### **Инструкция к выполнению домашнего задания**

1. Сделайте копию шаблона себе на Google Disk.
2. Выполните домашнее задание в шаблоне.
3. Для проверки домашнего задания отправьте ссылку на ваш документ в личном кабинете Нетологии.
4. Перед тем как выслать ссылку, убедитесь, что ее содержимое не является приватным (открыто на просмотр всем, у кого есть ссылка). Если необходимо прикрепить дополнительные ссылки, просто добавьте их в свой Google Docs.
5. Любые вопросы по решению задач задавайте в чате учебной группы.

**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](https://reestr.fstec.ru/reg3)

|  |  |
| --- | --- |
| **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, срок действия сертификата истек 07.09.2021 |
| «Страж NT» версия 4.0 | Не подходит, срок действия сертификата истек 20.04.2024 |
| Dallas Lock 7.0 | Не подходит, срок действия сертификата истек 11.05.2019 |
| Dallas Lock Linux | Не подходит, данное ПО для другой операционной системы и срок действия сертификата истек 04.07.2024 |
| Dallas Lock 8.0-K | Подходит |
| Secret Net Studio | Подходит |
| ARMlock | Подходит |
| Zecurion Zlock | Не подходит, отсутствует в реестре сертифицированных средств защиты информации |
| **Средства антивирусной защиты информации**  **(САВЗ)** | |
| Kaspersky Endpoint Security 10 для Windows | Не подходит, срок действия сертификата истек 25.11.2019 |
| Kaspersky Endpoint Security для Linux | Не подходит, данное ПО для другой операционной системы. |
| Dr.Web Enterprise Security Suite | Подходит |
| Kaspersky Endpoint Security для Windows | Подходит |
| Avast | Не подходит, отсутствует в реестре сертифицированных средств защиты информации |
| 360 Total Security | Не подходит, отсутствует в реестре сертифицированных средств защиты информации |
| ESET NOD32 Secure Enterprise Pack» (версия 5) | Подходит |
| **Межсетевые экраны**  **(МЭ)** | |
| Межсетевой экран ESR-20, версия программного обеспечения 1.5 | Подходит |
| Межсетевой экран ESR-1000, версия программного обеспечения 1.5 | Не подходит, отсутствует в реестре сертифицированных средств защиты информации |
| Межсетевой экран ИВК КОЛЬЧУГА-К | Подходит |
| Программно-аппаратный комплекс Dionis-NX | Подходит |
| Межсетевой экран TP-LINK ER8411 | Не подходит, отсутствует в реестре сертифицированных средств защиты информации |
| **Средства доверенной загрузки**  **(СДЗ)** | |
| Программно-аппаратный комплекс «Соболь». Версия 4» | Подходит |
| Аккорд-АМДЗ | Подходит |
| Модуль доверенной загрузки «Аккорд-МКТ» | Подходит |
| Программный модуль доверенной загрузки ViPNet SafeBoot | Подходит |
| Программный комплекс «Электронный замок «ВИТЯЗЬ», версия 2.2 | Не подходит, срок действия сертификата истек 11.07.2024 |
| **Системы обнаружения вторжений**  **(СОВ)** | |
| Межсетевой экран и система обнаружения вторжений «Рубикон» | Подходит |
| Система обнаружения вторжений ViPNet IDS HS | Подходит |
| Программный комплекс «Система обнаружения вторжений «Сириус» | Подходит |
| Программный комплекс обнаружения вторжений «Ребус-СОВ» | Подходит |

**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. | Cредство защиты информации Secret Net Studio | * защита информации от несанкционированного доступа; * антивирусная защита; * межсетевое экранирование; * контроль действий приложений (HIPS); * защита от сетевых атак (NIPS); * создание защищенного соединения с удаленными компьютерами; * шифрование контейнеров; * централизованное развертывание, управление и мониторинг.   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) |

**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](https://u.netology.ru/backend/uploads/lms/attachments/files/data/54671/%D0%9F%D1%80%D0%B8%D0%BA%D0%B0%D0%B7_%D0%A4%D0%A1%D0%A2%D0%AD%D0%9A_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%BE%D1%82_29_%D0%B0%D0%BF%D1%80%D0%B5%D0%BB%D1%8F_2021_%D0%B3._N_77.pdf)

|  |  |
| --- | --- |
|  | **Список документов для аттестации** |
| 1. | Технический паспорт на объект информатизации по форме согласно приложениям N 1, 2 к Приказу\_ФСТЭК\_России от 29 апреля 2021 г. №77 |
| 2. | Акт классификации информационной (автоматизированной) системы по форме согласно  приложению N 3 к Приказу ФСТЭК России от 29 апреля 2021 г. №77 |
| 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 (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) (в случае их разработки в  ходе создания объекта информатизации) |
| 5. | Проектную документацию на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации) |
| 6. | Эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации |
| 7. | Организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации |
| 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?** |
| *0.* | ***Пример***  *Наличие аттестата соответствия не ниже 2 уровня защищенности* | *Приказ ФСТЭК России № 17* |
| 1. |  |  |