## Ответ к заданию 1.
## Определение СЗИ для аттестации ГИС

**Шаг 1. Определите, какие средства защиты информации в каждой категории вы можете использовать в ГИС (имеют сертификат), чтобы успешно пройти аттестацию.**
Для поиска используйте Государственный реестр сертифицированных средств защиты информации от ФСТЭК России

| **Название средства защиты информации** | **Подходит/Не подходит (указать причину почему не подходит)** |
|---|---|
| **Средства защиты информации от несанкционированного доступа (СЗИ от НСД)** | |
| Secret Net 7 | Не подходит. Истек срок действия сертификата |
| «Страж NT» версия 4.0 | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), РД СВТ(3) |
| Dallas Lock 7.0 | Не подходит. Истек срок действия сертификата |
| Dallas Lock Linux | Не подходит. Используется Windows |
| Dallas Lock 8.0-K<br>https://dallaslock.ru/products/szi-nsd-dallas-lock/szi-ot-nsd-dallas-lock-8-0-k/ | Подходит. Нет САВ. Если выбирать вместо Secret Net Studio (из-за срока лицензии).<br>Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к СКН, Профиль защиты СКН(контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.Н4.ПЗ), Профиль защиты СКН(контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), Требования к СОВ, Профили защиты СОВ(узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ), РД СВТ(5) |
| Secret Net Studio<br>https://www.securitycode.ru/products/secret-net-studio/ | Подходит. Но через месяц истекает сертификат.<br>Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к САВЗ, |

| | |
|---|---|
| | Профиль защиты САВЗ(А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ), Профиль защиты САВЗ(Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ), Профиль защиты САВЗ(В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ), Профиль защиты САВЗ(Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ), Требования к СКН, Профиль защиты СКН(контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), Требования к СОВ, Профили защиты СОВ(узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ), ЗБ, РД СВТ(5) |
| ARMlock<br>https://armlock.pro/ | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), РД СВТ(5) |
| Zecurion Zlock | Не подходит. Нет в реестре |
| **Средства антивирусной защиты информации (САВЗ)** | |
| Kaspersky Endpoint Security 10 для Windows | Не подходит. Нет в реестре |
| Kaspersky Endpoint Security для Linux | Не подходит. Используется Windows |
| Dr.Web Enterprise Security Suite | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования доверия(4), Требования к САВЗ, Профиль защиты САВЗ(А второго класса защиты. ИТ.САВЗ.А2.ПЗ), Профиль защиты САВЗ(А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ), Профиль защиты САВЗ(Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ), Профиль защиты САВЗ(Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ), Профиль защиты САВЗ(В второго класса защиты. ИТ.САВЗ.В2.ПЗ), Профиль защиты САВЗ(В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ), Профиль защиты САВЗ(Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ), Профиль защиты САВЗ(Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ), ЗБ |

| | |
|---|---|
| Kaspersky Endpoint Security для Windows | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования к САВЗ, Профиль защиты САВЗ(Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ), Профиль защиты САВЗ(В второго класса защиты. ИТ.САВЗ.В2.ПЗ), Профиль защиты САВЗ(Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ), Требования к СКН, Профиль защиты СКН(контроля подключения съемных машинных носителей информации второго класса защиты. ИТ.СКН.П2.ПЗ), ЗБ |
| Avast | Не подходит. Нет в реестре |
| 360 Total Security | Не подходит. Нет в реестре |
| ESET NOD32 Secure Enterprise Pack» (версия 5) | Не подходит. Нет в реестре |
| **Межсетевые экраны (МЭ)** | |
| межсетевой экран ESR-20, версия программного обеспечения 1.5 | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ) |
| межсетевой экран ESR-1000, версия программного обеспечения 1.5 | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ) |
| межсетевой экран ИВК КОЛЬЧУГА-К | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ) |
| программно-аппаратный комплекс Dionis-NX | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования к МЭ, Профиль защиты МЭ(А второго класса защиты. ИТ.МЭ.А2.ПЗ), Требования к СОВ, |

| | |
|---|---|
| | Профили защиты СОВ (сети второго класса защиты. ИТ.СОВ.С2.ПЗ) |
| Межсетевой экран TP-LINK ER8411 | Не подходит. Нет в реестре |
| **Средства доверенной загрузки (СДЗ)** | |
| программно-аппаратный комплекс «Соболь». Версия 4» | Подходит.<br>Соответствует требованиям документов: Требования доверия (2), Требования к СДЗ, Профиль защиты СДЗ (платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ) |
| Аккорд-АМДЗ | Не подходит. Это средство СЗИ от НСД |
| модуль доверенной загрузки «Аккорд-МКТ» | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), Требования к СДЗ, Профиль защиты СДЗ(базовой системы ввода-вывода четвертого класса защиты. ИТ.СДЗ.УБ4.ПЗ) |
| Программный модуль доверенной загрузки ViPNet SafeBoot | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования к СДЗ, Профиль защиты СДЗ(базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ) |
| программный комплекс «Электронный замок «ВИТЯЗЬ», версия 2.2 | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования к САВЗ, Профиль защиты САВЗ(Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ), Требования к СДЗ, Профиль защиты СДЗ(базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ) |
| **Системы обнаружения вторжений (СОВ)** | |
| Межсетевой экран и система обнаружения вторжений «Рубикон» | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования к МЭ, Профиль защиты МЭ(А второго класса защиты. ИТ.МЭ.А2.ПЗ), Требования к СОВ, Профили защиты СОВ (сети второго класса защиты. ИТ.СОВ.С2.ПЗ) |

| | |
|---|---|
| система обнаружения вторжений ViPNet IDS HS | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), Требования к СОВ, Профили защиты СОВ(узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ) |
| программный комплекс «Система обнаружения вторжений «Сириус» | Подходит.<br>Соответствует требованиям документов: Требования доверия(4), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ) |
| программный комплекс обнаружения вторжений «Ребус-СОВ» | Подходит.<br>Соответствует требованиям документов: Требования доверия(2), Требования к СОВ, Профили защиты СОВ (сети второго класса защиты. ИТ.СОВ.С2.ПЗ), Профили защиты СОВ(узла второго класса защиты. ИТ.СОВ.У2.ПЗ) |

**Шаг 2. Определите, какое средство защиты информации включает в себя функционал всех категорий, за исключением категории “Средства доверенной загрузки” и напишите цель его применения.**

| № | **Название СЗИ** | **Цель применения** |
|---|---|---|
| 1. | Secret Net Studio | Защита от несанкционированного доступа (НСД);<br>Защита от вредоносного ПО и кибератак;<br>Защита конфиденциальных данных;<br>Централизованное управление безопасностью;<br>Соответствие требованиям регуляторов. |

## Ответ к заданию 2.

## Подготовка к аттестации ИС по требованиям ФСТЭК

При подготовке списка используйте Приказ ФСТЭК России от 29 апреля 2021 г. N 77

| | **Список документов для аттестации** |
|---|---|
| 1. | Технический паспорт на объект информатизации |
| 2. | Акт классификации информационной (автоматизированной) системы |

| | |
|---|---|
| 3. | Модель угроз безопасности информации |
| 4. | Техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации |
| 5. | Проектная документация на систему защиты информации объекта информатизации |
| 6. | Эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации |
| 7. | Документы по защите информации владельца объекта информатизации |
| 8. | Документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации) |

## Ответ к заданию со звездочкой 3. Защита ЦОД

| № | **Требование к ЦОД** | **На какой нормативный документ опирается?** |
|---|---|---|
| 1. | Наличие в договоре пункта, что обработка ПДн ведется в рамках ИСПДн 2 уровня защищенности | ФЗ-152, ПП 1119 |
| 2. | Физическая защита ЦОД | ФЗ-152 "О персональных данных" (ст. 19 – меры защиты).<br><br>Приказ ФСТЭК 21 (п. 5.2 - требования к физической защите).<br><br>ГОСТ Р 56938-2016 "Требования к проектированию и эксплуатации ЦОД". |
| 3. | Техническая защита информации | Приказ ФСТЭК 21 (п. 4, 5 – меры защиты для 2 уровня).<br><br>ГОСТ Р 57580.1-2017 (требования к безопасности инфраструктуры). |
| 4. | Отказоустойчивость и надежность | ГОСТ Р 56938-2016 (п. 5.3 – требования к надежности) |
| 5. | Запрет на хранение/обработку ПДн за пределами РФ | ПП 1119 (п. 10 – локализация данных) |