Рекомендации по обеспечению защиты общедоступной информации в информационных системах

Для целей настоящих рекомендаций применяются термины в значениях, определенных в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», а также следующий термин и его определение:

объекты информационной системы – средства вычислительной техники, сетевое оборудование, системное и прикладное программное обеспечение, средства технической и криптографической защиты информации (ОИС).

Рекомендуется реализовать следующие меры в собственных информационных системах (ИС), а также контролировать их выполнение подчиненными организациями.

Защита ОИС

1. Обеспечить защиту средств вычислительной техники (СВТ) от вредоносного программного обеспечения.
2. Использовать криптографические алгоритмы защиты информации, интегрированные в программное обеспечение (ПО), в том числе самих носителей информации.
3. Отключить функции автозагрузки внешних машинных носителей информации при их подключении к СВТ.
4. Обеспечить контроль (автоматизированный) за составом ОИС.
5. Определить перечень разрешенного ПО, регламентировать и контролировать порядок его установки и использования.
6. Регламентировать порядок использования внешних машинных носителей информации, мобильных технических средств.

Управление доступом и идентификация пользователей

7. Использовать ОИС с правами пользовательских учетных записей.
8. Обеспечить управление (централизованное) (создание, активация, блокировка, уничтожение) учетными записями пользователей для доступа к ОИС.
9. Ограничить возможности использования общих учетных записей пользователей для доступа к ОИС.
10. Разграничить доступ пользователей к ОИС.
11. Обеспечить идентификацию и аутентификацию пользователей ИС.

12. Своевременно блокировать (уничтожать) неиспользуемые (временно неиспользуемые) учетные записи пользователей.
13. Обеспечить доступ пользователей к ОИС на основе ролей.
14. Блокировать доступ к ОИС после истечения установленного времени бездействия (неактивности) пользователя или по его запросу.
15. Обеспечить изменение атрибутов безопасности сетевого оборудования, ПО, установленных по умолчанию.
16. Ограничить количество неуспешных попыток доступа к ОИС.
17. Контролировать соблюдение правил генерации и смены паролей пользователей.
18. Обеспечить управление физическим доступом в помещения, а также к шкафам со СВТ, сетевым и другим оборудованием.
19. Предоставлять уникальные учетные записи привилегированных пользователей для авторизованного доступа к сетевому оборудованию.
20. Предоставлять временные учетные записи пользователей для авторизованного доступа в целях обслуживания ОИС неуполномоченными сотрудниками (сторонними организациями), обеспечить их контроль и отключение.
21. Предоставлять пользователям авторизованный доступ при подключении к ОИС из-за ее пределов.

Защита почтовых серверов

22. Использовать услуги хостинга уполномоченных поставщиков интернет-услуг.
23. Обеспечить в реальном масштабе времени автоматическую антивирусную проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ.
24. Обеспечить спам-фильтрацию почтовых сообщений.
25. Использовать механизмы шифрования почтовых сообщений и (или) передачу почтовых сообщений с использованием криптографических протоколов передачи данных (SMTPS, STARTTLS).
26. Обеспечить фильтрацию почтовых сообщений с использованием списков нежелательных отправителей почтовых сообщений.
27. Использовать механизмы проверки PTR-записи почтовых сервисов.
28. Использовать механизмы проверки SPF-записи почтовых сервисов.
29. Использовать механизмы почтовой аутентификации отправителя почтовых сообщений (DKIM).
30. Блокировать массовую рассылку почтовых сообщений.

Менеджмент активов

31. Обеспечить централизованный учет информации об ОИС, разработать схемы физических и(или) логических соединений данных объектов с указанием активов с высоким уровнем важности.
32. Регламентировать порядок удаления информации с машинных носителей информации в случае вывода их из эксплуатации.
33. Регламентировать порядок хранения неиспользуемых машинных носителей информации.

Менеджмент сети

34. Обеспечить сегментацию (изоляцию) сети доступа в Интернет от сети передачи данных (СПД) ИС.
35. Обеспечить сегментацию (изоляцию) сети управления ОИС системами видеонаблюдения, СКУД и другими объектами от СПД ИС.
36. Обеспечить сегментацию (изоляцию) сети доступа в Интернет сторонних пользователей от СПД ИС.
37. Ограничить входящий и исходящий трафик (фильтрация) определенных приложений и сервисов (мессенджеры, социальные сети, онлайн-маркеты, анонимайзеры и др.).
38. Ограничить входящий и исходящий трафик (фильтрация) ИС только необходимыми соединениями (использование межсетевого экрана).
39. Отключить неиспользуемые порты сетевого оборудования.
40. Обнаруживать и предотвращать вторжения в ИС (IPS/IDS).
41. Обеспечить доступ пользователей в сеть Интернет с применением технологии проксирования сетевого трафика.
42. Использовать ОИС локальной системы доменных имен (DNS-сервер), в том числе для доступа в сеть Интернет, либо системы доменных имен, расположенной на территории Республики Беларусь.

Менеджмент уязвимостей

43. Периодически, но не менее одного раза в год осуществлять контроль отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих ОИС.
44. Обеспечить обновление ПО ОИС.
45. Обеспечить исправление выявленных уязвимостей ОИС.

Аудит безопасности

46. Разработать и внедрить план реагирования на инциденты информационной безопасности.

47. Организовать взаимодействие с подразделениями информационной безопасности (командами реагирования на компьютерные инциденты) по вопросам управления событиями (инцидентами) информационной безопасности.
48. Сформировать подразделения либо назначить сотрудника(ов), ответственных за информационную безопасность.
49. Обеспечить централизованный сбор и хранение не менее одного года информации о функционировании СВТ, средств защиты информации, сетевого оборудования, систем, сервисов (netflow-трафик, лог-файлы запросов пользователей к локальным системам доменных имен, лог-файлы системы проксирования подключения к сети Интернет, лог-файлы предоставления пользователям динамических ip-адресов, лог-файлы работы серверов печати и др.), о действиях пользователей, а также о событиях информационной безопасности.
50. Периодически, но не менее одного раза в неделю осуществлять мониторинг (просмотр, анализ) событий информационной безопасности, функционирования ОИС.
51. Обеспечить защиту от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования и системного ПО, средствам защиты информации и событиям безопасности.
52. Осуществлять контроль за внешними подключениями к ИС.

Резервирование информации

53. Определить состав и содержание информации, подлежащей резервированию (в том числе конфигурационных файлов сетевого оборудования, лог-файлов служб и сервисов).
54. Обеспечить резервирование информации.

Дополнительные рекомендации

55. Осуществлять синхронизацию системного времени от единого источника.

Защита виртуальной инфраструктуры

56. Обеспечить защиту виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин.