Установление ограничений доступа к базам данных Lotus Notes через браузер.

S4.126. Безопасность при конфигурировании клиента Lotus Notes.

S4.127. Конфигурация браузера доступа к Lotus Notes, соответствующая требованиям безопасности.

S4.128. Работа в Lotus Notes (аспекты безопасности).

S4.129. Поддержка файлов Notes ID (аспекты безопасности).

S4.130. Оценка уровня безопасности при создании базы данных Lotus Notes.

S4.131. Использование криптографии в базе данных Lotus Notes.

S4.132. Мониторинг в Lotus Notes.

S4.133. Выбор подходящего механизма аутентификации.

S4.134. Выбор подходящих форматов данных.

S4.135. Ограничения, которые позволят контролировать доступ к файлам.

S5. Защита коммуникаций

S5.1. Удаление или заземление неиспользуемых линий.

S5.2. Выбор подходящей топологии сети.

S5.3. Выбор кабелей.

S5.4. Документирование и маркировка кабелей.

S5.5. Прокладка кабелей с учетом минимизации возможных повреждений.

S5.6. Разрешение использования сетевых паролей.

S5.7. Управление сетью.

S5.8. Ежемесячные проверки сети с позиции безопасности.

S5.9. Ведение журналов.

S5.10. Ограничение прав доступа.

S5.11. Блокировка консоли сервера.

S5.12. Конфигурации для второго (дублирующего) администратора.

S5.13. Оборудование для соединения сетей.

S5.14. Экранирование удаленного доступа.

S5.15. Экранирование доступа извне.

S5.16. Обзор сетевых сервисов.

S5.17. Использование механизмов безопасности для NFS.

S5.18. Использование механизмов безопасности для NIS.

S5.19. Использование механизмов безопасности для sendmail.

S5.20. Использование механизмов безопасности для rlogin, rsh. rcp.

S5.21. Безопасность для telnet, ftp, tftp. rexec.

S5.22. Проверка совместимости систем приема и передачи.

S5.23. Выбор подходящего телекоммуникационного оборудования.

S5.24. Список доступа для fax.

S5.25. Анализ принятых и посланных log-файлов.

S5.26. Извещение о пришедших факсах по телефону.

S5.27. Подтверждение о пришедших факсах по телефону.

S5.28. Подтверждение корректности пришедших факсов по телефону.

S5.29. Периодические проверки списков рассылки.

S5.30. Включение опции call-back.

S5.31. Конфигурирование модемов.

S5.32. Вопросы безопасности при использовании коммуникационного ПО.

S5.33. Безопасность при использовании удаленных модемов.

S5.34. Одноразовые пароли.

S5.35. Использование механизмов безопасности UUCP.

S5.36. Криптография под UNIX и Windows NT.

S5.37. Ограничение возможностей взаимодействующих объектов одного уровня при использовании ОС Windows 95 и Windows NT в сетях, поддерживающих серверы.

S5.38. Безопасность интеграции ПК под управлением ОС DOS в сети под управлением ОС UNIX.

S5.39. Безопасность использования протоколов и сервисов.

S5.40. Безопасность интеграции ПК под управлением ОС DOS в сети под управлением ОС Windows NT.

S5.41. Настройки, обеспечивающие безопасность удаленного доступа под управлением ОС Windows NT.

S5.42. Конфигурирование сетей TCP/IP под управлением ОС Windows NT.

S5.43. Конфигурирование сетевых сервисов TCP/IP под управлением ОС Windows NT.

S5.44. Однонаправленное соединение модема.

S5.45. Безопасность браузера.

S5.46. Инсталляция автономных систем при использовании Internet.

S5.47. Конфигурирование замкнутых групп пользователей.

S5.48. Аутентификация телефонных звонков с использованием определителя номера (CLIP/COLP).

S5.49. Обратный вызов по зафиксированному определителем номеру.

S5.50. Аутентификация в ISDN с использованием протоколов PAP/CHAP.

S5.51. Требования в области безопасности к телекоммуникациям через публичные сети.

S5.52. Требования в области безопасности к компьютерам, выполняющим телекоммуникационные функции.

S5.53. Защита от вредоносного ПО, передаваемого по почте.

S5.54. Защита от переполнения почтового ящика и спама.

S5.55. Проверка псевдонимов и списков рассылки.

S5.56. Безопасность почтового сервера.

S5.57. Безопасная конфигурация почтовых клиентов.

S5.58. Инсталляция драйверов ODBC (Open Database Connectivity).

S5.59. Защита от несанкционированных действий в отношении DNS.

S5.60. Выбор подходящей технологии базовых сетей (backbone).

S5.61. Выбор подходящей физической сегментации.

S5.62. Выбор подходящей логической сегментации.

S5.63. Использование криптографии с открытыми ключами (PGP).

S5.64. Безопасное окружение.

S5.65. Использование S-HTTP.

S5.66. Использование SSL.

S5.67. Использование службы контроля времени.

S5.68. Использование криптозащиты в сетях.

S5.69. Защита от активного контента.

S5.70. Использование Network address translation (NAT).

S5.71. Активный аудит.

S5.72. Удаление ненужных сетевых сервисов.

S5.73. Обеспечение безопасности при работе с факс-сервером.

S5.74. Поддержка адресной книги и списков рассылки факс-сервера.

S5.75. Защита от переполнения факс-сервера.

S5.76. Использование подходящих туннельных протоколов в сетях.

S5.77. Разбиение на подсети.

S5.78. Защита данных, передаваемых через мобильные телефоны, от использования в системе аутентификации.

S5.79. Защита от применения автоматически определенного номера мобильного телефона в системах аутентификации при использовании мобильных телефонов.

S5.80. Защита от утечки информации (подслушивания) с помощью мобильных телефонов.

S5.81. Безопасность при передаче данных через мобильные телефоны.

S5.82. Безопасность при использовании протокола SAMBA

S5.83. Безопасность при соединении с внешними сетями под Linux FreeS/WAN.

S5.84. Процедуры криптографической защиты при использовании Lotus Notes.

S5.85. Криптографическая защита e-mail Lotus Notes.

S5.86. Процедуры криптографической защиты при доступе через браузер к Lotus Notes.

S5.87. Соглашения, регулирующие связи с сетями третьих сторон.

S5.88. Соглашения, регулирующие вопросы передачи данных по сетям третьих сторон.

S6. Планирование непрерывности бизнеса

S6.1. Формулировка требований по доступности.

S6.2. Определение категорий опасности, персональная ответственность за обеспечение безопасности.

S6.3. Руководство по процедурам обеспечения безопасности.

S6.4. Требования к ресурсам, необходимым для работы приложений.

S6.5. Режим работы с минимальными ресурсами. Приоритеты информационных процессов.

S6.6. Исследование внешних и внутренних возможностей обеспечения бесперебойной работы.

S6.7. Ответственные за действия в чрезвычайных ситуациях.

S6.8. План действий в чрезвычайных ситуациях.

S6.9. План обеспечения бесперебойной работы в отдельных ситуациях.

S6.10. План обеспечения бесперебойной работы при выходе из строя связи.

S6.11. План восстановления нормальной работы.

S6.12. Тренировки по работе в чрезвычайных ситуациях.

S6.13. Резервное копирование и восстановление данных.

S6.14. План поставки оборудования.

S6.15. Соглашения с поставщиками.

S6.16. Страхование.

S6.17. Звуковая сигнализация на случай чрезвычайных обстоятельств.

S6.18. Обеспечение избыточности линий.

S6.19. Резервное копирование данных на ПК.

S6.20. Подходящие носители информации для резервного копирования.

S6.21. Резервное копирование программного обеспечения.

S6.22. Проверки качества резервных копий.

S6.23. Процедуры при обнаружении вирусов.

S6.24. Аспекты безопасности, связанные с FDD (дискеты).

S6.25. Регулярное резервное копирование жесткого диска сервера.

S6.26. Регулярное копирование данных конфигурации.

S6.27. Регулярное копирование CMOS RAM.

S6.28. Соглашение о сроках поставки отдельных элементов офисной АТС.

S6.29. Вызовы офисной АТС, связанные с авариями и безопасностью.

S6.30. Аварийные коммуникации.

S6.31. Примеры действий, приводящих к потере целостности данных.

S6.32. Регулярное резервное копирование данных.

S6.33. Политика резервного копирования.

S6.34. Определение факторов, препятствующих выполнению резервного копирования.

S6.35. Условия начала процедуры резервного копирования.

S6.36. Данные и ПО, подлежащие обязательному копированию.

S6.37. Документирование процедуры резервного копирования.

S6.38. Резервное копирование передаваемых данных.

S6.39. Процедуры, связанные с вводом в действие нового факса.

S6.40. Контроль и своевременная замена аккумуляторов.

S6.41. Обучение восстановлению данных.

S6.42. Создание start-up-дисков для Windows NT.

S6.43. Избыточность ресурсов в серверах Windows NT.

S6.44. Резервное копирование Windows NT.

S6.45. Резервное копирование Windows 95.

S6.46. Создание start-up-дисков для Windows 95.

S6.47. Хранение резервных копий как часть организации телекоммуникационных процедур.

S6.48. Процедуры в случае потери целостности базы данных.

S6.49. Резервное копирование баз данных.

S6.50. Активизация баз данных.

S6.51. Восстановление баз данных.

S6.52. Регулярное резервное копирование информации о конфигурационных данных.

S6.53. Дополнительные условия, связанные с установкой сетевых компонентов.

S6.54. Процедуры в случае нарушения целостности сети.

S6.55. Уменьшение времени нового запуска серверов под управлением ОС Novell Netware.

S6.56. Резервное копирование с криптографической защитой данных.

S6.57. Разработка планов бесперебойной работы на случай отказа системы управления.

S6.58. Система разбора и анализа инцидентов в области ИБ.

S6.59. Спецификация нарушений в области ИБ.

S6.60. Действия в случае обнаружения нарушений в области ИБ.

S6.61. Стратегия уклонения от инцидентов в области ИБ.

S6.62. Приоритеты при реагировании на инциденты в области ИБ.

S6.63. Расследование и оценка последствий инцидентов.

S6.64. Коррективы, вносимые после инцидентов.

S6.65. Оповещение об инцидентах.

S6.66. Оценка серьезности инцидентов.

S6.67. Фиксация инцидента и определение степени его серьезности.

S6.68. Проверка эффективности системы управления предотвращением инцидентов.

S6.69. Планирование бесперебойной работы для факс-серверов.

S6.70. Планирование бесперебойной работы для удаленных и мобильных элементов системы.

S6.71. Резервное копирование данных на мобильных ПК.

S6.72. Отказ мобильной связи.

S6.73. Планирование бесперебойной работы в случае сбоев Lotus Notes.

S6.74. Ведение архива аварий и инцидентов.

S6.75. Избыточность коммуникационных каналов.