КЕМЕРОВСКАЯ ОБЛАСТЬ-КУЗБАСС

**Администрация Беловского городского округа**

# ПОСТАНОВЛЕНИЕ

20.05.2024 № 2058-п

Об определении типов угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Администрации Беловского городского округа и в подведомственных организациях

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Администрация Беловского городского округа

ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Администрации Беловского городского округа и в подведомственных организациях, согласно приложению к настоящему постановлению.

2. Управлению по работе со средствами массовой информации (Косвинцева Е.В.), отделу информационных технологий (Александрова С.А.) обеспечить размещение настоящего постановления в средствах массовой информации и на официальном сайте Администрации Беловского городского округа в информационно-телекоммуникационной сети «Интернет».

3. Данное постановление вступает в законную силу после его опубликования.

4. Контроль за исполнением настоящего постановления возложить на заместителя Главы беловского городского округа по экономике, финансам, налогам и собственности Е.Т.Муратова.

Глава Беловского
городского округа А.В. Курносов

Администрация Беловского городского округа Кемеровская область - Кузбасс
Управление делами
*2*

Приложение
к постановлению Администрации
Беловского городского округа
от 20.05.2024 № 2058-п

# Типы угроз безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Администрации Беловского городского округа и в подведомственных организациях

## Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Администрации Беловского городского округа и в подведомственных организациях (далее - актуальные угрозы безопасности персональных данных в ИСПДн), разработаны в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008, Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждёнными 3 руководством 8-го Центра ФСБ России от 31.03.2011 149/7/2/6-432, Базовой моделью угроз безопасности персональных данных

при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

2.Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) в Администрации Беловского городского округа и в подведомственных организациях.

3.Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в актуальных угрозах безопасности ИСПДн, подлежат адаптации в ходе разработки органами власти частных моделей угроз безопасности персональных данных для каждой информационной системы.

4. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик информационной системы, эксплуатируемой при осуществлении органом власти функций и полномочий, а также применяемых в ней информационных технологий и особенностей ее функционирования. В частной модели угроз безопасности персональных данных указываются:

4.1. Описание ИСПДн и ее структурно-функциональных характеристик;

4.2. Описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

4.3. Описание возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Частная модель угроз безопасности персональных данных для государственных органов разрабатывается с учетом требований приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в актуальных угрозах безопасности ИСПДн, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. В Администрации Беловского городского округа и подведомственных учреждениях функционируют информационные системы, обрабатывающие специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора, общедоступные персональные данные менее чем 100000

субъектов персональных данных, не являющихся сотрудниками оператора, и персональные данные менее чем 10000 субъектов персональных данных, являющихся сотрудниками оператора. Информационные системы персональных данных Администрации Беловского городского округа и подведомственных учреждениях характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы, имеющие подключение к единому центру обработки данных. Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются съемные носители.

Персональные данные субъектов персональных данных обрабатываются с целью получения государственных услуг, а также в целях:

1.Ведения финансово-экономической деятельности в соответствии с требованиями законодательства Российской Федерации;

2. Проведения конкурсного отбора на государственную гражданскую службу в Администрацию Беловского городского округа;

3. Ведения кадрового резерва Администрации Беловского городского округа;

4. Награждения наградами Администрации Беловского городского округа;

5. Выплат социального характера в натуральной и денежной форме;

6. Рассмотрения запросов, обращений граждан

Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее - СКЗИ).

Контролируемой зоной ИСПДн является административное здание и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования. В административном здании осуществляется пропускной режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники запрещено. Помещения оборудованы запирающимися дверями. В коридорах, вестибюлях и холлах ведется видеонаблюдение.

## Актуальные угрозы безопасности персональных данных в информационных системах персональных данных.

Учитывая особенности обработки персональных данных в Администрации Беловского городского округа и подведомственных учреждениях, а также категорию и объем обрабатываемых в ИСПДн

персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Целостность-состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Основной целью применения в ИСПДн Администрации Беловского городского округа и подведомственных учреждениях СКЗИ является защита персональных данных, в том числе при информационном обмене по сетям связи общего пользования.

Объектами защиты являются:

1.Персональные данные;

2. СКЗИ;

3. Среда функционирования СКЗИ (далее-СФ СКЗИ);

4. Информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

5. Носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

6. Используемые информационной системой каналы (линии) связи, включая кабельные системы; помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

Основными актуальными угрозами безопасности персональных данных в ИСПДн согласно требованиям ФСТЭК России являются:

1.Угрозы несанкционированного доступа (далее-НСД) на рабочих местах, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн;

2. Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

3. Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение НСД с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных) с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

4. Угрозы локального внедрения вредоносных программ;

5. Угрозы выявления паролей;

6. Угрозы удаленного запуска приложений;

7. Угрозы внедрения по сети вредоносных программ;

8. Угрозы «Анализ сетевого трафика» с перехватом, передаваемой из ИСПДн и принимаемой в ИСПДн информации из внешних сетей информации;

9. Угрозы сканирования сети, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и другое;

10. Угрозы внедрения ложного объекта сети как в ИСПДн, так и во внешних сетях;

11. Угрозы подмены доверенного объекта сети;

12. Угрозы навязывания ложного маршрута сети путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;

13. Угрозы непреднамеренного или преднамеренного вывода из строя технических средств и средств защиты информации;

14. Угрозы несанкционированного отключения средств защиты информации;

15. Угрозы непреднамеренной модификации (уничтожения) информации пользователями;

16.Угрозы недостаточности надежности технических средств и коммуникационного оборудования;

17.Угрозы снижения достаточности и качества применяемых средств защиты информации;

18.Подготовки и проведения атак за пределами контролируемой зоны;

19.Угрозы проведения атак при нахождении в пределах контролируемой зоны;

20.Угрозы утечки видовой информации;

21.Угрозы нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;

22. Угрозы несанкционированного доступа к виртуальным каналам передачи;

Основными актуальными угрозами безопасности персональных данных в ИСПДн согласно требованиям ФСБ России, являются:

1.Угрозы непредумышленного искажения или удаления программных компонентов ИСПДн;

2.Угрозы внедрения и использования неучтенных программ;

3.Угрозы игнорирования организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации;

4.Угрозы нарушения правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности: ключевой, парольной и аутентифицирующей информации);

5.Угрозы предоставления посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требованиям;

6.Угрозы несообщения о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа;

7.Угрозы внесения негативных функциональных возможностей в технические и программные компоненты СКЗИ и СФ СКЗИ, в том числе с использованием вредоносных программ (компьютерные вирусы и т.д.);

8.Угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения (безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее - атака) при нахождении в пределах контролируемой зоны;

9.Угрозы проведения атак на этапе эксплуатации СКЗИ на следующие объекты:

9.1. Документацию на СКЗИ и компоненты СФ СКЗИ;

9.2. Помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее СВТ), на которых реализованы СКЗИ и СФ СКЗИ;

9.3. Угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

9.3.1. Сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

9.3.2. Сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

9.3.3. Сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ СКЗИ;

9.3.4. Угрозы использования штатных средств ИСПДн, не ограниченного мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

9.3.5. Угрозы физического доступа к СВТ, на которых реализованы СКЗИ и СФ СКЗИ;

9.3.6. Угрозы возможностей воздействия на аппаратные компоненты СКЗИ и СФ СКЗИ, не ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

9.3.7. Угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ СКЗИ, и в области использования для реализации атак недокументированных (не декларированных) возможностей прикладного программного обеспечения;

9.3.8. Угрозы проведения лабораторных исследований СКЗИ, используемых вне контролируемой зоны, не ограниченного мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

9.3.9. Угрозы проведения работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ СКЗИ, в том числе с использованием исходных текстов входящего в СФ СКЗИ прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ;

9.3.10. Угрозы создания способов, подготовки и проведения атак с привлечением специалистов в области использования для реализации атак недокументированных (не декларированных) возможностей системного программного обеспечения;

9.3.11. Угрозы возможностей располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ СКЗИ;

9.3.12. Угрозы возможностей воздействовать на любые компоненты СКЗИ и СФ СКЗИ.