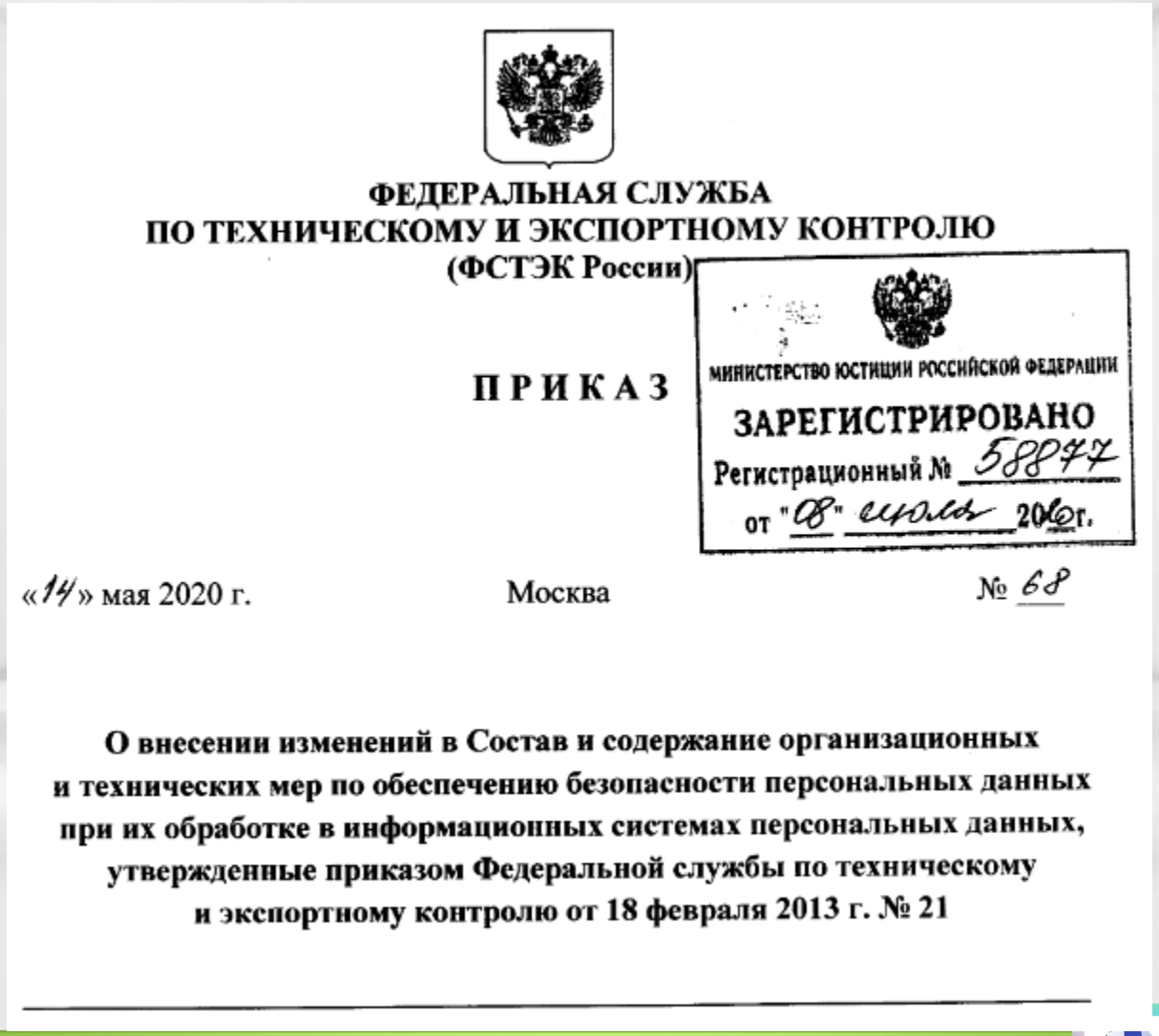
Обратить внимание!

https://minjust.consultant.ru/special/documents/document/46792



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 58877
от "08" июля 2020 г.

П Р И К А З

«14» мая 2020 г. Москва № 68

О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701), подпунктом 9.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2018, № 20, ст. 2818), **П Р И К А З Ы В А Ю**:

1. Внести в пункт 12 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 (зарегистрирован Министерством юстиции Российской Федерации 14 мая 2013 г., регистрационный № 28375) (с изменениями, внесенными приказом Федеральной службы по техническому и экспортному контролю от 23 марта 2017 г. № 49 (зарегистрирован Министерством юстиции Российской Федерации 25 апреля 2017 г., регистрационный № 46487),

следующие изменения:

абзац третий после слов «средства защиты информации не ниже 4 класса» дополнить словами «и 4 уровня доверия»;

абзац четвертый после слов «средства защиты информации не ниже 5 класса» дополнить словами «и 5 уровня доверия»;

в абзаце пятом слова «средства защиты информации не ниже 6 класса» заменить словами «средства защиты информации 6 класса и 6 уровня доверия»;

в абзаце шестом слова «средства защиты информации не ниже 6 класса» заменить словами «средства защиты информации 6 класса и 6 уровня доверия»;

дополнить новым абзацем восьмым следующего содержания:

«Уровни доверия устанавливаются в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом ФСТЭК России от 30 июля 2018 г. № 131 (зарегистрирован Минюстом России 14 ноября 2018 г., регистрационный № 52686).»;

абзацы восьмой – десятый считать соответственно абзацами девятым – одиннадцатым;

абзац одиннадцатый признать утратившим силу.

2. Установить, что настоящий приказ вступает в силу с 1 января 2021 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)**

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

15.10.2020 № 240/24/4268

На №_____

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

Указанный документ предназначен для организаций, осуществляющих в соответствии с законодательством РФ работы по созданию программных, программно-технических средств технической защиты информации, средств обеспечения безопасности информационных технологий, включая защищённые средства обработки информации (далее - средства), заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств на соответствие обязательным требованиям по безопасности информации.

В соответствии с приказом ФСТЭК России от 2 июня 2020 г. № 76 Требования вступают в силу **с 1 января 2021 г.**, за исключением:
абзаца 7 пункта 12.2 и абзаца 9 пункта 12.4, вступающих в силу **с 01.01.2022**;
абзаца 5 пункта 12.5, вступающего в силу **с 01.01.2024**;
абзаца 5 пункта 12.3, вступающего в силу **с 01.01.2028**.
Кроме того с 01.01.2021 признается утратившим силу приказ ФСТЭК России от 30.07.2018 № 131 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».
Изготовителям средств, сертифицированных по схеме сертификации для серийного производства, необходимо привести средства в соответствие Требованиям в сроки, установленные приказом ФСТЭК России от 02.06.2020 № 76, и проинформировать об этом ФСТЭК России в целях переоформления сертификатов соответствия.
Требования применяются к средствам и устанавливают уровни, характеризующие безопасность применения средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа.

Одновременно сообщаем, что в соответствии с приказом ФСТЭК России от 11.08.2020 № 96 при выполнении работ по сертификации средств защиты информации **с 15.08.2020 не применяется** руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», утверждённый приказом Гостехкомиссии России от 4 июня 1999 г. № 114.

Заместитель директора ФСТЭК России  В.Лютиков

ВНИМАНИЕ!

Перечень ГОСТов по ИБ от Росстандарта

- **ГОСТ Р 59343-2021** Системная инженерия Защита информации в процессе гарантии качества для системы (Применяется с 30.11.2021)
- **ГОСТ Р 59346-2021** Системная инженерия Защита информации в процессе определения системных требований (Применяется с 30.11.2021)
- **ГОСТ Р 59352-2021** Системная инженерия Защита информации в процессе верификации системы (Применяется с 30.11.2021)
- **ГОСТ Р 59356-2021** Системная инженерия Защита информации в процессе сопровождения системы (Применяется с 30.11.2021)
- **ГОСТ Р 59381-2021** Информационные технологии Методы и средства обеспечения безопасности Основы управления идентичностью Часть 1 Терминология и концепции (ISO/IEC 24760-1:2019, NEQ)
- **ГОСТ Р 59382-2021** Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы (Применяется с 30.11.2021)
- **ГОСТ Р 59383-2021** Информационные технологии Методы и средства обеспечения безопасности Основы управления доступом (ISO/IEC 29146:2016, NEQ) (Применяется с 30.11.2021)
- **ГОСТ Р 59407-2021** Информационные технологии Методы и средства обеспечения безопасности Базовая архитектура защиты персональных данных (ISO/IEC 29101:2018, NEQ) (Применяется с 30.11.2021)

ВНИМАНИЕ!

Перечень ГОСТов по ИБ от Росстандарта

- **ГОСТ Р 59494-2021** Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5-1. Структуры данных протоколов и мер обеспечения безопасности приложений. XML-схемы (Применяется с 30.11.2021)
- **ГОСТ Р 59502-2021** Единая система условных обозначений в области информационно-телекоммуникационных систем (Применяется с 30.11.2021)
- **ГОСТ Р 59503-2021** Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации (Применяется с 30.11.2021)
- **ГОСТ Р 59515-2021** Информационные технологии Методы и средства обеспечения безопасности Подтверждение идентичности (ISO/IEC TS 29003:2018, NEQ) (Применяется с 30.11.2021)
- **ГОСТ Р 59516-2021** Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности (Применяется с 30.11.2021)
- **ГОСТ Р ИСО/МЭК 27000-2021** Информационные технологии Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности. Общий обзор и терминология (ISO/IEC 27000:2018, IDT) (Применяется с 30.11.2021) ГОСТ Р ИСО/МЭК 27000-2021 утвержден и вводится в действие с 30.11.2021 взамен ГОСТ Р ИСО/МЭК 27000-2012 (приказ Росстандарта от 19.05.2021 № 392-ст).

ВНИМАНИЕ!

Перечень ГОСТов по ИБ от Росстандарта

- **ГОСТ Р ИСО/МЭК 27003-2021** Информационные технологии Методы и средства обеспечения безопасности Системы менеджмента информационной безопасности. Руководство по реализации (ISO/IEC 27003:2017, Information tehnology – Security techniques – Information Security management systems – Guidance, IDT) (Применяется с 30.11.2021) ГОСТ Р ИСО/МЭК 27003-2021 утвержден и вводится в действие с 30.11.2021 взамен ГОСТ Р ИСО/МЭК 27003-2012 (приказ Росстандарта от 19.05.2021 № 387-ст).
- **ГОСТ Р ИСО/МЭК 27017-2021** Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб (Применяется с 30.11.2021)
- **ГОСТ Р ИСО/МЭК 27033-2-2021** Информационные технологии Методы и средства обеспечения безопасности Безопасность сетей Часть 2 Рекомендации по проектированию и реализации безопасности сетей (ISO/IEC 27033-2:2012, IDT) (Применяется с 30.11.2021)
- **ГОСТ Р ИСО/МЭК 27033-4-2021** Информационные технологии Методы и средства обеспечения безопасности Безопасность сетей Часть 4 Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности (ISO/IEC 27033-4:2014, IDT) (Применяется с 30.11.2021)
- **ГОСТ Р ИСО/МЭК 27033-5-2021** Информационные технологии Методы и средства обеспечения безопасности Безопасность сетей Часть 5 Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС) (ISO/IEC 27033-5:2013, IDT) (Применяется с 30.11.2021)

ВНИМАНИЕ!

Перечень ГОСТов по ИБ от Росстандарта

- **ГОСТ Р ИСО/МЭК 27034-2-2021** Информационные технологии Методы и средства обеспечения безопасности Безопасность приложений Часть 2 Нормативная структура организации (ISO/IEC 27034-2:2015, IDT) (Применяется с 30.11.2021)
- **ГОСТ Р ИСО/МЭК 27034-3-2021** Информационные технологии Методы и средства обеспечения безопасности Безопасность приложений Часть 3 Процесс менеджмента безопасности приложений (ISO/IEC 27034-3:2018, Information technology – Aplication security – Part 3: Application security management process, IDT) (Применяется с 30.11.2021)
- **ГОСТ Р ИСО/МЭК 27036-1-2021** Информационные технологии Методы и средства обеспечения безопасности Информационная безопасность в отношениях с поставщиками Часть 1 Обзор и основные понятия

Ваши вопросы?

Обратить внимание!

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
от « 29 » апреля 2021 г. №240/24/2087

Об утверждении порядка аттестации объектов информатизации и особенностях его реализации

В соответствии с подпунктом 13.3 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, приказом ФСТЭК России от 28 сентября 2020 г. № 110 утвержден Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, содержащей сведения, составляющие государственную тайну (далее — Порядок аттестации).

Порядок аттестации предназначен для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений, организаций, которым на праве собственности или ином законном основании принадлежат объекты информатизации, а также для организаций, выполняющих работы по аттестации объектов информатизации на основании лицензии на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации с правом проведения мероприятий и (или) оказания услуг по аттестации объектов информатизации на соответствие требованиям о защите информации), выданной ФСТЭК России.

Указанный документ определяет состав и содержание работ по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, а также требования к форме разрабатываемых при проведении таких работ документов и применяется с 1 июня 2021 г.

Обратить внимание!

В связи с вступлением в силу Порядка аттестации с 1 июня 2021 г. при организации и проведении работ по аттестации объектов информатизации, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, не применяются следующие документы:

Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.;

Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 5 января 1996 г. № 3;

ГОСТ Р 58189-2018 Защита информации. Требования к органам по аттестации объектов информатизации;

ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения.

Порядком аттестации установленно, что аттестационные испытания объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, проводятся организациями, имеющими лицензию ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации с правом проведения мероприятий и (или) оказания услуг по аттестации объектов информатизации на соответствие требованиям о защите информации). Наличие аттестата аккредитации органа по аттестации для проведения указанных работ с 1 июня 2021 г. не требуется. Аккредитация органов по аттестации ФСТЭК России проводиться не будет. Перечень организаций, имеющих право выполнять работы по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, будет размещен на официальном сайте ФСТЭК России.

С целью организации контроля за выполнением работ по аттестации объектов информатизации Порядком аттестации предусмотренно ведение ФСТЭК России единого реестра аттестованных объектов информатизации, а также представление организациями, проводившими аттестацию, материалов с результатами аттестационных испытаний каждого объекта информатизации в территориальные органы ФСТЭК России. В случае установления по результатам экспертизы указанных материалов факта несоответствия аттестованного объекта информатизации требованиям о защите информации действие аттестата соответствия будет приостановлено до устранения выявленного несоответствия объекта информатизации установленным требованиям.

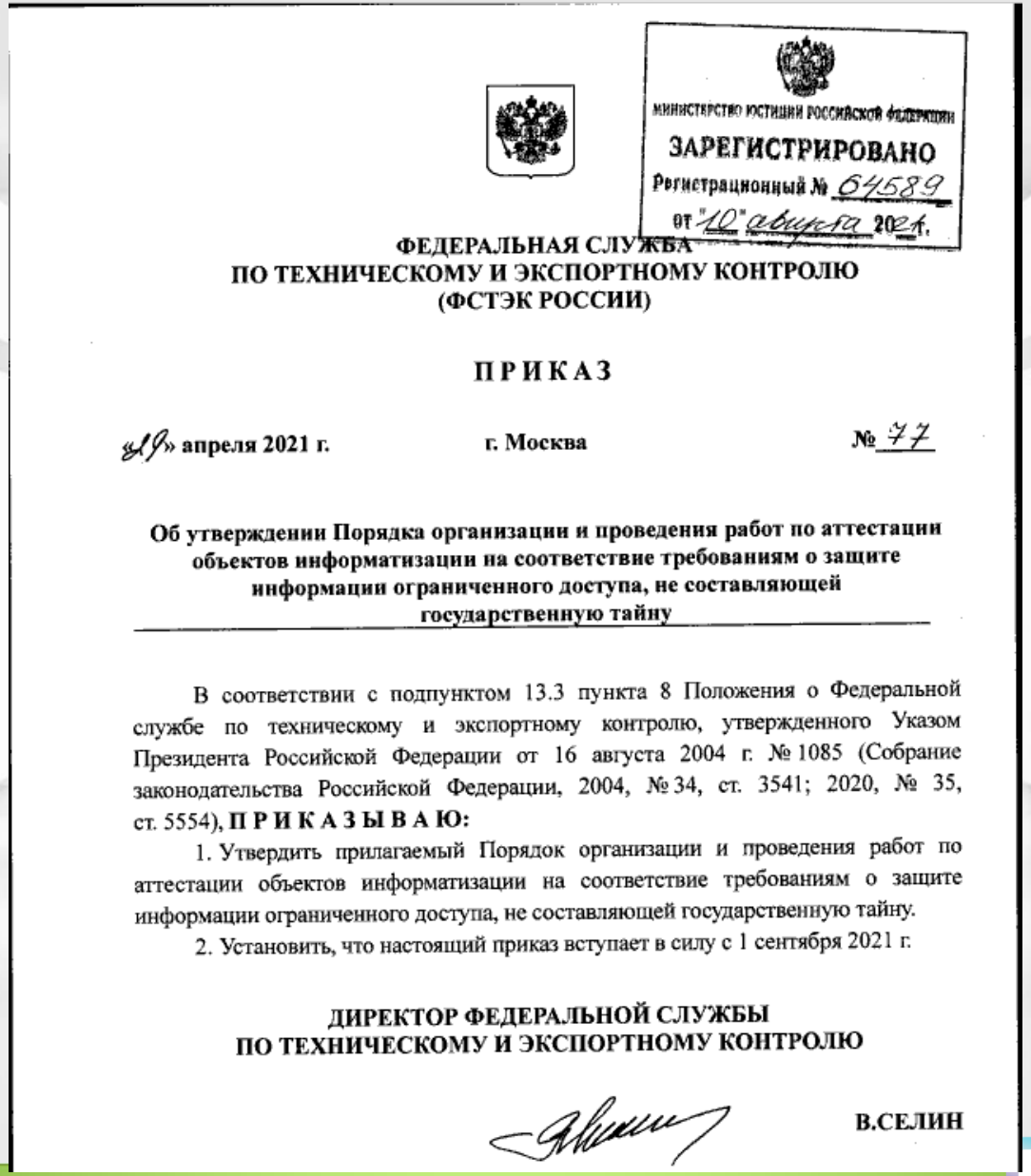
Федеральные органы исполнительной власти обеспечиваются Порядком аттестации центральным аппаратом ФСТЭК России, органы государственной власти субъектов Российской Федерации, органы местного

Обратить внимание!

самоуправления и организации, имеющие лицензию ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации с правом проведения мероприятий и (или) оказания услуг по аттестации объектов информатизации на соответствие требованиям о защите информации) обеспечиваются указанным документом территориальными органами ФСТЭК России (по запросу). Обеспечение документом иных предприятий, учреждений и организаций осуществляется в соответствии с Порядком обеспечения органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций документами ФСТЭК России, размещенном на официальном сайте ФСТЭК России www.fstec.ru в подразделе «Обеспечение документами» раздела «Документы».

Заместитель директора В.Лютиков

ВНИМАНИЕ!



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 64589
от "10" августа 2021 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

П Р И К А З

«19» апреля 2021 г. г. Москва № 77

Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

В соответствии с подпунктом 13.3 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2020, № 35, ст. 5554), **П Р И К А З Ы В А Ю:**

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

2. Установить, что настоящий приказ вступает в силу с 1 сентября 2021 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

ВНИМАНИЕ!

УТВЕРЖДЕН
приказом 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

I. Общие положения

1. Настоящий Порядок определяет состав и содержание работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (далее – требования по защите информации)[1], а также требования к форме и содержанию разрабатываемых при организации и проведении таких работ документов.

---

1 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608), с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933), приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924), приказом ФСТЭК России от 27 апреля 2020 г. № 61 (зарегистрирован Минюстом России 12 мая 2020 г., регистрационный № 58322).

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. № 31 (зарегистрирован Минюстом России 18 мая 2017 г., регистрационный № 46769), с изменениями, внесенными приказом ФСТЭК России от 14 января 2019 г. № 5 (зарегистрирован Минюстом России 27 февраля 2019 г., регистрационный № 53916), приказом ФСТЭК России от 28 октября 2020 г. № 122 (зарегистрирован Минюстом России 25 марта 2021 г., регистрационный № 62868).

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239 (зарегистрирован Минюстом России 26 марта 2018 г., регистрационный № 50524), с изменениями, внесенными приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071), приказом ФСТЭК России от 26 марта 2019 г. № 60 (зарегистрирован Минюстом России 18 апреля 2019 г., регистрационный № 54443), приказом ФСТЭК России от 20 февраля 2020 г. № 35 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59793).

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объекта, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 46769), с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071).

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрирован Минюстом России 14 мая 2013 г., регистрационный № 28375), с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 14 мая 2020 г. № 68 (зарегистрирован Минюстом России 8 июля 2020 г., регистрационный № 58877).

Положение по защите информации при использовании оборудования с числовым программным управлением, предназначенного для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, утвержденные приказом ФСТЭК России от 29 мая 2009 г. № 191 (зарегистрирован Минюстом России 6 июля 2009 г., регистрационный № 14230).

https://www.securitylab.ru/analytics/523324.php

Обзор статей нового порядка аттестации ОИ

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»

10.08.2021 августа Министерство юстиции РФ утвердило новый приказ ФСТЭК России от 29.04.2021 № 77 «Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

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 01.09.2021.

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 11.02.2013 № 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 ГИС, обрабатывающая защищаемую общедоступную информацию, в область регулирования данного Порядка не попадает.

А если ГИС одновременно не является и ИС общего пользования (на основании приказа ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»), то защиту информации в ней регулирует только ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Аттестация ОИ на соответствие требованиям о защите информации осуществляется федеральными ОГВ, ОГВ субъектов РФ, органами местного самоуправления, организациями, которым на праве собственности или ином законном основании принадлежат ОИ, а также лицами, заключившими контракт на создание ОИ, или лицами, осуществляющими эксплуатацию ОИ (владельцы ОИ).

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

5. Аттестация ОИ 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 бывает ситуация, когда заказчик заявлял о необходимости аттестационных мероприятий для ИС, выведенных из эксплуатации. Теперь явно названы этапы жизненного цикла ИС, на которых эти испытания требуются.

6. По решению руководителя федерального ОГВ, ОГВ субъекта РФ, органа местного самоуправления аттестация принадлежащих этому органу ОИ проводится в соответствии с настоящим Порядком структурным подразделением (работниками), ответственными за ЗИ.

Это нововведение позволяет перечисленным ОГВ при выполнении ряда условий самостоятельно аттестовать свои ОИ без наличия лицензии ФСТЭК России на ТЗКИ, что может быть обусловлено необходимостью выполнения положений ПП РФ от 06.07.2015 № 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 3-х.

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 ТЗКИ (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 аттестовать свои ОИ.

Еще один важный вопрос пока остается открытым. Он касается критериев определения независимости экспертов органа по аттестации от владельца ОИ: может ли теперь коммерческая организация аттестовать свои ОИ и ОИ головной компании?

Раньше это было явно разрешено при условии, что «аттестатор» не проектировал и не внедрял СОИБ аттестуемого ОИ.

9. Для проведения работ по аттестации владелец ОИ в качестве исходных данных представляет в орган по аттестации копии ряда документов, включая «документы, содержащие результаты анализа уязвимостей ОИ и приемочных испытаний системы защиты информации ОИ (в случае проведения анализа и испытаний в ходе создания ОИ).

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

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

Ранее орган по аттестации принимал только бумажные варианты утвержденных документов (с подписью и печатью организации).

Теперь 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 (простая, квалифицированная, усиленная квалифицированная)?

11. Аттестационные испытания включают следующие мероприятия и работы:

.....

б) проверку наличия и согласования с ФСТЭК России … модели УБИ, ТЗ на создание (развитие, модернизацию) ОИ или частного технического задания на создание (развитие, модернизацию) ОИ (только для ГИС).

Здесь Порядок ужесточает имеющиеся ранее требования – необходимо будет согласовать с регулятором оба документа сразу. В ПП РФ от 06.07.2015 № 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 согласовать или модель УБИ, или ТЗ: «*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*». ПП имеет больший приоритет, чем приказ ФОИВ. Поэтому необходимо ждать пояснений ФСТЭК.

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

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

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 ОИ всех выявленных недостатков, а также делается вывод о возможности выдачи аттестата соответствия требованиям по защите информации на ОИ.

В ряде случаев в номенклатуре аттестационных документов в явном виде появляется дополнительный.

Как он будет называться – заключение № 2, повторное заключение?

14. Владелец ОИ 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 ОИ и органом по аттестации – возможно только обращение владельца ОИ в ФСТЭК России. Явного запрета на урегулирование споров между владельцем ОИ и органом по аттестации нет. Но, учитывая, что у владельца ОИ имеется всего 5 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 «+».

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 ОИ;

б) технического паспорта на ОИ;

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

г) программы и методик аттестационных испытаний ОИ;

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 многоэтапных, требующих различных согласований процедур внутри органа по аттестации.

Максимальная длительность работ по аттестации согласно положениям рассматриваемого Порядка не может превышать 4-х 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 ОИ в реестр аттестованных ОИ.

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

18. ФСТЭК России (территориальный орган ФСТЭК России) после внесения сведений об аттестованном ОИ в реестр аттестованных ОИ 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 тоже «+».

19. Аттестат соответствия выдается на весь срок эксплуатации ОИ.

Согласно новому Порядку это касается всех типов ОИ – ГИС, ИСПДн, КИИ, АСУ ТП, ЗП, ИСОП.

Ранее бессрочный аттестат соответствия был только у ГИС на основании приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Срок действия аттестатов соответствия других типов ОИ регламентировал ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения», и он составлял не более 3-х лет.

20. Протоколы контроля защиты информации на аттестованном ОИ не реже 1 раза в 2 года предоставляются владельцем ОИ в ФСТЭК России (территориальный орган ФСТЭК России).

Проводить контроль уровня защиты на аттестованном ОИ будет нужно не реже чем 1 раз в 2 года. Раньше это требовалось делать ежегодно согласно ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

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

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

В явном виде определены критерии, при выполнении которых проводятся дополнительные аттестационные испытания или повторная аттестация.
Остается 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».

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 открытый.

23. В случае утраты аттестата соответствия владелец ОИ 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. В новом Порядке о таком варианте ничего не говорится.

Необходимо учитывать, что согласно нормам делопроизводства, при выдаче копии документа сохраняются номер и дата выдачи оригинального документа, а вот дубликат документа должен иметь новые реквизиты.

Будет ли это отражено 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 ОИ, содержащие наименование ОИ, адрес места его размещения, наименование владельца ОИ, 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 ПП РФ от 06.07.2015 № 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 части, которая касается аттестации.

25. Из Приложения № 1 исключена необходимость указания в техническом паспорте границ КЗ, линий связи и питания, выходящих за границы КЗ, 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 КЗ 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 ОИ, 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 ОИ, при эксплуатации аттестованного ОИ 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 титульном листе), а не строгое указание по содержанию и данный момент возможно будет исключить из перечня ограничений на эксплуатацию ИС.

ВЫВОД:

Новый Порядок организации и проведения работ по аттестации ОИ, 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.

ВОПРОС.

При каких условиях новый Порядок позволит эксплуатировать ГИС даже без аттестата соответствия (пусть и не на постоянной основе)? (Частное оценочное суждение экспертов)

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 очевиден и вопросов не вызывает.

А далее, п. 42 гласит: «В случае прекращения действия аттестата соответствия владелец ОИ прекращает эксплуатацию ОИ, если действие аттестата соответствия ранее не было приостановлено».

То есть на этапе прекращения действия аттестата соответствия требование о прекращении эксплуатации ОИ 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 п. 37 говорится, что в случае приостановления действия аттестата соответствия владелец ОИ прекращает эксплуатацию ОИ или по согласованию ФСТЭК России принимает меры, исключающие возможность возникновения УБИ».

Если на этапе приостановления действия аттестата соответствия ГИС согласовать с ФСТЭК России и принять меры, исключающие возможность возникновения УБИ, 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 УБИ, их условия и ограничения. Вполне возможно, что реализовать эти меры будет сложнее, чем переаттестовать ОИ заново.

ТЕМА 9

Установка и настройка программных и программно-аппаратных средств защиты информации от НСД

1. Установка САВЗ
2. Установка СрЗИ от НСД
3. Установка и настройка МСЭ, СОВ (могут входить в состав СрЗИ от НСД, например, DallasLock 8.0-К)
4. ……
5. Рекомендации по установке СрЗИ от НСД

Методики (аттестационных) испытаний системы защиты от НСД

Используемые программные средства

«Terrier»	Программа поиска и гарантированного уничтожения информации на дисках
«ФИКС»	Программа контроля состояния сертифицированных программных средств защиты информации
«Ревизор 1 XP»	Программное средство создания модели системы разграничения доступа
«Ревизор 2 XP»	Программное средство контроля полномочий доступа к информационным ресурсам

Объём проводимых испытаний

- **Анализ и оценка технологического процесса обработки защищаемой информации.**
- **Испытания подсистемы управления доступом:**
  - проверка механизма идентификации
  - проверка механизма аутентификации
  - проверка реализации механизма контроля доступа
- **Испытания подсистемы регистрации и учета.**
- **Испытания подсистемы обеспечения целостности.**
- **Испытания криптографической подсистемы.**

Анализ и оценка технологического процесса обработки информации

Комиссии, представляется описание технологического процесса обработки информации в аттестуемых АС, включающее в себя следующую информацию:

- перечень объектов доступа
- перечень субъектов доступа
- перечень штатных средств доступа к информации в АС
- перечень средств защиты информации
- описание реализованных правил разграничения доступа
- описание информационных потоков

Проверяется соответствие описания технологического процесса обработки и хранения защищаемой информации реальному процессу.

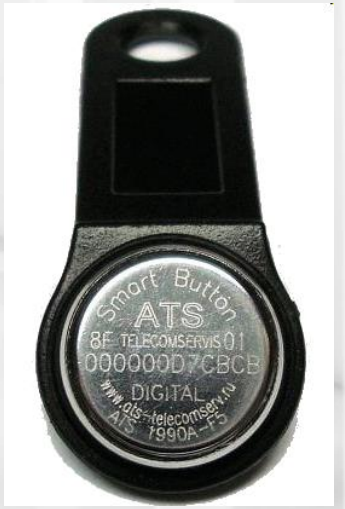
Оценивается возможность переноса информации большего уровня конфиденциальности на информационный носитель меньшего уровня.

Проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретным ОТСС и штатному персоналу.

Оценивается соответствие разрешенных и запрещенных связей разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки.

Испытания подсистемы управления доступом

Проверка правильности **идентификации** субъектов доступа при входе в систему проверяется путем обращения субъектов АС к объектам доступа при помощи штатных средств, для чего системе предъявляются персональные идентификаторы.



Испытания подсистемы управления доступом

Условия соответствия:

при предъявлении идентификатора, незарегистрированного в системе, средства управления должны приостанавливать процесс предоставления доступа;

при неоднократном предъявлении незарегистрированного в системе идентификатора процесс предоставления доступа в систему должен быть прекращен;

при предъявлении зарегистрированного в АС идентификатора процесс предоставления доступа должен быть продолжен.

Испытания подсистемы управления доступом

Проверка подтверждения подлинности субъекта доступа (**аутентификации**).

Производится ввод пароля пользователя, соответствующего предъявленному идентификатору.

Испытания подсистемы управления доступом

Условия соответствия:

- при вводе пароля, не соответствующего предъявленному идентификатору, средства управления должны приостанавливать процесс предоставления доступа;
- при неоднократном вводе пароля, не соответствующего предъявленному идентификатору, процесс предоставления доступа в систему должен быть прекращен;
- при вводе пароля, соответствующего предъявленному идентификатору субъекта доступа должен быть предоставлен доступ в систему в соответствии с его полномочиями.

Испытания подсистемы управления доступом

Проверка **надежности аутентификации**.

Оценивается работоспособность процессов, затрудняющих подбор или несанкционированное получение (хищение) пароля посторонними.

- длина пароля
  - не менее 8 символов в случае смены ежемесячно
  - не менее 12 символов в случае смены ежеквартально
- неотображаемость пароля на экране монитора при его вводе в процессе аутентификации;

- наличия и работоспособности механизма изменения пароля, указания в инструкциях администратору безопасности и пользователям АС требования о его периодической смене.

Испытания подсистемы управления доступом

Проверка **идентификации объектов доступа** проверяется путем обращения субъектов доступа к объектам доступа в АС по идентификаторам объектов.

Обращение должно осуществляться однозначно только к данному объекту.

Объект доступа *(Access object)* - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Испытания подсистемы управления доступом

Проверка **правильности реализации механизма контроля доступа**:

- выборочная проверка соответствия реально установленных средствами СЗИ НСД правил разграничения доступа (разрешительной системе) матрице доступа;
- выборочные попытки совершить НСД, пользуясь при этом правами различных субъектов АС;

проверка осуществляется с помощью сертифицированных программных средств «Ревизор 1 XP» и «Ревизор 2 XP»

Испытания подсистемы управления доступом

Условия правильной реализации контроля доступа:

- установленные СЗИ НСД правила разграничения доступа соответствуют матрице доступа
- попытки НСД к объектам доступа блокируются

Испытания подсистемы регистрации и учета

- Регистрация и учет событий, должны производиться на всех этапах технологического процесса хранения и обработки защищаемой информации.
- Регистрация должна охватывать все события, определенные для АС установленного класса.
- Для проверки необходимо: просмотреть результаты регистрации всех действий, которые были произведены с защищаемыми ресурсами.
- **Должны быть зарегистрированы все требуемые события с требуемыми параметрами регистрации.**

Испытания подсистемы регистрации и учета

- **Проверяется ведение учета информации**, выводимой на печать и всех защищаемых носителей информации, осуществляемого вручную персоналом, путем проверки:
- технологических инструкций,
- степени ознакомления с ними конкретных исполнителей,
- проверки правильности ведения карточек и журналов учета.

Для **проверки средств сигнализации**, попыток нарушения защиты моделируется несанкционированное обращение к защищаемым объектам доступа и отслеживаются появления определенных сигналов в местах интерфейса с администратором системы.

Испытания подсистемы регистрации и учета

- Проверка функционала очистки освобождаемых областей памяти ПЭВМ и внешних носителей (анализатор функционала очистки внешней памяти «Terrier 3.0»)

Для проверки необходимо:

- произвести перезагрузку ПЭВМ;
- получить доступ к ПЭВМ как администратор СЗИ;
- создать на конфиденциальном логическом диске файл, содержащий контрольную комбинацию символов;
- определить местонахождение секторов файла с помощью «Terrier 3.0»;
- удалить файл с диска используя штатные возможности операционной системы и запустить программу «Terrier 3.0» для чтения физических секторов по заданному адресу.

Испытания подсистемы обеспечения целостности

- Надежность функций контроля целостности программных средств СЗИ НСД, обрабатываемой информации и программной среды проверяется при помощи внесения изменений в отдельные их компоненты или подмены этих компонентов.

- **При этом фиксируется реакция системы защиты на произведенные нарушения.**

Испытания подсистемы обеспечения целостности

Условия успешного функционирования подсистемы контроля целостности:

- в АС отсутствуют средства разработки и отладки программ;
- перечень ресурсов, целостность которых подлежит контролю, соответствует требованиям РД для установленного класса;
- при загрузке системы автоматически проверяется целостность контролируемых ресурсов по критериям, заданным РД для установленного класса защищенности АС;
- целостность контролируемых ресурсов производится динамически в процессе работы АС (в случае наличия таких требований для установленного класса защищенности АС);
- при выявлении нарушения целостности контролируемых ресурсов должен выводиться отчет об этом, а обработка информации – блокироваться для всех субъектов доступа, кроме пользователя с правами администратора.

Испытания подсистемы обеспечения целостности

- Проверяется наличие и работоспособность технологии внесения новых программных средств в операционную среду, предусматривающую экспертную оценку или верификацию новых программных средств для выявления потенциально опасных для СЗИ программных функций.
- Оцениваются критерии санкционирования ввода программ в операционную среду и допуска определенных категорий пользователей к этим программам.
- Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду.

Испытания подсистемы обеспечения целостности

Проверяется выполнение требований по:

- физической охране средств ОИ и носителей информации
- пропускному режиму
- и оборудованию помещений необходимыми защитными средствами

Проверяется наличие назначенного администратора (службы) ЗИ, отвечающего за ведение, нормальное функционирование и контроль работы СЗИ НСД, обеспеченного средствами оперативного контроля и воздействия на безопасность АС.

Испытания подсистемы обеспечения целостности

- Производится выборочная проверка на устойчивость АС к заражению вирусами или иными видами разрушающего программного воздействия.
- Для чего производится попытка внедрения в систему тестовой программы-вируса.
- **Проверка считается успешной в случае обнаружения и блокирования попытки заражения штатными антивирусными средствами АС.**

Испытания подсистемы обеспечения целостности

- Проверяется наличие сертификатов соответствия на используемые средства защиты от НСД.
- Проверяется наличие процедур периодического тестирования всех функций СЗИ НСД, наличие графика проведения тестирования.
- Проверяется наличие технологии восстановления программных средств зашиты информации, ведения архива программных средств защиты.
- Автоматическое оперативное восстановление функций СЗИ НСД при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверки функций СЗИ НСД.

Периодичность тестирования

Для АС классов 3А, 3Б, 2А, 2Б, 1Д и 1Г

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

Для АС классов 1В

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств **не реже одного раза в год**;

Для АС классов 1А и 1Б

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств **не реже одного раза в квартал**;

Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по ЗИ.

Подсистема криптографической защиты

Назначение - для усиления защиты пользовательской информации, хранящейся на жестком диске ПЭВМ или сменных носителях.

Позволяет пользователю зашифровать/расшифровать свои данные с использованием индивидуальных ключей, как правило, хранящихся в персональном ТМ - идентификаторе.

Средство криптографической защиты информации (СКЗИ) - СВТ, осуществляющее криптографическое преобразование информации для обеспечения её безопасности

РД Защита от несанкционированного доступа к информации. Термины и определения.

Испытания криптографической подсистемы

- Проверяется наличие сертификатов соответствия на используемые в АС криптографические средства зашиты.
- Проверяется наличие и содержание эксплуатационной документации и инструкций по применению криптографических средств зашиты в АС.
- Проверяется соответствие фактической технологии использования криптографических средств защиты в АС содержанию эксплуатационной документации и инструкций по применению этих средств.

Ваши вопросы?

ТЕМА 10

Общий порядок разработки и производства средств защиты информации от НСД

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ
от 3 марта 2012 г. № 171

О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ПОЛОЖЕНИЕ
О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ
СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. Настоящее Положение определяет порядок лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством Российской Федерации), осуществляемой юридическими лицами и индивидуальными предпринимателями.

2. Лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации (далее - лицензируемый вид деятельности) осуществляет **Федеральная служба по техническому и экспортному контролю**, а в части разработки и производства средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации и Верховного Суда Российской Федерации, - **Федеральная служба безопасности Российской Федерации**

Проверяется наличие у соискателя в лицензиаты:

- Наличие квалифицированного персонала,
- наличие помещений, принадлежащих соискателю,
- наличие на праве собственности или ином законном основании оборудования,
- программных (программно-технических) средств, включая средства контроля эффективности защиты информации, сертифицированных по требованиям безопасности информации,

Проверяется наличие у соискателя в лицензиаты:

- наличие технической и технологической документации, национальных стандартов и методических документов,
- наличие системы производственного контроля.

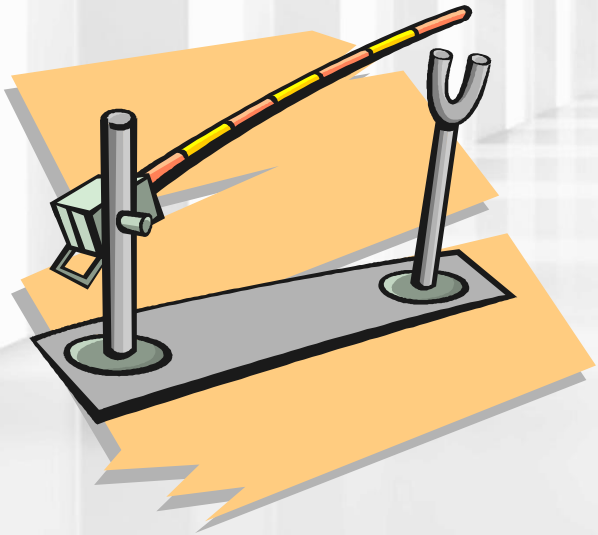
Ваши вопросы?

ТЕМА 11

Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности

Подсистема обеспечения целостности

- **должна** осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая:
  - контроль доступа в помещения АС посторонних лиц
  - надежные препятствия для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время



Федеральная служба войск национальной гвардии Российской Федерации

ГЛАВНОЕ УПРАВЛЕНИЕ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ
(ГУВО Росгвардии)

УТВЕРЖДЕНЫ
Начальником
ГУВО Росгвардии
генерал-лейтенантом полиции
А.В. Грищенко
4 апреля 2019 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

«ИНЖЕНЕРНО - ТЕХНИЧЕСКАЯ УКРЕПЛЕННОСТЬ И ОСНАЩЕНИЕ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ОХРАНЫ ОБЪЕКТОВ И МЕСТ ПРОЖИВАНИЯ И ХРАНЕНИЯ ИМУЩЕСТВА ГРАЖДАН, ПРИНИМАЕМЫХ ПОД ЦЕНТРАЛИЗОВАННУЮ ОХРАНУ ПОДРАЗДЕЛЕНИЯМИ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Р 078 – 2019

Москва 2019

Рекомендации в качестве примера

Мероприятия по **физической защите объекта информатизации и отдельных технических средств**, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности.

- Запираемые двери.
- Решетки на окнах.
- ……

РЕКОМЕНДАЦИИ на каждый день

1. Требования к рабочим местам персонала, занимающегося защитой информации:
   - АРМ с подключением к сети Интернет,
   - Установленная и периодически обновляемая справочная правовая система (КонсультантПлюс, Кодекс) с обязательным подключенным модулем ГОСТ
2. Термины и определения в вопросах профессиональной деятельности…
3. ГОСТ-ы…
4. СрЗИ установлены, но не настроены…
5. Распространение ПДн…передача ПДн…
6. Проверка лицензий у подрядчика…
7. Переписка в случае невыполнения ГК, договора…
8. Служебная переписка внутри организации в части своей профессиональной деятельности…

Ваши вопросы?

Заключение

- Рассмотрев 2 обширных вопроса, мы узнали различные угрозы безопасности информации, связанные с каналами НСД, ТКУИ – АК, ВАК;
- научились бороться с АК и ВАК, каналами НСД;
- теперь умеем применять СрЗИ от НСД на практике.

Список литературы по теме

Основная литература

- Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа: Пособие. - Воронеж: Кварта, 2015. - 440 с.
- Программно-аппаратная защита информации: Учебное пособие / П.Б.
- Хорев. - М.: Форум, 2012. - 352 с.
- Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: Учебное пособие/ В.Ф. Шаньгин. - М.: ДМК Пресс, 2008. - 544 с.;

Дополнительная литература

- Доп. Список – 63 наименования (см. по ссылке https://www.ed.cibit.ru/biblioteka/informacionno-metodicheskoe-obespechenie-tziod/)

Спасибо за внимание

Вопросы самопроверки

- Понятие и общая классификация угроз безопасности информации, связанных с НСД.
- Угрозы утечки информации по нетрадиционным информационным каналам.
- Методы анализа угроз безопасности информации.
- Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной информационной системы.
- Обеспечение защиты информации от НСД при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации
- Требования по защите информации от НСД.
- Требования к мерам защиты информации от НСД, реализуемым в информационной системе. Меры защиты информации от НСД.
- Средства защиты информации от НСД.
- Общий порядок разработки и производства средств защиты информации от НСД.
- Классификация методов контроля защищенности информации от НСД и их характеристика.

- Классификация методов контроля защищенности информации от НСД и их характеристика.
- Сканеры безопасности и их характеристика.
- Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.
- Классы защищенности автоматизированных систем в зависимости от степени секретности информации.
- Способы и комплекс средств защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
- Способы контроля целостности программного обеспечения и аппаратных средств.
- Программные и аппаратные средства защиты информации от программно-математического воздействия.
- Средства обеспечения целостности составных частей компьютера.
- Способы и средства контроля доступа к автоматизированным системам и рабочему месту пользователя.
- Программные средства выявления фактов физического доступа к системному блоку и узлам автоматизированной системы.