## Требования по защите информации при подключении пользователей к государственной информационной системе учета имущественно-земельного комплекса Республики Карелия

Настоящие Требования установлены на основании документа «Протокол проведения аттестационных испытаний по требованиям безопасности информации объекта информатизации — Государственная информационная система «Имущественно-земельный комплекс Республики Карелия» Министерства имущественных и земельных отношений Республики Карелия», согласованного с ФСТЭК России и определяют меры защиты информации обязательные при подключении к государственной информационной системе «Имущественно-земельный комплекс Республики Карелия» (ГИС ИЗК) [1].

Настоящие Требования соответствуют требованиям, предъявляемым к типовым сегментам ГИС ИЗК, в отношении которых были проведены аттестационные испытания и на которые распространяется действие «Аттестата соответствия требованиям безопасности информации ГИС ИЗК» АС210016К от 20.08.2021.

ГИС ИЗК с возможностью передачи зашифрованной общедоступной информации, информации, содержащей персональные данные с уровнем защищенности УЗ3 соответствует классу защищенности К2.

К ГИС ИЗК подключаются автоматизированные рабочие места пользователей, для которых установлены класс и/или уровень защищенности, соответствующие базовому сегменту ГИС.

|  |  |  |
| --- | --- | --- |
| Требования | Меры защиты информации  Условное обозначение [2] | Реализация |
| Технические меры  (применение средств защиты информации) | Меры группы ИАФ | – Применение на автоматизированном рабочем месте пользователя (АРМ) [3] средств защиты информации от несанкционированного доступа (СЗИ НСД) [4].  – Применение средств криптографической защиты информации [5]: программно-аппаратный комплекс ViPNet Coordinator HW4 необходимой производительности для организации и/или программный комплекс ViPNet Client 4 для индивидуального подключения АРМ пользователя. |
| Меры группы УПД | – Применение на АРМ пользователя СЗИ НСД «Secret Net Studio 8», встроенных СЗИ от НСД ОС «Astra Linux SE» и СЗИ НСД «Secret Net LSP»;  – Применение программного комплекса ViPNet Client.  – Запрет загрузки с внешних носителей средствами BIOS; установка на BIOS пароля из букв, цифр и символов не короче10 знаков; установка пароля на изменение настроек BIOS. – Применение сертифицированного СЗИ АПМДЗ ПАК «Соболь 3.0».  – Применение СКЗИ: программно-аппаратный комплекс ViPNet Coordinator HW4 необходимой производительности для организации и/или программный комплекс ViPNet Client 4 для индивидуального подключения АРМ пользователя;  – Применение межсетевого экрана [6] на границе (периметре) локальной вычислительной сети организации или АРМ пользователя. |
| Меры группы ОПС | – Применение на АРМ пользователя Применение СЗИ НСД «Secret Net Studio 8», встроенных СЗИ от НСД ОС «Astra Linux SE». |
| Меры группы ЗНИ | – Применение на АРМ пользователя СЗИ НСД.  – Контроль интерфейсов использования интерфейсов ввода-вывода с помощью СЗИ НСД «Secret Net Studio 8», встроенных СЗИ от НСД ОС «Astra Linux SE» и СЗИ НСД «Secret Net LSP». |
| Меры группы РСБ | – Применение на АРМ пользователя СЗИ НСД.  – Применение на АРМ средств антивирусной защиты (САВЗ) [7].  – Применение СКЗИ: программно-аппаратный комплекс ViPNet Coordinator HW4 необходимой производительности для организации и/или программный комплекс ViPNet Client 4 для индивидуального подключения АРМ пользователя. |
| Меры группы АВЗ | – Применение на АРМ пользователя САВЗ.  – Утверждены требования к использованию САВЗ, периодичности проведения антивирусных проверок. |
| Меры группы АНЗ | – Применение на АРМ пользователя СЗИ НСД;  – Применение сертифицированного сканера уязвимостей XSpider 7.8  – Применение средств анализа защищенности [8] или выполнение организационных мероприятий по анализу защищенности;  – Применение на АРМ САВЗ. |
| Меры группы ОЦЛ | – Применение на АРМ СЗИ НСД;  – Применение на АРМ САВЗ.  — Утвержден порядок восстановления программного обеспечения, в т.ч. средств защиты информации при возникновении нештатных ситуаций. |
| Меры группы ЗИС | – Применение на АРМ СЗИ НСД;  – Применение СКЗИ: программно-аппаратный комплекс ViPNet Coordinator HW4 необходимой производительности для организации и/или программный комплекс ViPNet Client 4 для индивидуального подключения АРМ пользователя;  – Применение межсетевого экрана на границе (периметре) локальной вычислительной сети организации или на АРМ пользователя. |
| Организационные меры  Правовые меры | Меры группы ИАФ | – Утверждена и выполняется парольная политика в организации, способствующая идентификации и аутентификации пользователей и используемых ими устройств, не допускающая компрометации учётных записей пользователей;  – Утвержден перечень пользователей, допущенных к работе в ГИС ИЗК;  – В адрес оператора ГИС ИЗК предоставлены заявки на работников (сотрудников) организации (внешних пользователей относительно оператора) на подключение к ГИС ИЗК, однозначно определяющие полномочия таких пользователей и информацию, к которой они могут получить доступ. |
| Меры группы УПД | – Назначены минимально необходимые права пользователям АРМ, исключающие возможность выполнение пользователем полномочий администратора операционной системы. |
| Меры группы ОПС | — Утвержден перечень разрешенного к использованию на АРМ пользователей программного обеспечения. |
| Меры группы ЗНИ | – Производится учет машинных носителей информации, уничтожение (стирание) информации на машинных носителях при их передаче между пользователями и в сторонние организации. |
| Меры группы РСБ | – Утвержден порядок мониторинга событий безопасности и реагирования на них. |
| Меры группы АВЗ | – Утверждены требования и порядок обновления средств антивирусной защиты. |
| Меры группы АНЗ | — Утвержден перечень разрешенного к использованию на АРМ программного обеспечения и средств защиты информации;  — Утвержден порядок обновления программного обеспечения, в т. ч. средств защиты информации. |
| Меры группы ОЦЛ, ОДТ | — Утвержден порядок восстановления программного обеспечения, в т. ч. средств защиты информации при возникновении нештатных ситуаций. |
| Меры группы ЗТС | — В организации установлены границы контролируемой зоны, все технические средства обработки информации и машинные носители информации размещены в пределах контролируемой зоны;  — В организации действует пропускной режим, исключающий неконтролируемое пребывание в организации посторонних лиц (не являющихся сотрудниками), имеется действующий договор на охрану помещений;  — В организации утвержден порядок доступа в помещения пользователей ГИС ИЗК, а также в помещения с технологическим оборудованием информационной системы в рабочее и нерабочие время, утвержден перечень лиц, имеющих право доступа в указанные помещения;  — Входные двери в указанные помещения оснащены надежными замками, обеспечено постоянное закрытие дверей указанных помещений на замок и их открытие только для санкционированного прохода;  — Указанные помещения оборудованы охранной сигнализацией и/или обеспечено опечатывание указанных помещений по окончанию рабочего дня;  — АРМ пользователей, с установленным СКЗИ, оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы);  — Все средства защиты информации учтены в специальных журналах. |
| ст. 16 ФЗ от 27 июля 2006 г. № 149-ФЗ | — Назначен ответственный за обеспечение защиты информации в организации  — Наличие утвержденных документов (приказов, распоряжений), закрепляющих выполнение в организации технических и организационных мер. |

Также в ГИС ИЗК реализуется ряд мер защиты информации, которые выполняются исключительно оператором:

* меры группы УПД, в части мер УПД.1, УПД.16;
* меры группы СОВ;
* меры группы ОЦЛ, в части виртуальной серверной инфраструктуры ГИС;
* меры группы ОДТ, в части виртуальной серверной инфраструктуры ГИС;
* меры группы ЗСВ.

Все средства защиты информации (СЗИ НСД, САВЗ, МЭ, СДЗ), применяемые в ГИС ИЗК, должны иметь действующие сертификаты соответствия ФСТЭК России по 5 или более высокому уровню доверия (классу защиты).

СКЗИ должны иметь действующие сертификаты соответствия ФСБ России по классу криптозащиты КС2 или выше.

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

[1] Далее – ГИС ИЗК

[2] Тут и далее меры защиты информации из:

* Приложения № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17;
* Приложения к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21.
* Полное описание мер в Методическом документе «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11 февраля 2014 г.)

[3] Далее – АРМ

[4] Далее – СЗИ НСД

Варианты СЗИ НСД: Secret Net Studio, сертификат соответствия ФСТЭК России № 3745; встроенные СЗИ НСД операционной системы «Astra Linux Special Edition», сертификат соответствия ФСТЭК России № 2557

[5] Далее – СКЗИ

[6] Варианты межсетевого экрана: программно-аппаратный комплекс ViPNet Coordinator HW 4, сертификат соответствия ФСТЭК России № 3692; программно-аппаратный комплекс ViPNet xFirewall 4, сертификат соответствия ФСТЭК России № 4093; универсальный шлюз безопасности UserGate, сертификат соответствия ФСТЭК России № 3905; встроенный МЭ СЗИ Secret Net Studio, сертификат соответствия ФСТЭК России № 3745

[7] Далее – САВЗ

Варианты САВЗ: «Kaspersky Endpoint Security 11» для Windows, сертификат соответствия ФСТЭК России № 4068; «Kaspersky Endpoint Security для виртуальных и облачных сред».

[8] Варианты средств анализа защищенности: XSpider 7.8, сертификат соответствия ФСТЭК России № 3247; Сканер-ВС, сертификат соответствия ФСТЭК России № 2204; Ревизор Сети 3.0, сертификат соответствия ФСТЭК России № 3413. Возможно применение программы ScanOVAL для проверок наличия уязвимостей программного обеспечения (размещена на официальном сайте ФСТЭК России <https://bdu.fstec.ru/scanoval>).