МИНИСТЕРСТВО ЭНЕРГЕТИКИ, ПРОМЫШЛЕННОСТИ И СВЯЗИ СТАВРОПОЛЬСКОГО КРАЯ

ПРИКАЗ

30 мая 2019 г. г. Ставрополь № 134- о/д

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности министерства энергетики, промышленности и связи Ставропольского края, с учетом содержания персональных данных, характера и способов их обработки

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях модернизации системы защиты информации в министерстве энергетики, промышленности и связи Ставропольского края

ПРИКАЗЫВАЮ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности министерства энергетики, промышленности и связи Ставропольского края (далее – министерство), с учетом содержания персональных данных, характера и способов их обработки согласно приложению к настоящему приказу.

2. Рекомендовать подведомственным министерству учреждениям определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки в соответствии с требованиями руководящих документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

3. Контроль за выполнением настоящего приказа возложить на заместителя министра Курашова Д.С.

4. Настоящий приказ вступает в силу на следующий день после дня его официального опубликования.

Министр В.П.Хоценко

Приложение

к приказу министерства энергетики,
промышленности и связи
Ставропольского края

от «30» мая 2019 г. № 134-о/д

УГРОЗЫ

безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности министерства энергетики, промышленности и связи Ставропольского края, с учетом содержания персональных данных, характера и способов их обработки

Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых для осуществления деятельности министерства энергетики, промышленности и связи Ставропольского края (далее – министерство), с учетом содержания персональных данных, характера и способов их обработки, в соответствии с документами ФСТЭК России являются:

№ п/п	Идентификатор угрозы	Название актуальной угрозы безопасности информации
1	2	3
1.	4	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой
2.	5	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, с применением специальных программ для осуществления НСД
3.	6	Угрозы внедрения вредоносных программ (локально)
4.	7	Угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации
5.	8	Угрозы сканирования, направленные на выявление типа операционной системы информационных систем, сетевых

		адресов рабочих станций, открытых портов и служб, открытых соединений
6.	9	Угрозы выявление паролей
7.	10	Угрозы получения несанкционированного доступа путем подмены доверенного объекта
8.	11	Угрозы типа «Отказ в обслуживании»
9.	12	Угрозы удалённого запуска приложений
10.	13	Угрозы внедрения по сети вредоносных программ
11.	УБИ.006	Угроза внедрения кода или данных
12.	УБИ.007	Угроза воздействия на программы с высокими привилегиями
13.	УБИ.008	Угроза восстановления аутентификационной информации
14.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
15.	УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
16.	УБИ.019	Угроза заражения DNS-кеша
17.	УБИ.023	Угроза изменения компонентов системы
18.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
19.	УБИ.030	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию
20.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
21.	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
22.	УБИ.049	Угроза нарушения целостности данных кеша
23.	УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера
24.	УБИ.063	Угроза некорректного использования функционала программного обеспечения
25.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
26.	УБИ.069	Угроза неправомерных действий в канал связи
27.	УБИ.071	Угроза несанкционированного восстановления удаленной защищаемой информации
28.	УБИ.073	Угроза несанкционированного доступа к активному и (или) пас-сивному виртуальному и (или) физическому сетевому оборудова-нию из физической и (или) виртуальной сети
29.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
30.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации

31.	УБИ.088	Угроза несанкционированного копирования защищаемой информации
32.	УБИ.089	Угроза несанкционированного редактирования реестра
33.	УБИ.090	Угроза несанкционированного создания учетной записи пользователя
34.	УБИ.091	Угроза несанкционированного удаления защищаемой информации
35.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
36.	УБИ.099	Угроза обнаружения хостов
37.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
38.	УБИ.103	Угроза определения типов объектов защиты
39.	УБИ.104	Угроза определения топологии вычислительной сети
40.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
41.	УБИ.121	Угроза повреждения системного реестра
42.	УБИ.122	Угроза повышения привилегий
43.	УБИ.124	Угроза подделки записей журнала регистрации событий
44.	УБИ.128	Угроза подмены доверенного пользователя
45.	УБИ.143	Угроза программного выведения из строя средств хранения, об-работки и (или) ввода/вывода/передачи информации
46.	УБИ.145	Угроза пропуска провёрки целостности программного обеспечения
47.	УБИ.152	Угроза удаления аутентификационной информации
48.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
49.	УБИ.155	Угроза утраты вычислительных ресурсов
50.	УБИ.156	Угроза утраты носителей информации
51.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
52.	УБИ.158	Угроза форматирования носителей информации
53.	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
54.	УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
55.	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
56.	УБИ.170	Угроза неправомерного шифрования информации
57.	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети

58.	УБИ.172	Угроза распространения «почтовых червей»
59.	УБИ.173	Угроза «спама» веб-сервера
60.	УБИ.174	Угроза «фарминга»
61.	УБИ.175	Угроза «фишинга»
62.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
63.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
64.	УБИ.179	Угроза несанкционированной модификации защищаемой информации
65.	УБИ.182	Угроза физического устаревания аппаратных компонентов
66.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
67.	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
68.	УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
69.	УБИ.188	Угроза подмены программного обеспечения
70.	УБИ.192	Угроза использования уязвимых версий программного обеспечения

Угрозами безопасности персональны́х данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых для осуществления деятельности министерства с учетом содержания персональных данных, характера и способов их обработки, в соответствии с документами ФСБ России являются:

1. Проведение атаки при нахождении в пределах контролируемой зоны;

2. Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.