**Информация о порядке осуществления аттестации членов Союза:**

Члены СТЭП представляют в адрес саморегулируемой организации документы по аттестации на свои информационные системы, обеспечивающие функционирование электронной площадки.

Аттестаты соответствия информационных систем ЭТП требованиям безопасности информации должны быть получены операторами электронных площадок самостоятельно по договору с лицензиатом ФСТЭК в отношении деятельности по технической защите конфиденциальной информации.

Направляемые в адрес СРО СТЭП аттестационные документы должны содержать указание на соответствие ИС оператора ЭТП классу защищённости К2 в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждёнными Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013г. №17.

Требования к классу защищённости ИС ЭТП основаны на следующих нормах:

-в п. 1.3 Приложения №2 «Требования к операторам электронных площадок, к электронным площадкам …» Приказа Минэкономразвития России № 495 от 23.07.2015 г. говорится о том, что оператор ЭТП должен обеспечить обнаружение (предотвращение) вторжений в ИС ЭТП.

Согласно разделу VII «Обнаружение вторжений (СОВ)» Приложения №2 «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности ИС» к «Требованиям о защите информации, не составляющей гос. тайну …» Приказа ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей гос. тайну, содержащейся в ГИС» от 11.02.2013 г. обнаружение вторжений необходимо в ИС, класс защищенности которых не ниже К2.

-в п. 1.3 Приложения №2 «Требования к операторам электронных площадок, к электронным площадкам …» Приказа Минэкономразвития России № 495 от 23.07.2015 г. говорится о том, что оператор ЭТП должен обеспечить целостность электронной площадки и информации, в том числе резервное копирование и восстановление информации в ИС ЭТП.

Согласно разделу IX «Обеспечение целостности информационной системы и информации (ОЦЛ)» и разделу X «Обеспечение доступности информации (ОДТ)» Приложения №2 «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности ИС» к «Требованиям о защите информации, не составляющей гос. тайну …» Приказа ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей гос. тайну, содержащейся в ГИС» от 11.02.2013 г. обеспечение целостности ИС и информации, а также ее периодического резервного копирования на резервные машинные носители информации, необходимо в ИС, класс защищенности которых не ниже К2.

-п. 1.3 Приложения №2 «Требования к операторам электронных площадок, к электронным площадкам …» Приказа Минэкономразвития России № 495 от 23.07.2015 г. говорится о том, что оператор ЭТП должен обеспечить доступность информации, в том числе защиту электронной площадки от угроз безопасности информации, направленных на отказ в обслуживании электронной площадки.

Согласно разделу X «Обеспечение доступности информации (ОДТ)» Приложения №2 «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности ИС» к «Требованиям о защите информации, не составляющей гос. тайну …» Приказа ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей гос. тайну, содержащейся в ГИС» от 11.02.2013 г. контроль безотказного функционирования тех. средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование необходимо в ИС, класс защищенности которых не ниже К2.