СЛУЖБА ПО ТАРИФАМ АСТРАХАНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

29.06.2020 № 14

Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в службе по тарифам Астраханской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Астраханской области от 06.04.2005 № 49-П «О службе по тарифам Астраханской области», протоколом заседания коллегии службы по тарифам Астраханской области от 29.06.2020 № 31:
служба по тарифам Астраханской области ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в службе по тарифам Астраханской области.

2. Заведующему организационным сектором службы по тарифам Астраханской области:

2.1. В срок не позднее трех рабочих дней со дня подписания настоящего постановления направить его копию в министерство государственного управления, информационных технологий и связи Астраханской области для официального опубликования.

2.2. Не позднее семи рабочих дней со дня подписания настоящего постановления направить его копию в прокуратуру Астраханской области.

2.3. В семидневный срок после дня первого официального опубликования настоящего постановления направить его копию, а также сведения об источниках его официального опубликования в Управление Министерства юстиции Российской Федерации по Астраханской области.

2.4. В семидневный срок со дня принятия настоящего постановления направить его копию в справочно-правовые системы «КонсультантПлюс» ООО «РентаСервис» и «Гарант» ООО «Астрахань-Гарант-Сервис» для включения в электронные базы данных.

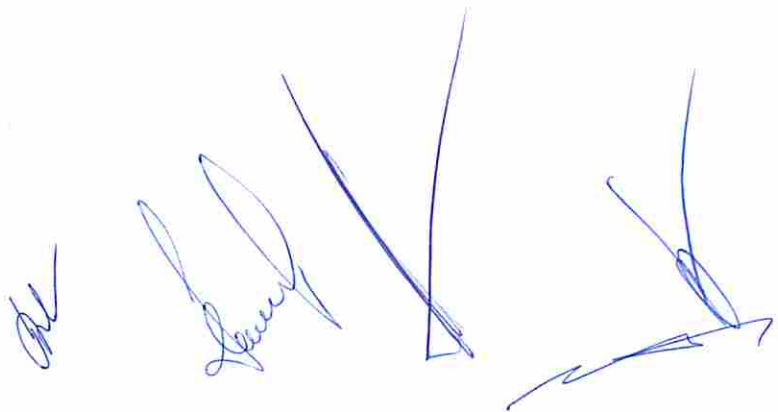
2.5. В семидневный срок со дня принятия настоящего постановления разместить его на официальном сайте службы по тарифам Астрахан-

004719 *

ской области в информационно-телекоммуникационной сети «Интернет» (www.astrtarif.ru).

3. Постановление вступает в силу по истечении 10 дней после дня его официального опубликования.

Руководитель О.В. Степанищева



УТВЕРЖДЕН
постановлением службы по
тарифам
Астраханской области
от 29.06.2020 № 14

Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в службе по тарифам Астраханской области

1. Угрозы утечки видовой информации
2. Угрозы утечки информации по каналам ПЭМИН
3. Кража ПЭВМ
4. Кража носителей информации
5. Кража ключей и атрибутов доступа
6. Кража информации
7. Действия вредоносных программ (вирусов)
8. Недекларированные возможности программного обеспечения СЗИ
9. Установка ПО, несвязанного с исполнением служебных обязанностей
10. Утрата ключей и атрибутов доступа
11. Непреднамеренное отключение СЗИ
12. Выход из строя аппаратно-программных средств
13. Сбой системы электроснабжения
14. Стихийное бедствие
15. Кража и разглашение информации лицами, допущенными к ее обработке
16. Несанкционированное отключение СЗИ
17. Угроза аппаратного сброса пароля BIOS (УБИ. 004)
18. Угроза внедрения вредоносного кода в BIOS (УБИ. 005)
19. Угроза внедрения кода или данных (УБИ. 006)
20. Угроза воздействия на программы с высокими привилегиями (УБИ. 007)

21. Угроза восстановления аутентификационной информации (УБИ. 008)
22. Угроза восстановления предыдущей уязвимой версии BIOS (УБИ. 009)
23. Угроза деструктивного изменения конфигурации/среды окружения программ (УБИ. 012)
24. Угроза деструктивного использования декларированного функционала BIOS (УБИ. 013)
25. Угроза длительного удержания вычислительных ресурсов пользователями (УБИ. 014)
26. Угроза доступа к защищаемым файлам с использованием обходного пути (УБИ. 015)
27. Угроза загрузки нештатной операционной системы (УБИ. 018)
28. Угроза избыточного выделения оперативной памяти (УБИ. 022)
29. Угроза изменения компонентов системы (УБИ. 023)
30. Угроза изменения режимов работы аппаратных элементов компьютера (УБИ. 024)
31. Угроза изменения системных и глобальных переменных (УБИ. 025)
32. Угроза искажения XML-схемы (УБИ. 026)
33. Угроза искажения вводимой и выводимой на периферийные устройства информации (УБИ. 027)
34. Угроза использования альтернативных путей доступа к ресурсам (УБИ. 028)
35. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания (УБИ. 051)
36. Угроза неправомерного ознакомления с защищаемой информацией (УБИ. 067)
37. Угроза несанкционированного восстановления удалённой защищаемой информации (УБИ. 071)
38. Угроза несанкционированного доступа к аутентификационной информации (УБИ. 074)
39. Угроза несанкционированного изменения аутентификационной информации (УБИ. 086)
40. Угроза несанкционированного копирования защищаемой информации (УБИ.

088)

41. Угроза несанкционированного редактирования реестра (УБИ. 089)
42. Угроза несанкционированного создания учётной записи пользователя (УБИ. 090)
43. Угроза несанкционированного удаления защищаемой информации (УБИ. 091)
44. Угроза несанкционированного управления буфером (УБИ. 093)
45. Угроза обнаружения хостов (УБИ. 099)
46. Угроза обхода некорректно настроенных механизмов аутентификации (УБИ. 100)
47. Угроза перебора всех настроек и параметров приложения (УБИ. 109)
48. Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники (УБИ. 113)
49. Угроза перехвата вводимой и выводимой на периферийные устройства информации (УБИ. 115)
50. Угроза перехвата привилегированного потока (УБИ. 117)
51. Угроза перехвата привилегированного процесса (УБИ. 118)
52. Угроза повреждения системного реестра (УБИ. 121)
53. Угроза повышения привилегий (УБИ. 122)
54. Угроза подбора пароля BIOS (УБИ. 123)
55. Угроза подделки записей журнала регистрации событий (УБИ. 124)
56. Угроза подмены действия пользователя путём обмана (УБИ. 127)
57. Угроза подмены резервной копии программного обеспечения BIOS (УБИ. 129)
58. Угроза получения предварительной информации об объекте защиты (УБИ. 132)
59. Угроза преодоления физической защиты (УБИ. 139)
60. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 143)
61. Угроза программного сброса пароля BIOS (УБИ. 144)
62. Угроза пропуска проверки целостности программного обеспечения (УБИ. 145)
63. Угроза сбоя процесса обновления BIOS (УБИ. 150)
64. Угроза удаления аутентификационной информации (УБИ. 152)
65. Угроза установки уязвимых версий обновления программного обеспечения

BIOS (УБИ. 154)

66. Угроза утраты вычислительных ресурсов (УБИ. 155)
67. Угроза утраты носителей информации (УБИ. 156)
68. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 157)
69. Угроза форматирования носителей информации (УБИ. 158)
70. Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ. 160)
71. Угроза внедрения системной избыточности (УБИ. 166)
72. Угроза наличия механизмов разработчика (УБИ. 169)
73. Угроза неправомерного шифрования информации (УБИ. 170)
74. Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты (УБИ. 176)
75. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью (УБИ. 177)
76. Угроза несанкционированной модификации защищаемой информации (УБИ. 179)
77. Угроза отказа подсистемы обеспечения температурного режима (УБИ. 180)
78. Угроза несанкционированного воздействия на средство защиты информации (УБИ. 187)
79. Угроза подмены программного обеспечения (УБИ. 188)
80. Угроза маскирования действий вредоносного кода (УБИ. 189)
81. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения (УБИ. 191)
82. Угроза использования уязвимых версий программного обеспечения (УБИ. 192)
83. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика (УБИ. 193)
84. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы (УБИ. 195)

85. Угроза хищения аутентификационной информации из временных файлов cookie (УБИ. 197)

86. Угроза скрытной регистрации вредоносной программной учетных записей администраторов (УБИ. 198)

87. Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты (УБИ.205)