ПРАВИТЕЛЬСТВО РОСТОВСКОЙ ОБЛАСТИ
МИНИСТЕРСТВО ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ И СПОРТУ РОСТОВСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

18.05.2018 **г. Ростов-на-Дону** **№ 2**

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых министерством по физической культуре и спорту Ростовской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» **п о с т а н о в л я ю** :

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых министерством по физической культуре и спорту Ростовской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки, согласно приложению.

2. Настоящее постановление вступает в силу со дня его официального опубликования.

3. Контроль за выполнением настоящего постановления возложить на заместителя министра Злобина И.И.

Министр С.Р. Аракелян

Приложение
к постановлению
министерства по физической
культуре и спорту
Ростовской области
от 18.05.2018 № 2

Угрозы безопасности персональных данных,
актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых министерством по физической культуре и спорту Ростовской области при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

1. Угроза анализа криптографических алгоритмов и их реализации.
2. Угроза аппаратного сброса пароля BIOS.
3. Угроза внедрения кода или данных.
4. Угроза воздействия на программы с высокими привилегиями.
5. Угроза восстановления аутентификационной информации.
6. Угроза деструктивного изменения конфигурации/среды окружения программ.
7. Угроза доступа к защищаемым файлам с использованием обходного пути.
8. Угроза доступа к локальным файлам сервера при помощи URL.
9. Угроза доступа/перехвата/изменения HTTP cookies.
10. Угроза загрузки нештатной операционной системы.
11. Угроза заражения DNS-кеша.
12. Угроза изменения компонентов системы.
13. Угроза искажения XML-схемы.
14. Угроза использования альтернативных путей доступа к ресурсам.
15. Угроза использования информации идентификации/аутентификации, заданной по умолчанию.
16. Угроза использования механизмов авторизации для повышения привилегий.
17. Угроза использования слабостей протоколов сетевого/локального обмена данными.
18. Угроза исследования механизмов работы программы.
19. Угроза межсайтовой подделки запроса.
20. Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера.
21. Угроза некорректного использования функционала программного обеспечения.
22. Угроза неправомерного ознакомления с защищаемой информацией.
23. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.
24. Угроза неправомерных действий в каналах связи.

25. Угроза несанкционированного восстановления удалённой защищаемой информации.

26. Угроза несанкционированного доступа к аутентификационной информации.

27. Угроза несанкционированного копирования защищаемой информации.

28. Угроза несанкционированного редактирования реестра.

29. Угроза несанкционированного создания учётной записи пользователя.

30. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.

31. Угроза обнаружения хостов.

32. Угроза обхода некорректно настроенных механизмов аутентификации.

33. Угроза опосредованного управления группой программ через совместно используемые данные.

34. Угроза перехвата привилегированного потока.

35. Угроза перехвата привилегированного процесса.

36. Угроза повышения привилегий.

37. Угроза подмены действия пользователя путём обмана.

38. Угроза подмены доверенного пользователя.

39. Угроза преодоления физической защиты.

40. Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL.

41. Угроза утраты носителей информации.

42. Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.

43. Угроза эксплуатации цифровой подписи программного кода.

44. Угроза перехвата исключения/сигнала из привилегированного блока функций.

45. Угроза заражения компьютера при посещении неблагонадёжных сайтов.

46. Угроза скрытного включения вычислительного устройства в состав бот-сети.

47. Угроза распространения «почтовых червей».

48. Угроза «фишинга».

49. Угроза несанкционированного использования системных и сетевых утилит.

50. Угроза несанкционированного изменения параметров настройки средств защиты информации.

51. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.

52. Угроза несанкционированного воздействия на средство защиты информации.

53. Угроза маскирования действий вредоносного кода.

54. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в информационно-телекоммуникационной сети «Интернет».

55. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

56. Угроза использования уязвимых версий программного обеспечения.

57. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика.

58. Угроза хищения аутентификационной информации из временных файлов cookie.

59. Угроза скрытной регистрации вредоносной программой учетных записей администраторов.

60. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере.

61. Проведение атаки при нахождении в пределах контролируемой зоны.

62. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы, сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы, сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования.

63. Физический доступ к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среда функционирования.

Заместитель министра
по физической культуре и спорту
Ростовской области  И.И. Злобин