Организации, подключаемой к ГИС «Контур ВВ ЕИС Росфинмониторинга» необходимо выполнить требования по защите информации в соответствии с Приказом ФСТЭК от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для ГИС К1, провести оценку эффективности реализованных в рамках системы защиты мер и предоставить в Центральный аппарат Росфинмониторинга копию Протокола оценки эффективности реализованных в рамках системы защиты мер и Акты установки средств защиты информации.

Для подключения к ГИС «Контур ВВ» ЕИС Росфинмониторинга необходимо приобрести и установить **продукт линейки С-Терра не ниже класса КС3 с целью организации защищенного канала передачи данных**.

На стороне Организации необходимо провести установку следующих средств защиты:

* информации от несанкционированного доступа;
* средство доверенной загрузки;
* средство анализа защищенности;
* средство обнаружения вторжений;
* средство антивирусной защиты.

Все установленные средства защиты информации должны соответствовать 4 уровню доверия к средствам защиты информации.

При отсутствии возможности реализации отдельных мер по обеспечению безопасности и (или) невозможности их применения, должны быть разработаны и внедрены компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации.

Так же в рамках реализации мер защиты информации Организации необходимо утвердить комплект организационно-распорядительной документации по ИБ:

1. Положение по защите информации;
2. Регламент управления доступом к информационным ресурсам;
3. Регламент по работе с машинными носителями информации;
4. Положение по антивирусной защите;
5. Положение по обеспечению сетевой безопасности;
6. Регламент по управлению уязвимостями;
7. Регламент по резервному копированию и восстановлению информации;
8. Регламент по реагированию на инциденты информационной безопасности;
9. Положение о работе с мобильными устройствами (при наличии);
10. Положение по обучению и повышению осведомленности в области ИБ;
11. Регламент по управлению изменениями конфигураций ИС;
12. Регламент проведения внутренних проверок ИБ;
13. Регламент защиты среды виртуализации;
14. Положение о порядке использования СКЗИ;
15. План мероприятий по защите информации в информационной системе;
16. Приказ (распоряжение) о назначении ответственных лиц за обеспечение безопасности информации;
17. Приказ об утверждении «Перечня лиц, имеющих доступ и/или обрабатывающих защищаемую информацию»;
18. Приказ (распоряжение) о назначении ответственных лиц за планирование и контроль мероприятий по защите информации.

Для проведения работ по внедрению (установка, настройка конфигураций) средств защиты информации и оценке эффективности реализованных в рамках системы защиты мер Организация может привлекать лицензиата ФСТЭК и ФСБ России.