МИНИСТЕРСТВО
строительства, архитектуры и территориального развития
Ростовской области

ПОСТАНОВЛЕНИЕ

«__» _____ 2017 г. № __ г. Ростов-на-Дону

Об утверждении угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных отдела исполнения бюджета и бухгалтерского учета, отдела правовой и кадровой работы, обеспечения доступным и комфортным жильем населения Ростовской области министерства строительства, архитектуры и территориального развития Ростовской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152 «О персональных данных» министерство строительства, архитектуры и территориального развития Ростовской области **п о с т а н о в л я е т:**

1. Утвердить угрозы безопасности персональных данных, актуальные при их обработке в информационных системах персональных данных отдела исполнения бюджета и бухгалтерского учета, отдела правовой и кадровой работы, обеспечения доступным и комфортным жильем населения Ростовской области министерства строительства, архитектуры и территориального развития Ростовской области согласно приложению № 1.
2. Постановление вступает в силу со дня его официального опубликования.
3. Контроль за выполнением настоящего постановления возложить на заместителя министра Дранникова А.В.

Министр Н.В. Безуглов

Приложение №1
к постановлению
министерства
строительства, архитектуры и
территориального развития
Ростовской области
от «___»_____2017 г. № ____

Угрозы безопасности персональных данных, актуальные при их обработке в информационных системах персональных данных отдела исполнения бюджета и бухгалтерского учета, отдела правовой и кадровой работы, обеспечения доступным и комфортным жильем населения Ростовской области министерства строительства, архитектуры и территориального развития Ростовской области.

Согласно Акту определения вероятных угроз безопасности персональных данных, при обработке персональных данных в информационных системах отдела исполнения бюджета и бухгалтерского учета, отдела правовой и кадровой работы, обеспечения доступным и комфортным жильем населения Ростовской области министерства строительства, архитектуры и территориального развития Ростовской области являются актуальными следующие угрозы:

№ п.п.	**Угрозы безопасности персональных данных**	**Актуальность угрозы**
1.	Кража ПЭВМ	актуальна
2.	Кража носителей информации	актуальна
3.	Кража ключей и атрибутов доступа	актуальна
4.	Кражи, модификации, уничтожения информации	актуальна
5.	Вывод из строя узлов ПЭВМ, каналов связи	актуальна
6.	Несанкционированное отключение средств защиты.	актуальна
7.	Действия вредоносных программ (вирусов)	актуальна
8.	Недекларированные возможности системного ПО и прикладного ПО	актуальна
9.	Установка ПО, не связанного с исполнением служебных обязанностей	актуальна
10.	Утрата ключей и атрибутов доступа	актуальна
11.	Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальна

12.	Непреднамеренное отключение средств защиты	актуальна
13.	Выход из строя аппаратно-программных средств	актуальна
14.	Сбой системы электроснабжения	актуальна
15.	Доступ к информации (модификация, уничтожение, копирование) лиц, не допущенных к ее обработке	актуальна
16.	Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.	актуальна
17.	Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации:	актуальна
17.1.	Перехват в пределах контролируемой зоны внешними нарушителями	актуальна
17.2.	Перехват в пределах контролируемой зоны внутренними нарушителями	актуальна
18.	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.	актуальна
19.	Угрозы выявления паролей по сети.	актуальна
20.	Угрозы навязывания ложного маршрута сети.	актуальна
21.	Угрозы подмены доверенного объекта в сети.	актуальна
22.	Угрозы внедрения ложного объекта, как в ИС, так и во внешних сетях.	актуальна
23.	Угрозы типа «Отказ в обслуживании».	актуальна
24.	Угрозы удаленного запуска приложений.	актуальна
25.	Угрозы внедрения по сети вредоносных программ.	актуальна

№ п.п	УБИ ФСТЭК России	Наименование угрозы	Актуальность угрозы
1.	3	Угроза анализа криптографических алгоритмов и их реализации	актуальна
2.	4	Угроза аппаратного сброса пароля BIOS	актуальна
3.	5	Угроза внедрения вредоносного кода в BIOS	актуальна
4.	6	Угроза внедрения кода или данных	актуальна
5.	8	Угроза восстановления аутентификационной информации	актуальна
6.	9	Угроза восстановления предыдущей уязвимой версии BIOS	актуальна
7.	12	Угроза деструктивного изменения конфигурации/среды окружения программ	актуальна
8.	13	Угроза деструктивного использования декларированного функционала BIOS	актуальна
9.	14	Угроза длительного удержания вычислительных ресурсов пользователями	актуальна
10.	15	Угроза доступа к защищаемым файлам с использованием обходного пути	актуальна
11.	16	Угроза доступа к локальным файлам сервера при помощи URL	актуальна
12.	17	Угроза доступа/перехвата/изменения HTTP cookies	актуальна
13.	18	Угроза загрузки нештатной операционной системы	актуальна
14.	19	Угроза заражения DNS-кеша	актуальна
15.	22	Угроза избыточного выделения оперативной памяти	актуальна
16.	23	Угроза изменения компонентов системы	актуальна
17.	24	Угроза изменения режимов работы аппаратных элементов компьютера	актуальна
18.	25	Угроза изменения системных и глобальных переменных	актуальна
19.	26	Угроза искажения XML-схемы	актуальна
20.	27	Угроза искажения вводимой и выводимой на периферийные устройства информации	актуальна
21.	28	Угроза использования альтернативных путей доступа к ресурсам	актуальна
22.	30	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	актуальна
23.	31	Угроза использования механизмов авторизации для повышения привилегий	актуальна
24.	32	Угроза использования поддельных цифровых подписей BIOS	актуальна
25.	33	Угроза использования слабостей кодирования входных данных	актуальна
26.	34	Угроза использования слабостей протоколов сетевого/локального обмена данными	актуальна

27.	36	Угроза исследования механизмов работы программы	актуальна
28.	37	Угроза исследования приложения через отчёты об ошибках	актуальна
29.	39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	актуальна
30.	41	Угроза межсайтового скриптинга	актуальна
31.	42	Угроза межсайтовой подделки запроса	актуальна
32.	45	Угроза нарушения изоляции среды исполнения BIOS	актуальна
33.	46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	актуальна
34.	49	Угроза нарушения целостности данных кеша	актуальна
35.	51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	актуальна
36.	53	Угроза невозможности управления правами пользователей BIOS	актуальна
37.	61	Угроза некорректного задания структуры данных транзакции	актуальна
38.	62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	актуальна
39.	67	Угроза неправомерного ознакомления с защищаемой информацией	актуальна
40.	69	Угроза неправомерных действий в каналах связи	актуальна
41.	71	Угроза несанкционированного восстановления удалённой защищаемой информации	актуальна
42.	72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	актуальна
43.	74	Угроза несанкционированного доступа к аутентификационной информации	актуальна
44.	83	Угроза несанкционированного доступа к системе по беспроводным каналам	актуальна
45.	86	Угроза несанкционированного изменения аутентификационной информации	актуальна
46.	87	Угроза несанкционированного использования привилегированных функций BIOS	актуальна
47.	88	Угроза несанкционированного копирования защищаемой информации	актуальна
48.	89	Угроза несанкционированного редактирования реестра	актуальна
49.	90	Угроза несанкционированного создания учётной записи пользователя	актуальна
50.	91	Угроза несанкционированного удаления защищаемой информации	актуальна
51.	92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	актуальна
52.	93	Угроза несанкционированного управления буфером	актуальна

53.	94	Угроза несанкционированного управления синхронизацией и состоянием	актуальна
54.	98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	актуальна
55.	99	Угроза обнаружения хостов	актуальна
56.	100	Угроза обхода некорректно настроенных механизмов аутентификации	актуальна
57.	102	Угроза опосредованного управления группой программ через совместно используемые данные	актуальна
58.	103	Угроза определения типов объектов защиты	актуальна
59.	104	Угроза определения топологии вычислительной сети	актуальна
60.	109	Угроза перебора всех настроек и параметров приложения	актуальна
61.	111	Угроза передачи данных по скрытым каналам	актуальна
62.	113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	актуальна
63.	115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	актуальна
64.	116	Угроза перехвата данных, передаваемых по вычислительной сети	актуальна
65.	117	Угроза перехвата привилегированного потока	актуальна
66.	118	Угроза перехвата привилегированного процесса	актуальна
67.	121	Угроза повреждения системного реестра	актуальна
68.	122	Угроза повышения привилегий	актуальна
69.	123	Угроза подбора пароля BIOS	актуальна
70.	127	Угроза подмены действия пользователя путём обмана	актуальна
71.	128	Угроза подмены доверенного пользователя	актуальна
72.	129	Угроза подмены резервной копии программного обеспечения BIOS	актуальна
73.	130	Угроза подмены содержимого сетевых ресурсов	актуальна
74.	131	Угроза подмены субъекта сетевого доступа	актуальна
75.	132	Угроза получения предварительной информации об объекте защиты	актуальна
76.	139	Угроза преодоления физической защиты	актуальна
77.	140	Угроза приведения системы в состояние «отказ в обслуживании»	актуальна
78.	143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	актуальна
79.	144	Угроза программного сброса пароля BIOS	актуальна
80.	145	Угроза пропуска проверки целостности программного обеспечения	актуальна
81.	149	Угроза, сбоя обработки специальным образом изменённых файлов	актуальна
82.	150	Угроза сбоя процесса обновления BIOS	актуальна

83.	151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	актуальна
84.	152	Угроза удаления аутентификационной информации	актуальна
85.	154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	актуальна
86.	155	Угроза утраты вычислительных ресурсов	актуальна
87.	156	Угроза утраты носителей информации	актуальна
88.	157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	актуальна
89.	158	Угроза форматирования носителей информации	актуальна
90.	159	Угроза «форсированного веб-браузинга»	актуальна
91.	160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	актуальна
92.	162	Угроза эксплуатации цифровой подписи программного кода	актуальна
93.	163	Угроза перехвата исключения/сигнала из привилегированного блока функций	актуальна
94.	167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	актуальна
95.	168	Угроза «кражи» учётной записи доступа к сетевым сервисам	актуальна
96.	169	Угроза наличия механизмов разработчика	актуальна
97.	170	Угроза неправомерного шифрования информации	актуальна
98.	171	Угроза скрытного включения вычислительного устройства в состав бот-сети	актуальна
99.	172	Угроза распространения «почтовых червей»	актуальна
100.	173	Угроза «спама» веб-сервера	актуальна
101.	174	Угроза «фарминга»	актуальна
102.	175	Угроза «фишинга»	актуальна
103.	176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	актуальна
104.	178	Угроза несанкционированного использования системных и сетевых утилит	актуальна
105.	179	Угроза несанкционированной модификации защищаемой информации	актуальна
106.	181	Угроза перехвата одноразовых паролей в режиме реального времени	актуальна
107.	182	Угроза физического устаревания аппаратных компонентов	актуальна
108.	185	Угроза несанкционированного изменения параметров настройки средств защиты информации	актуальна
109.	186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	актуальна

110.	187	Угроза несанкционированного воздействия на средство защиты информации	актуальна
111.	188	Угроза подмены программного обеспечения	актуальна
112.	189	Угроза маскирования действий вредоносного кода	актуальна
113.	190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	актуальна
114.	191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	актуальна
115.	192	Угроза использования уязвимых версий программного обеспечения	актуальна
116.	193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика	актуальна