**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ**

**ВОЛОВСКИЙ РАЙОН**

ПОСТАНОВЛЕНИЕ

от 25.02.2025 № 102

**Об определении угроз безопасности персональных данных,**

**актуальных при обработке персональных данных в муниципальной информационной системе администрации муниципального образования Воловский район**

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2011, N 31, ст. 4701), на основании статьи 35 Устава муниципального образования Воловский район администрация муниципального образования Воловский район ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в муниципальной информационной системе администрации муниципального образования Воловский район, согласно приложению.

2. Комитету по организационным вопросам разместить постановление на официальном сайте муниципального образования Воловский район в сети «Интернет» и обнародовать на информационных стендах.

3. Постановление вступает в силу со дня обнародования.

 **Глава администрации**

**муниципального образования**

 **Воловский район С.Ю. Пиший**

Приложение

к постановлению администрации

муниципального образования

Воловский район

от 25.02.2025 № 102

**Угрозы безопасности персональных данных, актуальных при обработке персональных данных в муниципальной информационной системе администрации муниципального образования Воловский район**

Угрозами безопасности персональных данных, актуальными при обработке персональных данных в муниципальной информационной системе администрации муниципального образования Воловский район, являются:

УБИ. 003. Угроза анализа криптографических алгоритмов и их реализации

УБИ. 004. Угроза аппаратного сброса пароля BIOS

УБИ. 005. Угроза внедрения вредоносного кода в BIOS

УБИ. 006. Угроза внедрения кода или данных

УБИ. 007. Угроза воздействия на программы с высокими привилегиями

УБИ. 008. Угроза восстановления аутентификационной информации

УБИ. 009. Угроза восстановления предыдущей уязвимой версии BIOS

УБИ. 012. Угроза деструктивного изменения конфигурации/среды окружения программ

УБИ. 013. Угроза деструктивного использования декларированного функционала BIOS

УБИ. 014. Угроза длительного удержания вычислительных ресурсов пользователями

УБИ. 015. Угроза доступа к защищаемым файлам с использованием обходного пути

УБИ. 016. Угроза доступа к локальным файлам сервера при помощи URL

УБИ. 017. Угроза доступа/перехвата/изменения HTTP cookies

УБИ. 018. Угроза загрузки нештатной операционной системы

УБИ. 019. Угроза заражения DNS-кеша

УБИ. 022. Угроза избыточного выделения оперативной памяти

УБИ. 023. Угроза изменения компонентов системы

УБИ. 024. Угроза изменения режимов работы аппаратных элементов компьютера

УБИ. 025. Угроза изменения системных и глобальных переменных

УБИ. 026. Угроза искажения XML-схемы

УБИ. 027. Угроза искажения вводимой и выводимой на периферийные устройства информации

УБИ. 028. Угроза использования альтернативных путей доступа к ресурсам

УБИ. 030. Угроза использования информации идентификации/аутентификации, заданной по умолчанию

УБИ. 031. Угроза использования механизмов авторизации для повышения привилегий

УБИ. 032. Угроза использования поддельных цифровых подписей BIOS

УБИ. 033. Угроза использования слабостей кодирования входных данных

УБИ. 034. Угроза использования слабостей протоколов сетевого/локального обмена данными

УБИ. 035. Угроза использования слабых криптографических алгоритмов BIOS

УБИ. 036. Угроза исследования механизмов работы программы

УБИ. 037. Угроза исследования приложения через отчёты об ошибках

УБИ. 039. Угроза исчерпания запаса ключей, необходимых для обновления BIOS

УБИ. 041. Угроза межсайтового скриптинга

УБИ. 042. Угроза межсайтовой подделки запроса

УБИ. 045. Угроза нарушения изоляции среды исполнения BIOS

УБИ. 049. Угроза нарушения целостности данных кеша

УБИ. 051. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания

УБИ. 053. Угроза невозможности управления правами пользователей BIOS

УБИ. 059. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов

УБИ. 061. Угроза некорректного задания структуры данных транзакции

УБИ. 062. Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера

УБИ. 063. Угроза некорректного использования функционала программного обеспечения

УБИ. 067. Угроза неправомерного ознакомления с защищаемой информацией

УБИ. 068. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением

УБИ. 069. Угроза неправомерных действий в каналах связи

УБИ. 071. Угроза несанкционированного восстановления удалённой защищаемой информации

УБИ. 072. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS

УБИ. 074. Угроза несанкционированного доступа к аутентификационной информации

УБИ. 086. Угроза несанкционированного изменения аутентификационной информации

УБИ. 087. Угроза несанкционированного использования привилегированных функций BIOS

УБИ. 088. Угроза несанкционированного копирования защищаемой информации

УБИ. 089. Угроза несанкционированного редактирования реестра

УБИ. 090. Угроза несанкционированного создания учётной записи пользователя

УБИ. 091. Угроза несанкционированного удаления защищаемой информации

УБИ. 092. Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам

УБИ. 093. Угроза несанкционированного управления буфером

УБИ. 094. Угроза несанкционированного управления синхронизацией и состоянием

УБИ. 095. Угроза несанкционированного управления указателями

УБИ. 098. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб

УБИ. 099. Угроза обнаружения хостов

УБИ. 100. Угроза обхода некорректно настроенных механизмов аутентификации

УБИ. 102. Угроза опосредованного управления группой программ через совместно используемые данные

УБИ. 103. Угроза определения типов объектов защиты

УБИ. 104. Угроза определения топологии вычислительной сети

УБИ. 109. Угроза перебора всех настроек и параметров приложения

УБИ. 111. Угроза передачи данных по скрытым каналам

УБИ. 113. Угроза перезагрузки аппаратных и программно-аппаратных СВТ

УБИ. 114. Угроза переполнения целочисленных переменных

УБИ. 115. Угроза перехвата вводимой и выводимой на периферийные устройства информации

УБИ. 116. Угроза перехвата данных, передаваемых по вычислительной сети

УБИ. 117. Угроза перехвата привилегированного потока

УБИ. 118. Угроза перехвата привилегированного процесса

УБИ. 121. Угроза повреждения системного реестра

УБИ. 122. Угроза повышения привилегий

УБИ. 123. Угроза подбора пароля BIOS

УБИ. 124. Угроза подделки записей журнала регистрации событий

УБИ. 127. Угроза подмены действия пользователя путём обмана

УБИ. 128. Угроза подмены доверенного пользователя

УБИ. 129. Угроза подмены резервной копии программного обеспечения BIOS

УБИ. 130. Угроза подмены содержимого сетевых ресурсов

УБИ. 131. Угроза подмены субъекта сетевого доступа

УБИ. 132. Угроза получения предварительной информации об объекте защиты

УБИ. 139. Угроза преодоления физической защиты

УБИ. 140. Угроза приведения системы в состояние «отказ в обслуживании»

УБИ. 143. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

УБИ. 144. Угроза программного сброса пароля BIOS

УБИ. 145. Угроза пропуска проверки целостности программного обеспечения

УБИ. 149. Угроза сбоя обработки специальным образом изменённых файлов

УБИ. 150. Угроза сбоя процесса обновления BIOS

УБИ. 152. Угроза удаления аутентификационной информации

УБИ. 153. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов

УБИ. 154. Угроза установки уязвимых версий обновления программного обеспечения BIOS

УБИ. 155. Угроза утраты вычислительных ресурсов

УБИ. 156. Угроза утраты носителей информации

УБИ. 157. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

УБИ. 158. Угроза форматирования носителей информации

УБИ. 160. Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации

УБИ. 162. Угроза эксплуатации цифровой подписи программного кода

УБИ. 163. Угроза перехвата исключения/сигнала из привилегированного блока функций

УБИ. 165. Угроза включения в проект не достоверно испытанных компонентов

УБИ. 166. Угроза внедрения системной избыточности

УБИ. 167. Угроза заражения компьютера при посещении неблагонадёжных сайтов

УБИ. 168. Угроза «кражи» учётной записи доступа к сетевым сервисам

УБИ. 169. Угроза наличия механизмов разработчика

УБИ. 170. Угроза неправомерного шифрования информации

УБИ. 171. Угроза скрытного включения вычислительного устройства в состав бот-сети

УБИ. 172. Угроза распространения «почтовых червей»

УБИ. 174. Угроза «фарминга»

УБИ. 175. Угроза «фишинга»

УБИ. 176. Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты

УБИ. 177. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью

УБИ. 178. Угроза несанкционированного использования системных и сетевых утилит

УБИ. 179. Угроза несанкционированной модификации защищаемой информации

УБИ. 180. Угроза отказа подсистемы обеспечения температурного режима

УБИ. 181. Угроза перехвата одноразовых паролей в режиме реального времени

УБИ. 182. Угроза физического устаревания аппаратных компонентов

УБИ. 185. Угроза несанкционированного изменения параметров настройки средств защиты информации

УБИ. 186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент

УБИ. 187. Угроза несанкционированного воздействия на средство защиты информации

УБИ. 188. Угроза подмены программного обеспечения

УБИ. 189. Угроза маскирования действий вредоносного кода

УБИ. 190. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет

УБИ. 191. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

УБИ. 192. Угроза использования уязвимых версий программного обеспечения

УБИ. 193. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика

УБИ. 195. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы

УБИ. 197. Угроза хищения аутентификационной информации из временных файлов cookie

УБИ. 198. Угроза скрытной регистрации вредоносной программой учетных записей администраторов

УБИ. 201. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере

УБИ. 203. Угроза утечки информации с неподключенных к сети Интернет компьютеров

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

УБИ. 208. Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники

УБИ. 209. Угроза несанкционированного доступа к защищаемой памяти ядра процессора

УБИ. 210. Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения

УБИ. 211. Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования ИС

УБИ. 212. Угроза перехвата управления ИС

УБИ. 213: Угроза обхода многофакторной аутентификации

УБИ. 214. Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации

УБИ. 215. Угроза несанкционированного доступа к системе при помощи сторонних сервисов

УБИ. 217. Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.