РОССИЙСКАЯ ФЕДЕРАЦИЯ

РАСПОРЯЖЕНИЕ

ГЛАВЫ КАРАЧАЕВО-ЧЕРКЕССКОЙ РЕСПУБЛИКИ

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Главы и Правительства Карачаево-Черкесской Республики и органах исполнительной власти Карачаево-Черкесской Республики при осуществлении соответствующих видов деятельности с учетом содержания персональных данных, характера и способов их обработки

В соответствии с частью 5 статьи 19 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», в целях совершенствования системы защиты персональных данных, обрабатываемых в информационных системах персональных данных Администрации Главы и Правительства Карачаево-Черкесской Республики и органах исполнительной власти Карачаево-Черкесской Республики при осуществлении соответствующих видов деятельности с учетом содержания персональных данных, характера и способов их обработки:

1. Утвердить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Главы и Правительства Карачаево-Черкесской Республики, органах исполнительной власти Карачаево-Черкесской Республики, согласно приложению.

2. Администрации Главы и Правительства Карачаево-Черкесской Республики, органам исполнительной власти Карачаево-Черкесской Республики при разработке частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных

данных, эксплуатируемых при осуществлении соответствующих видов деятельности, руководствоваться настоящим распоряжением.

Глава
Карачаево-Черкесской Республики Р.Б. Темрезов

г.Черкесск
Дом Правительства
02 декабря 2019 года
№ 348-р

Приложение к распоряжению
Главы Карачаево-Черкесской
Республики от 02.12.2019 № 348-р

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Главы и Правительства Карачаево-Черкесской Республики, органах исполнительной власти Карачаево-Черкесской Республики

1. Угроза аппаратного сброса пароля BIOS.
2. Угроза внедрения кода или данных.
3. Угроза восстановления аутентификационной информации.
4. Угроза восстановления предыдущей уязвимой версии BIOS.
5. Угроза деструктивного изменения конфигурации/среды окружения программ.
6. Угроза деструктивного использования декларированного функционала BIOS.
7. Угроза длительного удержания вычислительных ресурсов пользователями.
8. Угроза доступа к защищаемым файлам с использованием обходного пути.
9. Угроза доступа/перехвата/изменения HTTP cookies.
10. Угроза загрузки нештатной операционной системы.
11. Угроза заражения DNS-кеша.
12. Угроза избыточного выделения оперативной памяти.
13. Угроза изменения компонентов системы.
14. Угроза искажения вводимой и выводимой на периферийные устройства информации.
15. Угроза использования альтернативных путей доступа к ресурсам.
16. Угроза использования информации идентификации/аутентификации, заданной по умолчанию.
17. Угроза использования механизмов авторизации для повышения привилегий.
18. Угроза использования слабостей протоколов сетевого/локального обмена данными.
19. Угроза межсайтового скриптинга.
20. Угроза нарушения изоляции среды исполнения BIOS.
21. Угроза нарушения целостности данных кеша.
22. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания.
23. Угроза невозможности управления правами пользователей BIOS.

24. Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера.

25. Угроза неправомерного ознакомления с защищаемой информацией.

26. Угроза неправомерных действий в каналах связи.

27. Угроза несанкционированного восстановления удалённой защищаемой информации.

28. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.

29. Угроза несанкционированного доступа к аутентификационной информации.

30. Угроза несанкционированного изменения аутентификационной информации.

31. Угроза несанкционированного использования привилегированных функций BIOS.

32. Угроза несанкционированного копирования защищаемой информации.

33. Угроза несанкционированного редактирования реестра.

34. Угроза несанкционированного создания учётной записи пользователя.

35. Угроза несанкционированного удаления защищаемой информации.

36. Угроза несанкционированного управления буфером.

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

38. Угроза обнаружения хостов.

39. Угроза обхода некорректно настроенных механизмов аутентификации.

40. Угроза определения типов объектов защиты.

41. Угроза определения топологии вычислительной сети.

42. Угроза отключения контрольных датчиков.

43. Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.

44. Угроза перехвата вводимой и выводимой на периферийные устройства информации.

45. Угроза перехвата данных, передаваемых по вычислительной сети.

46. Угроза повреждения системного реестра.

47. Угроза подбора пароля BIOS.

48. Угроза подделки записей журнала регистрации событий.

49. Угроза подмены доверенного пользователя.

50. Угроза подмены резервной копии программного обеспечения BIOS.

51. Угроза подмены содержимого сетевых ресурсов.

52. Угроза приведения системы в состояние «отказ в обслуживании».

53. Угроза программного сброса пароля BIOS.

54. Угроза пропуска проверки целостности программного обеспечения.

55. Угроза удаления аутентификационной информации.

56. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.

57. Угроза утраты вычислительных ресурсов.

58. Угроза утраты носителей информации.

59. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.

60. Угроза форматирования носителей информации.

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

62. Угроза эксплуатации цифровой подписи программного кода.

63. Угроза заражения компьютера при посещении неблагонадёжных сайтов.

64. Угроза «кражи» учётной записи доступа к сетевым сервисам.

65. Угроза неправомерного шифрования информации.

66. Угроза скрытного включения вычислительного устройства в состав ботсети.

67. Угроза распространения «почтовых червей».

68. Угроза «фарминга».

69. Угроза «фишинга».

70. Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты.

71. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью.

72. Угроза несанкционированного использования системных и сетевых утилит.

73. Угроза несанкционированной модификации защищаемой информации.

74. Угроза отказа подсистемы обеспечения температурного режима.

75. Угроза физического устаревания аппаратных компонентов.

76. Угроза несанкционированного изменения параметров настройки средств защиты информации.

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

78. Угроза получения 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 СВТ, на которых реализованы СКЗИ и СФ.

79. Угроза возможности самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны.

80. Угроза возможности самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования.