ГОСУДАРСТВЕННАЯ ЖИЛИЩНАЯ ИНСПЕКЦИЯ РОСТОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 21.03.2019 № 1

г. Ростов-на-Дону

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационной системе персональных данных «Госжилинспекция РО» Государственной жилищной инспекции Ростовской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» Государственная жилищная инспекция Ростовской области, **п о с т а н о в л я е т:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационной системе персональных данных «Госжилинспекция РО» Государственной жилищной инспекции Ростовской области, согласно приложению.

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

3. Контроль за выполнением настоящего постановления оставляю за собой.

Начальник
Государственной жилищной инспекции
Ростовской области П.В. Асташев

Приложение
к постановлению
Государственной жилищной
инспекции Ростовской области
от 21.03.2019 № 1

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационной системе персональных данных «Госжилинспекция РО» Государственной жилищной инспекции Ростовской области:

1. Угроза аппаратного сброса пароля BIOS.
2. Угроза внедрения кода или данных.
3. Угроза воздействия на программы с высокими привилегиями.
4. Угроза восстановления аутентификационной информации.
5. Угроза восстановления предыдущей уязвимой версии BIOS.
6. Угроза деструктивного использования декларированного функционала BIOS.
7. Угроза доступа к защищаемым файлам с использованием обходного пути.
8. Угроза доступа/перехвата/изменения HTTP cookies.
9. Угроза загрузки нештатной операционной системы.
10. Угроза изменения компонентов системы.
11. Угроза использования альтернативных путей доступа к ресурсам.
12. Угроза использования механизмов авторизации для повышения привилегий.
13. Угроза исследования механизмов работы программы.
14. Угроза межсайтового скриптинга.
15. Угроза нарушения изоляции среды исполнения BIOS.
16. Угроза нарушения целостности данных кэша.
17. Угроза невозможности управления правами пользователей BIOS.
18. Угроза некорректного задания структуры данных транзакции.
19. Угроза некорректного использования функционала программного обеспечения.
20. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.
21. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
22. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.
23. Угроза несанкционированного доступа к аутентификационной информации.
24. Угроза несанкционированного изменения аутентификационной информации.
25. Угроза несанкционированного использования привилегированных функций BIOS.
26. Угроза несанкционированного копирования защищаемой информации.
27. Угроза несанкционированного редактирования реестра.

28. Угроза несанкционированного создания учётной записи пользователя.
29. Угроза несанкционированного удаления защищаемой информации.
30. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
31. Угроза обнаружения хостов.
32. Угроза определения типов объектов защиты.
33. Угроза определения топологии вычислительной сети.
34. Угроза отключения контрольных датчиков.
35. Угроза перебора всех настроек и параметров приложения.
36. Угроза передачи данных по скрытым каналам.
37. Угроза повреждения системного реестра.
38. Угроза подбора пароля BIOS.
39. Угроза подделки записей журнала регистрации событий.
40. Угроза подмены доверенного пользователя.
41. Угроза подмены резервной копии программного обеспечения BIOS.
42. Угроза приведения системы в состояние «отказ в обслуживании».
43. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
44. Угроза пропуска проверки целостности программного обеспечения.
45. Угроза сбоя процесса обновления BIOS.
46. Угроза удаления аутентификационной информации.
47. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.
48. Угроза установки уязвимых версий обновления программного обеспечения BIOS.
49. Угроза утраты вычислительных ресурсов.
50. Угроза утраты носителей информации.
51. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
52. Угроза форматирования носителей информации.
53. Угроза хищения средств хранения, обработки и (или) ввода/вывода/ передачи информации.
54. Угроза эксплуатации цифровой подписи программного кода.
55. Угроза включения в проект не достоверно испытанных компонентов.
56. Угроза внедрения системой избыточности.
57. Угроза наличия механизмов разработчика.
58. Угроза скрытого включения вычислительного устройства в состав бот-сети.
59. Угроза распространения «почтовых червей».
60. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью.
61. Угроза несанкционированной модификации защищаемой информации.
62. Угроза физического устаревания аппаратных компонентов.
63. Угроза несанкционированного изменения параметров настройки средств защиты информации.

64. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.
65. Угроза несанкционированного воздействия на средство защиты информации.
66. Угроза использования уязвимых версий программного обеспечения.
67. Угроза утечки информации с неподключенных к сети Интернет компьютеров.

Перечень возможностей нарушителей, которые могут использоваться при создании способов и направлении атак (актуальные угрозы):

1. Проведение атаки при нахождении в пределах контролируемой зоны.
2. 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 СВТ, на которых реализованы СКЗИ и СФ.
3. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.
4. Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.

Ответственный за информационную безопасность
в Государственной жилищной инспекции
Ростовской области

специалист-эксперт отдела делопроизводства
и контрольно-аналитической работы А.В. Живица