Определение класса ИС

Время чтения: 4 минуты

Классификатор информационной системы

Класс информационной системы

5-гос 3-ин 3-юл

Предъявляемые требования

Примечание: Отметка НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ означает, что владелец ИС по своему усмотрению может выполнять или не выполнять данное требование информационной безопасности и самостоятельно выбирать меры и средства для реализации данных требований.

Все остальные требования (не отмеченные как необязательные) ДОЛЖНЫ быть реализованы в информационной системе определённого выше класса (или совокупности классов).

- 1.1 Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности, информация о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации и другое)
- 1.2 Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года Пример реализации
- 1.3 Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года Пример реализации
- 1.4 Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности

уполномоченными на это пользователями информационной системы Пример реализации

- 1.5 Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года Пример реализации

2. Требования по обеспечению защиты данных

- 2.1 Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием
- 2.2 Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации
- 2.3 Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности Пример реализации

3. Требования по обеспечению идентификации и аутентификации

- 3.1 Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации Пример реализации
- 3.2 Обеспечение идентификации и аутентификации пользователей информационной системы
- 3.3 Обеспечение защиты обратной связи при вводе аутентификационной информации
- 3.4 Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей

информационной системы
- 3.5 Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы
- 3.6 Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы
- 3.7 Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу

4. Требования по защите системы защиты информации информационной системы

- 4.1 Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию
- 4.2 Обеспечение обновления объектов информационной системы
- 4.3 Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы
- 4.4 Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации

5. Обеспечение криптографической защиты информации

- 5.1 Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного шифрования), если не осуществлено предварительное шифрование защищаемой информации Пример реализации

- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  5.2 Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)
- 5.3 Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)
- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  5.4 Обеспечение контроля целостности данных в информационной системе (средства контроля целостности) Пример реализации
- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  5.5 Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены)
- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  5.6 Обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в информационной системе (криптографический токен и (или) средства выработки электронной цифровой подписи)

6. Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре

- 6.1 Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг
- 6.2 Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин
- 6.3 Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных
- 6.4 Обеспечение резервного копирования пользовательских виртуальных машин

- 6.5 Обеспечение резервирования сетевого оборудования по схеме N+1
- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  6.6 Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам

- 7.1 Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования
- 7.2 Обеспечение контроля за составом объектов информационной системы Пример реализации
- 7.3 Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования
- 7.4 Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы)
- 7.5 Определение состава и содержания информации, подлежащей резервированию
- 7.6 Обеспечение резервирования информации, подлежащей резервированию
- 7.7 Обеспечение резервирования конфигурационных файлов сетевого оборудования
- 7.8 Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления
- 7.9 Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных
  Пример реализации

- 7.10 Обеспечение защиты средств вычислительной техники от вредоносных программ
- 7.11 Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ
- 7.12 Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ
- 7.13 Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего) Пример реализации
- 7.14 Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях Пример реализации
- 7.15 Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях Пример реализации
- 7.16 Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений Пример реализации
- 7.17 Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений

- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  7.18 Обеспечение обнаружения утечек информации из информационной системы. Использование системы обнаружения утечек информации из информационной системы
- 7.19 Определение перечня внешних подключений к информационной системе и порядка такого подключения
- 7.20 Обеспечение контроля за внешними подключениями к информационной системе Пример реализации
- НЕОБЯЗАТЕЛЬНОЕ ТРЕБОВАНИЕ:
  7.21 Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы Пример реализации

Теперь вы можете заполнить акт отнесения вашей информационной системы к классу типовых информационных систем

Акт отнесения информационной системы к классу типовых ИС