



АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА СТУПИНО

МОСКОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

26.11.2024 № 430-р

г. Ступино

Об утверждении требований к защите информации при информационном взаимодействии защищаемых объектов информатизации администрации городского округа Ступино Московской области

В целях исполнения федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 26.07.2014 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», нормативных правовых актов и методических документов Российской Федерации в сфере защиты информации:

1. Утвердить Требования к защите информации при информационном взаимодействии защищаемых объектов информатизации администрации городского округа Ступино Московской области (далее - Требования) (Приложение).

2. Ответственным за эксплуатацию защищаемых объектов информатизации руководствоваться Требованиями при взаимодействии с иными объектами информатизации.

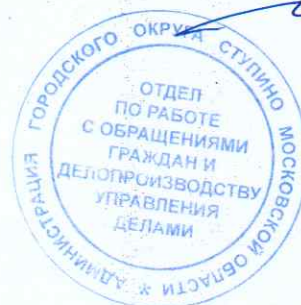
3. Опубликовать (разместить) настоящее распоряжение на официальном сайте администрации, Совета депутатов и контрольно-счётной палаты городского округа Ступино Московской области.

4. Контроль за исполнением настоящего распоряжения возложить на

заместителя главы городского округа Ступино Московской области по режиму
(безопасности) Севрюгина А.В.

Глава городского округа Ступино
Московской области

С.Г. Мужальских



Приложение
Утверждено
распоряжением администрации
городского округа Ступино
Московской области
от « 26 » 11.2014 № 430-р

**Требования
к защите информации при информационном взаимодействии защищаемых
объектов информатизации администрации городского округа Ступино
Московской области, а также их компонентов**

1. Общие положения

1.1. Настоящие Требования разработаны в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 26.07.2014 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», нормативными правовыми актами и методическими документами Российской Федерации и Московской области в области защиты информации.

1.2. В документе устанавливаются требования к защите информации при информационном взаимодействии защищаемых объектов информатизации администрации городского округа Ступино Московской области (далее - Администрация) с другими информационными системами и автоматизированными рабочими местами, а также требования к защите информации при информационном взаимодействии сегментов и компонентов таких объектов между собой.

1.3. Перечень защищаемых объектов информатизации Администрации с указанием их типов, классов защищенности, возможности обработки в них персональных данных, уровней защищенности обрабатываемых в них персональных данных (при наличии), а также принадлежности к объектам критической информационной инфраструктуры Российской Федерации, утверждается правовым актом Администрации.

1.4. Обработка информации, доступ к которой ограничен законодательством Российской Федерации (в том числе персональных данных), с использованием технических средств, не входящих в состав защищаемых объектов информатизации, не допускается за исключением случая, когда на такие технические средства распространяется действие аттестатов соответствия требованиям к защите информации (протоколов проведения оценки эффективности) других объектов

информатизации.

1.5. Требования настоящего документа не распространяются на тестовые ресурсы объектов информатизации при условии отсутствия их взаимодействия с компонентами, находящимися в эксплуатации, а также на объекты информатизации, не введенные в эксплуатацию в порядке, предусмотренном законодательством Российской Федерации.

1.6. Требования настоящего документа не распространяются на объекты информатизации, предназначенные для обработки информации, содержащей сведения, составляющие государственную тайну.

2. Перечень определений и сокращений

2.1. В настоящих Требованиях используются следующие сокращения:

- АРМ - автоматизированное стационарное или мобильное рабочее место пользователя или потребителя ЗОИ;
- ГИС - государственная информационная система;
- ЗОИ - защищаемый объект информатизации Администрации;
- ЗОКИИ - защищаемый объект критической информационной инфраструктуры Российской Федерации;
- ИОД - информация, доступ к которой ограничен законодательством Российской Федерации;
- ИС - информационная система;
- ОИ - объект информатизации;
- КЗ - контролируемая зона;
- ПДн - персональные данные;
- СКЗИ - средство криптографической защиты информации.

2.2. В настоящих Требованиях используются следующие основные определения:

- автоматизированное рабочее место, оператором которых является Администрация и к которой предъявляются требования защиты обрабатываемой в ней информации (далее - автоматизированное рабочее место);
- администратор - пользователь ЗОИ, уполномоченный выполнять действия по администрированию этого ЗОИ и (или) администрированию системы защиты информации этого ЗОИ в соответствии с установленной ролью;
- аттестат соответствия требованиям по защите информации (далее - аттестат соответствия), протокол проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных в информационной системе

персональных данных (далее – протокол проведения оценки эффективности) - документ, выдаваемый по результатам проведения комплекса организационно-технических мероприятий по защите информации на ОИ и подтверждающий, что объект соответствует требованиям нормативных правовых актов и методических документов в области защиты информации;

- внешний ОИ - ОИ, взаимодействующий с ЗОИ и не входящий в состав этого ЗОИ;

- закрытый контур ОИ - часть ОИ, предназначенная для обработки информации, доступ к которой ограничен законодательством Российской Федерации;

- общедоступный ОИ - ОИ, предназначенный исключительно для обработки информации, доступ к которой не ограничен законодательством Российской Федерации;

- общедоступный (публичный) контур ОИ - часть ОИ, предназначенная исключительно для обработки информации, доступ к которой не ограничен законодательством Российской Федерации;

- категория персональных данных - в рамках настоящего документа рассматривается как принадлежность персональных данных к одному из следующих типов: «специальные»; «биометрические»; «общедоступные»; «иные», устанавливаемых в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- компонент ОИ - часть ОИ, включающая совокупность информации и обеспечивающих ее обработку информационных технологий и технических средств;

- контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств;

- конфиденциальность информации - свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право;

- личный кабинет - это часть ЗОИ, доступная пользователю после его авторизации и предназначенная для внесения пользовательских данных и работы с ними;

- потребитель информации ЗОИ - лицо, получающее доступ к ограниченному набору информации, результатам функционирования ЗОИ и не имеющее обязанностей выполнять действия (операции) по обработке информации в ЗОИ;

- пользователь ЗОИ - лицо, наделенное правами и функциональными обязанностями выполнять действия (операции) по обработке информации в ЗОИ;

- сегмент ЗОИ - совокупность нескольких компонентов ЗОИ, на которые в установленном порядке распространено действие аттестата соответствия (протокола проведения оценки эффективности);

- уровень конфиденциальности информации - в рамках настоящего документа рассматривается как принадлежность информации к одному из следующих типов: «общедоступная информация»; «информация, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации», устанавливаемых в соответствии с положениями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2.3 Понятия, значение которых определено в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральном законе от 26.07.2014 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», применяются в значениях, указанных в соответствующих федеральных законах.

3. Общие требования к организации взаимодействия ЗОИ

3.1. Взаимодействие компонентов ЗОИ между собой не должно нарушать требования аттестационной, эксплуатационной, организационно-распорядительной документации ЗОИ и требования эксплуатационной документации средств защиты информации.

3.2. Взаимодействие ЗОИ с внешними ОИ не должно нарушать требования аттестационной, эксплуатационной, организационно-распорядительной документации ЗОИ и требования эксплуатационной документации средств защиты информации.

3.3. При взаимодействии ЗОИ с внешними ОИ должны применяться сертифицированные по требованиям безопасности информации средства межсетевого экранирования, если иное не предусмотрено аттестационной документацией ЗОИ.

3.4. При необходимости передачи ИОД по каналам связи, выходящим за пределы КЗ ЗОИ, за исключением информационного взаимодействия, описанного в п.5.6. настоящих Требований, дополнительно предъявляются требования защиты передаваемой информации, указанные в разделе 4 настоящих Требований.

4. Требования к информационному взаимодействию уровня «сервер - сервер»

4.1. Взаимодействие уровня «сервер - сервер» компонентов одного ЗОИ между собой в случае, если эти компоненты предназначены для обработки информации одинакового уровня конфиденциальности и обработки ПДн одинаковой категории (при наличии) допускается без предъявления дополнительных требований к защите информации при условии соблюдения требований раздела 3 настоящих Требований.

4.2. Взаимодействие уровня «сервер - сервер» компонентов одного ЗОИ между собой в случае, если эти компоненты предназначены для обработки информации различного уровня конфиденциальности, допускается при условии обеспечения невозможности передачи информации в результате такого взаимодействия в компоненты ЗОИ, не предназначенные для обработки информации соответствующего уровня конфиденциальности.

4.3. Взаимодействие уровня «сервер - сервер» компонентов одного ЗОИ между собой в случае, если эти компоненты предназначены для обработки ПДн различной категории, допускается при условии обеспечения невозможности передачи ПДн в результате такого взаимодействия в компоненты ЗОИ, не предназначенные для обработки ПДн соответствующей категории.

4.4. Взаимодействие уровня «сервер - сервер» общедоступного ЗОИ с общедоступным внешним ОИ, допускается без предъявления дополнительных требований к защите информации при условии соблюдения требований раздела 3 настоящих Требований.

4.5. Взаимодействие уровня «сервер - сервер» общедоступного контура ЗОИ с общедоступным контуром внешнего ОИ, допускается без предъявления

дополнительных требований к защите информации при условии соблюдения требований раздела 3 настоящих Требований.

4.6. Взаимодействие уровня «сервер - сервер» ЗОИ, предназначенного для обработки ИОД, с внешними ОИ, за исключением случаев, указанных в пунктах 4.4 и 4.5 настоящих Требований, допускается при условии наличия у внешнего ОИ действующего аттестата соответствия (протокола проведения оценки эффективности), подтверждающего возможность обработки информации уровня конфиденциальности не ниже передаваемой из ЗОИ. Передача ПДн из ЗОИ во внешний ОИ допускается при наличии отметки о возможности обработки ПДн соответствующей категории в аттестате соответствия (протоколе проведения оценки эффективности) внешнего ОИ.

4.7. В случае если внешний ОИ не относится к ГИС, требования, указанные в пункте 4.6. настоящих Требований, вместо аттестата соответствия могут быть подтверждены иным документом по решению оператора внешнего ОИ.

4.8. При необходимости передачи ИОД по каналам связи, находящимся за пределами КЗ ЗОИ, при информационном взаимодействии, описанном в пунктах 4.1., 4.2., 4.3. и 4.6. настоящих Требований, дополнительно предъявляются требования защиты передаваемой информации, указанные в разделе 6.

4.9. Передача ИОД, в том числе ПДн, из ЗОИ на ресурсы, не входящие в состав какого-либо ОИ, или входящие в состав не введенных в эксплуатацию ОИ, не допускается.

5. Требования к информационному взаимодействию уровня «автоматизированное рабочее место - сервер»

5.1. Взаимодействие уровня «АРМ - сервер» АРМ, за исключением АРМ администраторов, с общедоступным ЗОИ или общедоступным контуром ЗОИ допускается без предъявления дополнительных требований к защите информации при условии соблюдения требований раздела 3 настоящих Требований.

5.2. Взаимодействие уровня «АРМ - сервер» АРМ администраторов с общедоступным ЗОИ или общедоступным контуром ЗОИ допускается при условии соблюдения требований раздела 3 настоящих Требований, при этом сведения о таких АРМ должны быть внесены в организационно-распорядительную документацию ЗОИ в установленном порядке

5.3. Взаимодействие уровня «АРМ - сервер» АРМ пользователей и администраторов с ЗОИ, не являющимся ЗОКИИ и предназначенным для обработки

ИОД, за исключением взаимодействия с общедоступными контурами такого ЗОИ, допускается при условии соблюдения требований раздела 3 настоящих Требований и только в любом из случаев:

- взаимодействующий с ЗОИ АРМ входит в состав соответствующего ЗОИ, сведения об этом внесены в организационно-распорядительную документацию ЗОИ в установленном порядке;

- взаимодействующий с ЗОИ АРМ входит в состав сегмента соответствующего ЗОИ, сведения об этом внесены в организационно-распорядительную документацию сегмента ЗОИ в установленном порядке;

- взаимодействующий с ЗОИ АРМ входит в состав внешнего ОИ, предназначенной для обработки ИОД и ПДн соответствующей категории (при наличии), сведения об этом внесены в организационно-распорядительную документацию внешнего ОИ или сегмента внешнего ОИ в установленном порядке. При этом возможность обработки ИОД и ПДн соответствующей категории (при наличии) в таком внешнем ОИ должна быть подтверждена наличием действующего аттестата соответствия (протокола проведения оценки эффективности).

В случае если внешний ОИ или сегмент ОИ, в состав которого входит АРМ, не относится к ГИС, возможность обработки ИОД и ПДн соответствующей категории (при наличии) вместо аттестата соответствия может быть подтверждена иным документом по решению оператора внешнего ОИ.

5.4. Взаимодействие уровня «АРМ - сервер» АРМ пользователей и администраторов с ЗОИ, являющимся ЗОКИИ, за исключением общедоступных контуров такого ЗОИ, допускается при условии соблюдения требований раздела 3 настоящих Требований и только в любом из случаев:

- взаимодействующий с ЗОИ АРМ входит в состав соответствующего ЗОИ, сведения об этом внесены в организационно-распорядительную документацию ЗОИ в установленном порядке;

- взаимодействующий с ЗОИ АРМ входит в состав сегмента соответствующего ЗОИ, сведения об этом внесены в организационно-распорядительную документацию сегмента ЗОИ в установленном порядке.

5.5. Взаимодействие уровня «АРМ - сервер» АРМ пользователей и администраторов с ЗОИ, являющимся ЗОКИИ, за исключением общедоступных контуров таких ЗОИ, не допускается, если на взаимодействующий с таким ЗОИ АРМ не распространяется действие аттестата соответствия (протокола проведения оценки эффективности) такого ЗОИ, независимо от действия на АРМ иных

аттестатов и прочих документов, подтверждающих соответствие требованиям о защите информации других ОИ.

5.6. Взаимодействие уровня «АРМ - сервер» АРМ потребителей информации ЗОИ с этим ЗОИ, в рамках которого потребитель информации такого ЗОИ получает доступ к собственным ПДн в личном кабинете или общедоступной информации, допускается без предъявления дополнительных требований к защите информации при условии соблюдения требований раздела 3 настоящих Требований.

6. Требования к передаче информации, обрабатываемой защищаемыми объектами информатизации, по каналам связи

6.1. Взаимодействие с ЗОИ, при котором осуществляется передача ИОД по каналам связи, выходящим за пределы КЗ такого ЗОИ, допускается только с применением сертифицированных ФСБ России СКЗИ, за исключением случая, указанного в пункте 5.6. настоящих Требований.

6.2. Применение средств (в том числе VPN-сервисов), не сертифицированных ФСБ России, в качестве альтернативы средствам, указанным в пункте 6.1. настоящих Требований, не допускается. При этом применение таких средств может допускается в качестве дополнительных мер для обеспечения технической возможности взаимодействия с ЗОИ.

6.3. Тип применяемых СКЗИ при взаимодействии компонентов ЗОИ между собой определяется требованиями аттестационной документации ЗОИ.

6.4. Тип применяемых СКЗИ при взаимодействии ЗОИ с другими ОИ определяется требованиями аттестационной документации ЗОИ, и при необходимости дополняется соглашением взаимодействующих сторон в установленном порядке.

6.5. Применение СКЗИ не требуется при взаимодействии компонентов ЗОИ между собой или с внешними ОИ в пределах КЗ такого ЗОИ.

6.6. Применение СКЗИ не требуется при взаимодействии АРМ или внешних ОИ с общедоступным ЗОИ или общедоступными контурами ЗОИ.

6.7. Применение СКЗИ не требуется при взаимодействии АРМ потребителей информации ЗОИ с этим ЗОИ, в рамках которого потребитель информации такого ЗОИ получает доступ к собственным ПДн в личном кабинете или общедоступной информации, при условии соблюдения требований раздела 3 настоящих Требований.

7. Заключительные положения

7.1. Законодательством Российской Федерации, Московской области, нормативными правовыми актами и методическими документами в области защиты информации, аттестационной и эксплуатационной документацией взаимодействующих объектов информатизации, иными документами могут предъявляться дополнительные требования к обеспечению защиты информации при взаимодействии ЗОИ и их компонентов.

7.2. Нарушение требований к защите информации при информационном взаимодействии ЗОИ влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.