Приложение № 18 к приказу №\_\_\_\_

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

УТВЕРЖДАЮ

Исполняющий

обязанности директора

\_\_\_\_\_\_\_\_\_\_\_\_ В.П. Воинов

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

 М.П.

**Технические условия**

по подключению к Государственной информационной системе обеспечения

градостроительной деятельности Тверской области

(ГИСОГД ТО)

г. Тверь

2023 г.

**Список используемых сокращений**

|  |  |  |
| --- | --- | --- |
| АРМ | – | Автоматизированное рабочее место |
| ГИСОГД ТО | – | Государственная информационная система Государственная информационная система |
| ЛВС | – | Локальная вычислительная сеть |
| НСД | – | Несанкционированный доступ |
| Оператор | – | Министерство цифрового развития и информационных технологий Тверской области |
| ОМСУ | – | Органы местного самоуправления муниципальных образований Тверской области |
| ОИВ | – | Исполнительные органы государственной власти Тверской области |
| ПДн | – | Персональные данные |
| СЗИ | – | Средство защиты информации |
| СКЗИ | – | Средство криптографической защиты информации |
| ТУ | – | Технические условия |
| ФСБ России | – | ФСБ России |
| ФСТЭК России | – | ФСТЭК России |
| ЭД | – | Эксплуатационная документация |

1. **Правовые основания**

Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами Российской Федерации (далее – НПА):

* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Приказ 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»;
* Приказ 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»;
* Приказ ФСБ России от 24.10.2022 г. № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».
1. **Общие сведения**

Настоящие Технические условия (далее – ТУ) устанавливают состав и содержание работ по организации защищенного взаимодействия автоматизированных рабочих мест (далее – АРМ) ОИВ и ОМСУ, включая Главное управление архитектуры и градостроительной деятельности Тверской области, а также прочих организаций, подключаемых по согласованию с оператором ГИСОГД ТО (далее - организации) к Государственной информационной системе обеспечения градостроительной деятельности Тверской области (ГИСОГД ТО) и

Архитектура ГИСОГД ТО включает служебный контур, в котором осуществляется обработка информации ограниченного доступа и открытый контур (публичный сегмент), в котором осуществляется обработка свободно распространяемой информации.

Внутренними пользователями ГИСОГД ТО, осуществляющими доступ к служебному контуру являются администраторы ГИСОГД ТО (администратор информационной безопасности и системные администраторы).

Внешними пользователями ГИСОГД ТО, осуществляющими доступ к служебному контуру являются сотрудники Главного управления архитектуры и градостроительной деятельности Тверской области, ОИВ и ОМСУ, разработчики программного обеспечения, имеющие действующие договоры, контракты на сопровождение (модернизацию) ГИСОГД ТО, а также сотрудники прочих организаций, подключаемые по согласованию с оператором ГИСОГД ТО.

Внешними пользователями ГИСОГД ТО, осуществляющими доступ к открытой части ГИСОГД ТО, являются граждане в сети Интернет.

Настоящие ТУ устанавливают состав и содержание работ по организации защищенного взаимодействия АРМ пользователей, осуществляющих доступ с служебному контору ГИСОГД ТО.

Требования к обеспечению информационной безопасности АРМ пользователей ГИСОГД ТО, осуществляющих доступ к открытому контуру ГИСОГД ТО, не предъявляются.

1. **Требования по обеспечению информационной безопасности при подключении АРМ пользователей к защищенной сети ГИСОГД ТО**

Для организации защищенного взаимодействия АРМ пользователей с ГИСОГД ТО, должны быть выполнены организационные и технические мероприятия, подтверждающие соответствие системы обеспечения безопасности информации АРМ пользователя требованиям безопасности информации.

Для обеспечения защиты информации на АРМ пользователя, должны применяться средства защиты информации, прошедшие процедуру оценки соответствия в форме сертификации на соответствие требованиям по безопасности информации.

Информационное взаимодействие АРМ пользователей с защищенной сетью ГИСОГД ТО должно осуществляться по защищенному каналу связи.

Подключение к защищенной сети ГИСОГД ТО производится с использованием средств криптографической защиты (далее – СКЗИ), обеспечивающих безопасное информационное взаимодействие с защищенной сетью ГИСОГД ТО.

В соответствии с руководящими документами ФСТЭК России на АРМ пользователей необходимо применение средств защиты информации 5 класса не ниже 5 уровня доверия, а также средства вычислительной техники не ниже 5 класса.

На АРМ, подключаемым к ГИСОГД ТО, должны быть выполнены требования по:

* обеспечению антивирусной защиты;
* обеспечению защиты от несанкционированного доступа;
* обеспечению межсетевого экранирования;
* обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации;
* выполнение обязательных организационных мероприятий, необходимых при эксплуатации СКЗИ в соответствии с требованиями нормативных документов ФСБ России;
* проведение оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится не реже одного раза в 3 года Организацией самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

1. **Перечень необходимых средств защиты информации для подключения к ГИСОГД ТО**

Перечень необходимых типов средств защиты информации и их состав в зависимости от варианта подключения представлены ниже.

Вариант 1:

Применяется в случае подключения отдельных АРМ с установленной операционной системой Astra Linux SE 1.7 Воронеж.

|  |  |  |
| --- | --- | --- |
| № п/п | Тип средств защиты информации | Наименование средств защиты информации |
| 1 | Средство антивирусной защиты | Kaspersky Endpoint Security for Linux или аналог |
| 2 | Средство межсетевого экранирования | ViPNet Personal Firewall 4.5 |
| 2 | Средство криптографической защиты информации | ViPNet Client 4U for Linux |

Вариант 2:

Применяется в случае подключения отдельных АРМ с установленной операционной системой Windows.

|  |  |  |
| --- | --- | --- |
| № п/п | Тип средств защиты информации | Наименование средств защиты информации |
| 1 | Средство защиты от несанкционированного доступа | Secret Net Studio 8 (Постоянная защита)  |
| 2 | Средство антивирусной защиты | Kaspersky Endpoint Security for Windows или аналог |
| 3 | Средство криптографической защиты информации | ViPNet Client 4 for Windows |

1. **Порядок подключения АРМ пользователей к защищенной сети ГИСОГД ТО**

Для подключения АРМ пользователей к ГИСОГД ТО Организации необходимо:

* для каждого АРМ, претендующего на подключение к ГИСОГД ТО, приобрести, установить и настроить сертифицированные средства защиты информации в соответствии с пунктом 4 настоящих ТУ, в зависимости от установленной на АРМ ОС.
* разработать либо актуализировать организационно-распорядительную документацию, регламентирующую использование СКЗИ в соответствии с требованиями нормативных документов ФСБ России;
* по результатам установки и настройки СЗИ (СКЗИ) Организация составляет Акт установки и настройки средств защиты информации (в том числе криптографических) (Приложение № 2);
* по результатам установки и настройки СЗИ (СКЗИ), разработки (актуализации) организационно-распорядительной документации, регламентирующей использование СКЗИ в соответствии с требованиями нормативных документов ФСБ России, Организация составляет Акт оценки полноты выполнения мер по защите информации для подключения к ГИСОГД ТО (Приложение № 1) и направляет его скан-копию и скан-копию Акта установки и настройки средств защиты информации на адрес электронной почты Министерства цифрового развития и информационных технологий Тверской области: aristovva@tverreg.ru

Ответственность за соблюдение требований настоящих ТУ, обеспечение защиты информации в ходе эксплуатации АРМ пользователей, а также ответственность за соблюдение требований к эксплуатации средств защиты информации и СКЗИ, лежит на владельцах подключаемых АРМ.

Оператор имеет право проводить проверки реализации схем подключения.

В случае выявления нарушений требований настоящих ТУ, Оператор имеет право ограничить доступ АРМ к ГИСОГД ТО.

Приложение № 1. Форма акта оценки полноты выполнения мер
по защите информации для подключения к ГИСОГД ТО

|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ |
|  |  | Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(наименование Организации) |
|  |  | \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) (расшифровка подписи) |
|  |  |  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. м.п. |

**Акт оценки полноты выполненных мер по защите информации
при обработке информации, не содержащей сведения, составляющие государственную тайну, в информационной системе ГИСОГД ТО**

|  |
| --- |
|  |
| *(наименование Организации)* |

Составлен комиссией:

|  |  |
| --- | --- |
| Председатель комиссии: |  |
| Члены комиссии: |  |
|  |  |
|  |  |

Комиссия провела проверку технических и организационных мер по защите информации для работы в ГИСОГД ТО.

Комиссия проверила факт наличия Акта установки и настройки средств защиты информации (в том числе криптографических) № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_;

Разработан и утвержден комплект документации по эксплуатации криптографических средств в соответствии с требованиями нормативных документов ФСБ России:

1. Приказ от \_\_\_\_\_\_\_\_ № \_\_\_\_\_ «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты»,
2. Инструкция ответственного пользователя криптосредств,
3. Инструкция пользователя криптосредств,
4. Перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну,
5. Перечень помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств,
6. Перечень лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств,
7. Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств,
8. Форма Журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов,
9. Форма Журнала учета и выдачи носителей с ключевой информацией,
10. Форма Лицевого счета пользователя криптосредств,
11. Форма Журнала обучения пользователей правилам работы с криптосредствами.

Комиссия сообщает:

**О готовности «**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

 **(**наименование Организации)

к подключению к ГИСОГД ТО.

Составлен в 2-х экземплярах.

Председатель комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 2. Форма акта установки и настройки

средств защиты информации (в том числе криптографических)

Акт
установки и настройки средств защиты информации
(в том числе криптографических) № \_\_\_\_\_

 «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

1. Настоящий акт составлен по результатам установки и настройки средств защиты информации (далее – СЗИ), криптографических средств защиты информации (далее – СКЗИ).
2. Основание: подключение к ГИСОГД ТО.
3. Организация: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
4. Месторасположение АРМ пользователя:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №№п/п | Адрес | Помещение (номер/ наименование) | Компьютер (инвентарный номер/ имя компьютера) | Дата |
|
|  |  |  |  |  |

1. Специалистами \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ произведена установка и настройка следующих СЗИ (СКЗИ):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | НаименованиеСЗИ(СКЗИ) | Идентификатор(Формат идентификатора: РОСС RU.01.xxxxx.xxxxxx) | Компьютер (инвентарный номер/ имя компьютера) | Дата установки |
| 1. |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Установка и настройка СЗИ (СКЗИ) выполнена в соответствии с требованиями эксплуатационной документации. Средства защиты информации работоспособны, реализуют заданные функции и готовы к эксплуатации.

Установку и настройку произвел:

 (должность) (подпись) (расшифровка подписи)