Новый порядок аттестации объектов информатизации: разбираем положения свежего документа от ФСТЭК России

09:02 / 12 августа, 2021

Новый Порядок организации и проведения работ по аттестации объектов информатизации будет способствовать обеспечению реальной безопасности ИС.

Андрей Семенов, заместитель руководителя отдела compliance и аттестации Дирекции по интеграции компании «Ростелеком-Солар»

10 августа Министерство юстиции РФ утвердило новый приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну». Как ясно из названия, он определяет порядок работ по аттестации объектов информатизации, а также требования к процессам, форме и содержанию документов, разрабатываемых при организации и проведении этих работ. Кроме основного нововведения – реестровой модели ведения аттестатов соответствия, данный документ содержит ряд интересных или неоднозначных положений, которые мы хотим подсветить в нашем обзоре. Разберем интересные моменты по порядку.

1. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

Формально изменились требования, на соответствие которым проводятся аттестационные испытания – если раньше это была аттестация на соответствие «*требованиям безопасности информации*», то теперь стало «*требованиям о защите информации*».

2. *Порядок применяется для аттестации объектов информатизации с 1 сентября 2021 года.*

Все работы по аттестации, которые будут выполняться начиная с этой даты, должны проходить в соответствии с новым Порядком. Важно, что это касается даже тех работ, которые будут проводиться в рамках уже ранее заключенных контрактов.

3. *Настоящий Порядок определяет состав и содержание работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.*

Здесь ситуация аналогична той, что была с приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», когда из области регулирования выпадает та защищаемая информация, которая является общедоступной. Формально государственная информационная система (далее – ГИС), обрабатывающая защищаемую общедоступную информацию, в область регулирования данного Порядка не попадает. А если ГИС одновременно не является и информационной системой общего пользования (на основании приказа ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»), то защиту информации в ней регулирует только федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

4. *Аттестация объектов информатизации на соответствие требованиям о защите информации (далее – аттестация) осуществляется федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями, которым на праве собственности или ином законном основании принадлежат объекты информатизации, а также лицами, заключившими контракт на создание объектов информатизации, или лицами, осуществляющими эксплуатацию объектов информатизации (далее – владельцы объектов информатизации).*

Здесь стоит обратить внимание на то, что аттестовывать объекты информатизации теперь имеют право и эксплуатирующие их организации – их в явном виде включили в состав *владельцев объектов информатизации*.

5. *Аттестация объекта информатизации проводится на этапе его создания или развития (модернизации) и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний).*

С одной стороны, положение очевидное. Но на практике нам приходилось сталкиваться с ситуацией, когда заказчик заявлял о необходимости аттестационных мероприятий для информационных систем, выведенных из эксплуатации. Теперь явно названы этапы жизненного цикла ИС, на которых эти испытания требуются.

6. ***По решению руководителя федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, органа местного самоуправления аттестация принадлежащих этому органу объектов информатизации проводится в соответствии с настоящим Порядком структурным подразделением (работниками), ответственными за защиту информации.***

Это нововведение позволяет перечисленным выше органам власти при выполнении ряда условий самостоятельно аттестовывать свои объекты информатизации без наличия лицензии ФСТЭК России на ТЗКИ. Вероятно, это обусловлено необходимостью выполнения положений Постановления Правительства РФ от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации». Оно запрещает ввод систем в эксплуатацию без действующего аттестата соответствия.

7. ***Для проведения аттестационных испытаний органом по аттестации из числа своих работников назначается аттестационная комиссия в составе руководителя комиссии и не менее двух экспертов, обладающих знаниями и навыками в области технической защиты конфиденциальной информации и аттестации объектов информатизации.***

Появился четкий ответ на вопрос о минимальном количестве участников аттестационной комиссии – не менее трех.

8. ***При назначении экспертов органа по аттестации должна быть обеспечена их независимость от владельца объекта информатизации с целью исключения возможности влияния владельца аттестуемого объекта информатизации на результаты аттестационных испытаний, проведенных экспертами органа по аттестации.***

Отметим, что под органом по аттестации Порядок подразумевает «*организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям о защите информации)*». Следовательно, под это определение не подпадают органы власти, решившие самостоятельно аттестовывать свои объекты информатизации.

Еще один важный вопрос пока остается открытым. Он касается критериев определения *независимости экспертов органа по аттестации от владельца объекта информатизации:* может ли теперь коммерческая организация аттестовывать свои объекты информатизации и объекты информатизации головной компании? Раньше это было явно разрешено при условии, что «аттестатор» не проектировал и не внедрял СОИБ аттестуемого объекта информатизации.

9. ***Для проведения работ по аттестации владелец объекта информатизации в качестве исходных данных представляет в орган по аттестации копии ряда документов, включая «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).***

Новый документ однозначно определил ответственного за предоставление результатов инструментального сканирования. Это не орган по аттестации, проводящий испытания, а именно владелец аттестуемого объекта информатизации.

10. ***По решению владельца объекта информатизации указанные в настоящем пункте копии документов представляются в орган по аттестации в виде электронных документов.***

Раньше орган по аттестации, как правило, принимал только бумажные варианты утвержденных документов (с подписью и печатью организации). Теперь же допустимо предоставлять их в электронном виде. Пока остался открытым вопрос о форме их заверения: требуется ли она и если да, то в каком виде? Будет ли достаточно пересылки с авторизованного почтового ящика или понадобится электронная подпись того или иного вида?

11. Аттестационные испытания включают следующие мероприятия и работы:

…

б) проверку наличия и согласования с ФСТЭК России … модели угроз безопасности информации, технического задания на создание (развитие, модернизацию) объекта информатизации или частного технического задания на создание (развитие, модернизацию) объекта информатизации (только для государственных информационных систем).

Тут Порядок ужесточает имеющиеся ранее требования – необходимо будет согласовать с регулятором оба документа сразу. В Постановлении Правительства РФ от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» есть требование в обязательном порядке согласовывать или модель угроз безопасности информации, или техническое задание: «*Техническое задание на создание системы и (или) модель угроз безопасности информации согласуются с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации*». Постановление Правительства имеет больший приоритет, чем приказ ФОИВ. Поэтому ждем пояснений регулятора.

12. ***Заключение и протоколы в течение 5 рабочих дней после утверждения органом по аттестации направляются владельцу объекта информатизации.***

Определен крайний срок, в течение которого необходимо выслать аттестационную документацию владельцу объекта информатизации.

13. ***По результатам устранения недостатков орган по аттестации повторно оформляет заключение, в которое наряду со сведениями, указанными в пункте 18 настоящего Порядка, включаются сведения об устранении владельцем объекта информатизации всех выявленных недостатков, а также делается вывод о возможности выдачи аттестата соответствия требованиям по защите информации на объект информатизации.***

В ряде случаев в номенклатуре аттестационных документов в явном виде появляется дополнительный. Как он будет называться – заключение № 2, повторное заключение?

14. ***Владелец объекта информатизации в случае несогласия с выявленными органом по аттестации недостатками и выводами, содержащимися в заключении и протоколах, направляет в течение 5 рабочих дней с момента получения заключения и протоколов письменное обращение с обоснованием такого несогласия в ФСТЭК России.***

В документе ничего не говорится о возможности «претензионной работы» между владельцем объекта информатизации и органом по аттестации – возможно только обращение владельца объекта информатизации в ФСТЭК России. Явного запрета на урегулирование споров между владельцем объекта информатизации и органом по аттестации нет. Но, учитывая, что у владельца объекта информатизации имеется всего пять дней, чтобы обратиться к регулятору в случае неуспешных переговоров с органом по аттестации, вряд ли вообще получится их провести.

15. ***ФСТЭК России (территориальный орган ФСТЭК России) в течение 10 календарных дней с даты получения обращения проводит оценку документов.***

При осуществлении «арбитражной» работы регулятор не предусмотрел «пауз» на длительные праздничные дни (например, новогодние или майские праздники) и оперирует календарными, а не рабочими днями – это не может не радовать.

16. Орган по аттестации в течение 5 рабочих дней после подписания аттестата соответствия представляет в ФСТЭК России (территориальный орган ФСТЭК России) в электронном виде копии следующих документов:

а) аттестата соответствия объекта информатизации;

б) технического паспорта на объект информатизации;

в) акта классификации системы (сети), акта категорирования значимого объекта;

г) программы и методик аттестационных испытаний объекта информатизации;

д) заключения и протоколов.

В договорах и ПМИ нужно аккуратно подходить к определению даты *подписания аттестата соответствия.* Особенно если есть необходимость иметь запас по времени на обработку, утверждение и отправку документации при наличии ~~бюрократических~~ многоэтапных, требующих различных согласований

процедур внутри органа по аттестации.

Напомним, что максимальная длительность работ по аттестации согласно положениям рассматриваемого Порядка не может превышать четырех месяцев.

17. ***ФСТЭК России (территориальный орган ФСТЭК России) в течение 3 рабочих дней со дня получения от органа по аттестации документов, предусмотренных пунктом 27 настоящего Порядка, вносит сведения об аттестованном объекте информатизации в реестр аттестованных объектов информатизации.***

Самое важное новшество: вводится реестровая (централизованная) система учета выданных аттестатов соответствия на ИС. Будет очень хорошо, если этот реестр (выписка из реестра) станет общедоступным, чтобы была возможность проверить наличие и действительность аттестатов соответствия в отношении интересующих объектов информатизации.

18. ***ФСТЭК России (территориальный орган ФСТЭК России) после внесения сведений об аттестованном объекте информатизации в реестр аттестованных объектов информатизации проводит экспертно-документальную оценку документов, представленных органом по аттестации в соответствии с пунктом 27 настоящего Порядка.***

Регулятор не только требует предоставлять документы по аттестованной ИС, но и будет анализировать их на предмет корректности. Очевидно, что это вызвано желанием ФСТЭК России улучшить качество проводимых органами по аттестации испытаний, что не может не радовать.

19. ***Аттестат соответствия выдается на весь срок эксплуатации объекта информатизации.***

Согласно новому Порядку это касается всех типов объектов информатизации – ГИС, ИСПДн, КИИ, АСУ ТП, ЗП, ИСОП. Раньше бессрочный аттестат соответствия был только у ГИС на основании приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Срок действия аттестатов соответствия других типов объектов информатизации регламентировал ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения», и он составлял не более трех лет.

20. ***Протоколы контроля защиты информации на аттестованном объекте информатизации не реже одного раза в два года предоставляются владельцем объекта информатизации в ФСТЭК России (территориальный орган ФСТЭК России).***

Проводить контроль уровня защиты на аттестованном объекте информатизации будет нужно не реже чем раз в два года. Раньше это требовалось делать ежегодно согласно ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

21. В случае развития (модернизации) объекта информатизации, в ходе которого изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичных средств или заменены на аналогичные средства проводятся дополнительные аттестационные испытания…

В случае развития (модернизации) объекта информатизации, приводящего к повышению класса защищенности (уровня защищенности, категории значимости) объекта информатизации и (или) к изменению архитектуры системы защиты информации объекта информатизации в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры системы защиты информации, состава и мест расположения объекта информации и его компонентов, проводится повторная аттестация…

В явном виде определены критерии, при выполнении которых проводятся дополнительные аттестационные испытания или повторная аттестация. Остается открытым вопрос: требуется ли при проведении повторной аттестации изменять номер и дату выдачи первоначального аттестата соответствия?

22. ***Действие аттестата соответствия приостанавливается ФСТЭК России (территориальным органом ФСТЭК России) в случае…***

Действие аттестата соответствия прекращается ФСТЭК России (территориальным органом ФСТЭК России) в случае…

Регулятор забрал себе полномочия по приостановлению и прекращению действия аттестата соответствия. Раньше они были у органа по аттестации согласно ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения». Хотя в явном виде запрет на приостановление и прекращение действия аттестата соответствия органом по аттестации в Порядке отсутствует, допустимо ли это и каков будет порядок – вопрос пока открытый.

23. ***В случае утраты аттестата соответствия владелец объекта информатизации вправе обратиться в орган по аттестации с заявлением о выдаче дубликата аттестата соответствия.***

Появилась новая возможность – выдача дубликата аттестата соответствия. Из интересного: орган по аттестации не имеет права выдать его копию. По крайней мере, в новом Порядке о таком варианте ничего не говорится. Нужно учитывать, что согласно нормам делопроизводства при выдаче копии документа сохраняются номер и дата выдачи оригинального документа, а вот дубликат документа должен иметь новые реквизиты. Найдет ли этот момент отражение в реестре аттестатов ФСТЭК России – вопрос открытый.

24. ***Орган по аттестации ежегодно не позднее 1 февраля года, следующего за отчетным, представляет в управление ФСТЭК России по федеральному округу, на территории которого расположен орган по аттестации, сведения об аттестованных им объектах информатизации, содержащие наименование объекта информатизации, адрес места его размещения, наименование владельца объекта информатизации, реквизиты выданного аттестата соответствия.***

Еще один из центральных моментов нового Порядка: орган по аттестации будет обязан ежегодно информировать ФСТЭК о проведенных аттестациях. Раньше такой обязанности у него не было (мы не говорим сейчас про аттестационные мероприятия в области государственной тайны). Теперь недобросовестные органы по аттестации не смогут из небытия предъявить аттестаты соответствия на якобы ранее аттестованные ИС. Вероятно, эта норма введена ФСТЭК России, чтобы повысить качество проводимых аттестаций и обеспечить исполнение Постановления Правительства РФ от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» в той части, которая касается аттестации.

25. ***Из Приложения № 1 исключена необходимость указания в техническом паспорте границ контролируемой зоны, линий связи и питания, выходящих за границы контролируемой зоны, а также инвентарных (учетных, серийных) номеров ОТСС и ВТСС, номера лицензий ПО.***

Это положение позволяет заменять СВТ на однотипные и обновлять лицензии на ПО без корректировки технического паспорта. Такая норма соотносится с бессрочным сроком действия аттестата соответствия и выполнением необходимых процедур на всех этапах жизненного цикла ИС.

Это нововведение говорит о том, что ФСТЭК не настаивает на обязательном выполнении требований о защите ИС, не обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, от ПЭМИН, что раньше и обуславливало необходимость отображать границы контролируемых зон и проводные линии.

В качестве ретроспективной информации: документ с названием «Технический паспорт» в российских ГОСТах отсутствует, а вот форму и содержание документа с названием «Паспорт» определяет ГОСТ 34.201-89 «Виды, комплектность и обозначения документов при создании автоматизированных систем».

26. Приложение № 4, определяющее форму аттестата соответствия объекта информатизации, вводит фиксированный формат номера аттестата соответствия.

Раньше каждый орган по аттестации сам определял формат номера аттестата соответствия. Текущий формат фиксирует в номере: <*номер лицензии ФСТЭК России на деятельность по технической защите информации, выданной органу по аттестации*> | <*номер аттестованного объекта информатизации в системе учета органа по аттестации*> | <*год выдачи аттестата соответствия*>. Это позволит сделать номер аттестата соответствия достаточно информативным.

Нераскрытой остается неопределенность с <*номером аттестованного объекта информатизации в системе учета органа по аттестации*> – должен он в обязательном порядке быть сквозным (00001, 00002, 00003) или допускается произвольное, но неповторяемое назначение номеров (00024, 01121, 00001)?

27. ***Приложение № 4, определяющее форму аттестата соответствия объекта информатизации, при эксплуатации аттестованного объекта информатизации не допускает проводить обработку информации в случае обнаружения инцидента безопасности.***

Пока не очень понятно, как реализовать это на практике – например, если инцидентом является компрометация пароля в ИС непрерывного цикла или даже просто попытка его подбора. Также это положение противоречит принципу PDCA и бессрочности аттестатов соответствия.

Будем надеяться, что данное Приложение определяет всего лишь форму (как и указано на его титуле), а не строгое указание по содержанию и данный момент возможно будет исключить из перечня ограничений на эксплуатацию ИС.

Новый Порядок организации и проведения работ по аттестации объектов информатизации, на наш взгляд, будет способствовать обеспечению реальной безопасности ИС. Но при этом в документе есть ряд нераскрытых моментов, а также положений, которые невыполнимы в реальных условиях эксплуатации.

При внесении изменений в нормативные правовые акты мы часто видим в заключении об оценке фактического воздействия НПА, что нововведения «*не несут дополнительных финансовых затрат*». Это не всегда соответствует действительности. В данном случае можно утверждать, что новые положения предложенного Порядка действительно не несут значительных дополнительных затрат по сравнению с ранее имеющимися требованиями.

Главное, чтобы последующие редакции документа учитывали и исправляли недостатки предыдущих, а сам он использовался как инструмент упорядочивания и улучшения ситуации с аттестацией объектов информатизации, а не наказания и запугивания.

***

В качестве бонуса расскажем, при каких условиях новый Порядок позволит эксплуатировать ГИС даже без аттестата соответствия (пусть и не на постоянной основе).

Существует три случая, при которых возможно запретить (временно или постоянно) эксплуатацию ГИС:

1) вновь созданная ГИС не введена в промышленную эксплуатацию (не проведены успешные аттестационные испытания);

2) действие аттестата соответствия приостановлено;

3) действие аттестата соответствия прекращено.

Первый вариант не рассматриваем – он очевиден и вопросов не вызывает.

А далее, как говорят фокусники, следите за руками.

Пункт *42 гласит: «В случае прекращения действия аттестата соответствия владелец объекта информатизации прекращает эксплуатацию объекта информатизации, если действие аттестата соответствия ранее не было приостановлено»*.

То есть на этапе прекращения действия аттестата соответствия требование о прекращении эксплуатации объекта информатизации не распространяется на случай, если *ранее действие аттестата соответствия было приостановлено.*

А есть ли варианты, при которых можно прийти к вышеописанному состоянию – *действие аттестата соответствия было приостановлено* – и при этом ГИС находилась бы в эксплуатации на законных основаниях? Давайте посмотрим.

В пункте 37 говорится, что *в случае приостановления действия аттестата соответствия владелец объекта информатизации прекращает эксплуатацию объекта информатизации или по согласованию ФСТЭК России принимает меры, исключающие возможность возникновения угроз безопасности информации*».

Если на этапе приостановления действия аттестата соответствия ГИС согласовать с ФСТЭК России и принять меры, исключающие возможность возникновения угроз безопасности информации, то даже последующее прекращение действия аттестата соответствия формально не потребует прекращения ее дальнейшей эксплуатации.

Можно предположить, что озвученная возможность связана с необходимостью в ряде случаев продолжать эксплуатацию критичных ИС (например, ИС непрерывного цикла, обеспечивающих критичные функции, или социально значимых систем), даже если в них в определенный момент не соблюдаются все требования безопасности информации.

Не стоит также упускать из виду, что согласно положениям данного Порядка «*действие аттестата соответствия может быть приостановлено на срок не более 90 календарных дней*».

Осталось получить практику согласования с ФСТЭК России мер, исключающих возможность возникновения угроз безопасности информации, их условия и ограничения. Вполне возможно, что реализовать эти меры будет сложнее, чем «переаттестоваться» заново и лайфхак окажется сугубо теоретическим.