ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 30 сентября 2021 г. № 1657

МОСКВА

Об утверждении Правил осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями и нотариусами, указанными в части 18^2 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации", организационных и технических мер по обеспечению безопасности персональных данных и использованием средств защиты информации, указанных в части 18^3 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации"

В соответствии с частью 18^4 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями, нотариусами, указанными в части 18^2 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации", организационных и технических мер по обеспечению безопасности

персональных данных и использованием средств защиты информации, указанных в части 18^3 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации".

2. Настоящее постановление вступает в силу со дня его официального опубликования.

Председатель Правительства
Российской Федерации М.Мишустин

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 30 сентября 2021 г. № 1657

П Р А В И Л А

осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями и нотариусами, указанными в части 18^2 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации", организационных и технических мер по обеспечению безопасности персональных данных и использованием средств защиты информации, указанных в части 18^3 статьи 14^1 Федерального закона "Об информации, информационных технологиях и о защите информации"

I. Общие положения

1. Настоящие Правила устанавливают порядок осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (далее - органы государственного контроля), в пределах их полномочий, предусмотренных законодательством Российской Федерации, мероприятий по контролю и надзору за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с частью 4 статьи 19 Федерального закона "О персональных данных", и использованием средств защиты информации (далее соответственно - контроль, требования по обеспечению безопасности персональных данных) при использовании единой информационной

системы персональных данных, обеспечивающей сбор, обработку и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее - единая биометрическая система), государственными органами, органами местного самоуправления, организациями финансового рынка, иными организациями, индивидуальными предпринимателями и нотариусами для аутентификации физического лица, выразившего согласие на ее проведение, в целях совершения определенных действий или подтверждения волеизъявления либо подтверждения полномочия лица на совершение определенных действий (далее - оператор персональных данных).

2. Контроль осуществляется посредством проведения следующих контрольных (надзорных) мероприятий:

плановая проверка;

внеплановая проверка.

Плановая проверка проводится в форме выездной или документарной проверки, внеплановая проверка - в форме выездной проверки (далее при совместном упоминании - проверка).

3. Выездная проверка проводится по месту нахождения оператора персональных данных. Документарная проверка проводится по месту нахождения органа государственного контроля.

4. Для осуществления плановой проверки органом государственного контроля создается комиссия, в состав которой входят не менее 3 должностных лиц. Внеплановая проверка, проводимая по основанию, указанному в подпункте "а" пункта 21 настоящих Правил, может осуществляться 2 должностными лицами органа государственного контроля.

5. Проверка проводится должностными лицами органа государственного контроля, которые указаны в приказе (распоряжении) органа государственного контроля о проведении проверки.

6. Срок проведения плановой проверки не может превышать 20 рабочих дней.

7. Срок проведения внеплановой проверки не может превышать 10 рабочих дней.

8. В исключительных случаях, связанных с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований на основании мотивированных предложений должностных лиц органа государственного контроля,

проводящих проверку, срок проведения проверки может быть продлен руководителем такого органа, но не более чем на 20 рабочих дней.

9. Срок проведения каждой из проверок, предусмотренных пунктом 2 настоящих Правил, в отношении оператора персональных данных, который осуществляет свою деятельность на территориях нескольких субъектов Российской Федерации, устанавливается отдельно по каждому филиалу, представительству и обособленному структурному подразделению оператора персональных данных, при этом общий срок проведения проверки не может превышать 60 рабочих дней.

10. Проверки в отношении операторов персональных данных, использующих информационные системы персональных данных, которые на праве собственности, аренды или на ином законном основании принадлежат Министерству обороны Российской Федерации, Службе внешней разведки Российской Федерации, Федеральной службе безопасности Российской Федерации, Федеральной службе охраны Российской Федерации и Главному управлению специальных программ Президента Российской Федерации, а также в отношении информационных систем персональных данных, защита которых входит в их компетенцию, проводятся по согласованию с руководителями указанных федеральных органов исполнительной власти.

11. Информация об организации проверок, в том числе об их планировании, о проведении и результатах таких проверок, в органы прокуратуры не направляется, за исключением информации о результатах проверок, проведенных на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

II. Организация плановой проверки

12. Предметом плановой проверки является соблюдение оператором персональных данных требований по обеспечению безопасности персональных данных.

13. Плановые проверки проводятся в соответствии с ежегодным планом, который утверждается руководителем органа государственного контроля, а также в случаях, предусмотренных пунктом 16 настоящих Правил.

14. Основаниями для включения в ежегодный план проверки являются:

а) истечение 1 года после начала использования единой биометрической системы оператором персональных данных для аутентификации физического лица;

б) истечение 5 лет со дня окончания осуществления последней плановой проверки в отношении оператора персональных данных.

15. Ежегодный план проведения плановых проверок содержит следующую информацию:

а) наименование органа государственного контроля;

б) сведения об операторе персональных данных (наименование, место нахождения и осуществления деятельности), в отношении операторов персональных данных, проверяемых по основаниям, указанным в пункте 14 настоящих Правил;

в) наименование подразделения контролирующего органа, проводящего проверки по основаниям, указанным в пункте 14 настоящих Правил;

г) месяц или квартал проведения проверок по основаниям, указанным в пункте 14 настоящих Правил.

16. Плановая проверка осуществляется по обращению оператора персональных данных, планирующего осуществлять аутентификацию физического лица путем проверки принадлежности ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями, размещенными в информационной системе персональных данных такого оператора персональных данных, а также по информации о степени соответствия предоставленных биометрических персональных данных физического лица биометрическим персональным данным, содержащимся в единой биометрической системе, по указанному идентификатору (идентификаторам) (далее - обращение оператора персональных данных).

Плановая проверка по обращению оператора персональных данных проводится не позднее окончания квартала, следующего за кварталом, в котором обращение поступило в орган государственного контроля.

17. Плановая проверка по обращению оператора персональных данных проводится в виде выездной или документарной проверки. Плановая проверка, осуществляемая в соответствии с ежегодным планом проверок, проводится в виде выездной проверки.

18. О дате проведения плановой проверки оператор персональных данных уведомляется органом государственного контроля не менее чем

за 3 рабочих дня до начала ее проведения посредством направления копии приказа (распоряжения) органа государственного контроля о проведении плановой проверки любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

19. Плановая проверка проводится на основании приказа (распоряжения) органа государственного контроля о проведении проверки, содержащего сведения в соответствии с пунктом 20 настоящих Правил.

20. В приказе (распоряжении) органа государственного контроля о проведении плановой проверки указываются:

а) наименование органа государственного контроля, номер и дата издания приказа (распоряжения);

б) должности, фамилии, имена и отчества (при наличии) должностных лиц органа государственного контроля, уполномоченных на проведение плановой проверки;

в) сведения об операторе персональных данных;

г) задачи плановой проверки;

д) дата начала и окончания плановой проверки;

е) срок проведения плановой проверки;

ж) правовые основания проведения плановой проверки, нормативные правовые акты, содержащие требования по обеспечению безопасности персональных данных.

III. Организация внеплановой проверки

21. Предметом внеплановой проверки является соблюдение оператором персональных данных требований по обеспечению безопасности персональных данных, выполнение предписания органа государственного контроля, а также проведение мероприятий по предотвращению нарушений конфиденциальности, целостности и доступности персональных данных, обрабатываемых в информационной системе персональных данных, причиной которых является возникновение компьютерного инцидента. Основаниями для осуществления внеплановой проверки являются:

а) истечение срока выполнения оператором персональных данных выданного органом государственного контроля предписания об устранении выявленного нарушения требований по обеспечению безопасности персональных данных;

б) возникновение компьютерного инцидента в информационной системе персональных данных, повлекшего нарушение конфиденциальности, целостности и доступности персональных данных;

в) приказ (распоряжение) органа государственного контроля, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора, об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям;

г) возникновение угрозы причинения вреда жизни, здоровью граждан либо угрозы безопасности государства.

22. Внеплановая проверка проводится в виде выездной проверки.

23. О проведении внеплановой проверки (за исключением внеплановой проверки, основания для осуществления которой указаны в подпунктах "б" и "г" пункта 21 настоящих Правил) оператор персональных данных уведомляется органом государственного контроля не менее чем за 24 часа до начала ее проведения любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

24. В случае если внеплановая проверка проводится по основаниям, указанным в подпунктах "б" и "г" пункта 21 настоящих Правил, орган государственного контроля вправе приступить к проведению внеплановой проверки незамедлительно.

25. Внеплановая проверка проводится на основании приказа (распоряжения) органа государственного контроля о проведении внеплановой проверки, оформленного в соответствии с пунктом 20 настоящих Правил.

IV. Проведение проверки

26. Проверка начинается с предъявления служебных удостоверений должностными лицами органа государственного контроля, обязательного ознакомления руководителя оператора персональных данных или уполномоченного им должностного лица с приказом (распоряжением) органа государственного контроля о проведении проверки.

27. Руководителю оператора персональных данных или уполномоченному им должностному лицу под расписку передается копия приказа (распоряжения) органа государственного контроля о проведении проверки, заверенная печатью органа государственного контроля.

28. Руководитель оператора персональных данных (уполномоченное им должностное лицо) предоставляет должностным лицам органа государственного контроля, осуществляющим проверку, возможность ознакомиться с документами, связанными с предметом и задачами проверки, а также обеспечивает с учетом требований пропускного режима беспрепятственный доступ проводящих проверку должностных лиц на территорию, в используемые при осуществлении деятельности оператором персональных данных помещения, к информационным системам персональных данных.

29. Для оценки эффективности принимаемых мер во исполнение требований по обеспечению безопасности персональных данных должностными лицами органа государственного контроля используются сертифицированные по требованиям безопасности информации или имеющие положительное заключение, выданное органом государственного контроля, программные и аппаратно-программные средства контроля, в том числе имеющиеся у оператора персональных данных. Использование таких средств контроля не должно нарушать штатный порядок функционирования информационных систем оператора персональных данных.

V. Ограничения при проведении проверки

30. При проведении проверки должностные лица органа государственного контроля не вправе:

а) проверять выполнение требований, если они не относятся к полномочиям органа государственного контроля, от имени которого действуют эти должностные лица;

б) требовать представления документов и информации, если они не относятся к предмету проверки, а также изымать оригиналы таких документов;

в) распространять информацию, полученную в результате проведения проверки и составляющую государственную, коммерческую, служебную или иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации;

г) превышать установленные сроки проведения проверки, за исключением случаев, указанных в пункте 8 настоящих Правил;

д) осуществлять выдачу оператору персональных данных предложений о проведении за его счет мероприятий по контролю.

VI. Обязанности должностных лиц органа государственного контроля при проведении проверки

31. Должностные лица органа государственного контроля при проведении проверки обязаны:

а) своевременно и в полной мере исполнять предоставленные в соответствии с законодательством Российской Федерации полномочия по предупреждению, выявлению и пресечению нарушений оператором персональных данных требований по обеспечению безопасности персональных данных;

б) соблюдать права оператора персональных данных, указанные в пункте 44 настоящих Правил, проверка которого проводится;

в) проводить проверку на основании приказа (распоряжения) органа государственного контроля о ее проведении в соответствии с ее предметом и задачами;

г) проводить проверку во время исполнения служебных обязанностей, при предъявлении служебных удостоверений и копии приказа (распоряжения) органа государственного контроля о проведении проверки;

д) не препятствовать руководителю оператора персональных данных или уполномоченному им должностному лицу присутствовать при проведении проверки и давать разъяснения по вопросам, относящимся к предмету проверки;

е) предоставлять руководителю оператора персональных данных или уполномоченному им должностному лицу, присутствующим при проведении проверки, информацию и документы, относящиеся к предмету проверки;

ж) знакомить руководителя оператора персональных данных или уполномоченное им должностное лицо с результатами проверки;

з) соблюдать сроки проведения проверки, установленные настоящими Правилами;

и) не требовать от оператора персональных данных документы и иные сведения, представление которых не предусмотрено задачами проверки и полномочиями проверяющих лиц органа государственного контроля;

к) осуществлять запись о проведенной проверке в журнале учета проверок при его наличии у оператора персональных данных.

VII. Порядок оформления результатов проверки

32. По результатам проверки должностными лицами органа государственного контроля, проводившими проверку, составляется акт проверки.

33. В акте проверки указываются:

а) дата и место составления акта проверки;

б) наименование органа государственного контроля;

в) дата и номер приказа (распоряжения) органа государственного контроля о проведении проверки;

г) продолжительность и место проведения проверки;

д) фамилии, имена, отчества (при наличии) и должности лиц, проводивших проверку;

е) сведения об операторе персональных данных;

ж) фамилия, имя и отчество (при наличии) руководителя оператора персональных данных или уполномоченного им должностного лица, присутствовавших при проведении проверки;

з) сведения о результатах проверки, в том числе о выявленных нарушениях требований по обеспечению безопасности персональных данных;

и) подписи должностных лиц органа государственного контроля, проводивших проверку;

к) сведения об ознакомлении или отказе от ознакомления с актом проверки руководителя оператора персональных данных или уполномоченного им должностного лица.

34. К акту проверки прилагаются протоколы или заключения по результатам мероприятий по контролю, проведенных с использованием программных и аппаратно-программных средств контроля, а также предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.

35. Акт проверки оформляется непосредственно после ее завершения. Один экземпляр акта проверки с приложениями вручается руководителю оператора персональных данных или уполномоченному им должностному лицу. Второй экземпляр акта проверки высылается в орган государственного контроля, проводивший проверку, третий - в территориальный орган органа государственного контроля, проводившего проверку (в случае проведения им проверки).

36. В случае проведения внеплановой проверки на основании требования прокурора об осуществлении внеплановой проверки в рамках

проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям копия акта проверки с копиями приложений высылается в соответствующий орган прокуратуры.

VIII. Меры, принимаемые должностными лицами органа государственного контроля в отношении фактов нарушения требований по обеспечению безопасности персональных данных, выявленных при проведении проверки

37. В случае выявления при проведении проверки нарушения оператором персональных данных требований по обеспечению безопасности персональных данных должностные лица органа государственного контроля, проводившие проверку, обязаны:

а) выдать оператору персональных данных предписание об устранении выявленного нарушения требований по обеспечению безопасности персональных данных с указанием срока его устранения, который устанавливается в том числе с учетом утвержденных и представленных оператором персональных данных программ (планов) по модернизации (дооснащению) информационной системы персональных данных;

б) принять меры по контролю за устранением выявленного нарушения.

38. В случае невозможности выполнения предписания, предусмотренного подпунктом "а" пункта 37 настоящих Правил, по причинам, не зависящим от оператора персональных данных, руководитель органа государственного контроля при поступлении в орган государственного контроля мотивированного обращения оператора персональных данных вправе продлить срок выполнения указанного предписания, но не более чем на 1 год, уведомив об этом оператора персональных данных в течение 30 дней со дня регистрации указанного обращения.

IX. Ответственность органа государственного контроля и его должностных лиц при проведении проверки

39. Орган государственного контроля и его должностные лица в случае ненадлежащего исполнения соответственно функций, служебных обязанностей и совершения противоправных действий (бездействия) при

проведении проверки несут ответственность в соответствии с законодательством Российской Федерации.

40. Орган государственного контроля осуществляет контроль за исполнением должностными лицами органа государственного контроля служебных обязанностей, ведет учет случаев ненадлежащего исполнения должностными лицами служебных обязанностей, проводит соответствующие служебные проверки и принимает в соответствии с законодательством Российской Федерации меры в отношении таких должностных лиц.

41. Орган государственного контроля обязан сообщить в письменной форме оператору персональных данных, права и (или) законные интересы которого нарушены, о мерах, принятых в отношении виновных в нарушении законодательства Российской Федерации должностных лиц, в течение 10 дней со дня принятия таких мер.

X. Недействительность результатов проверки, проведенной с грубым нарушением положений настоящих Правил

42. К грубым нарушениям положений настоящих Правил относятся:

а) отсутствие оснований для проведения проверки;

б) проведение проверки без приказа (распоряжения) органа государственного контроля;

в) проведение плановой проверки, не включенной в ежегодный план проведения плановых проверок.

43. Результаты проверки, проведенной органом государственного контроля с грубым нарушением положений настоящих Правил, не могут являться доказательствами нарушения оператором персональных данных требований по обеспечению безопасности персональных данных и подлежат отмене органом государственного контроля на основании заявления оператора персональных данных.

XI. Права, обязанности и ответственность оператора персональных данных при осуществлении государственного контроля

44. Руководитель оператора персональных данных или уполномоченное им должностное лицо при проведении проверки имеют право:

а) получать от органа государственного контроля и его должностных лиц информацию, которая относится к предмету проверки и предоставление которой предусмотрено настоящими Правилами;

б) знакомиться с результатами проверки и указывать в акте проверки информацию о своем ознакомлении с результатами проверки, согласии или несогласии с ними, а также с отдельными действиями должностных лиц органа государственного контроля;

в) обжаловать действия (бездействие) должностных лиц органа государственного контроля, повлекшие за собой нарушение прав оператора персональных данных при проведении проверки, в административном и (или) судебном порядке в соответствии с законодательством Российской Федерации.

45. Руководитель оператора персональных данных или уполномоченное им должностное лицо при проведении проверки обязаны:

а) непосредственно присутствовать при проведении проверки и давать пояснения по вопросам, относящимся к предмету проверки;

б) предоставить должностным лицам органа государственного контроля, проводящим проверку, возможность ознакомления с документами, связанными с задачами и предметом проверки;

в) выполнять предписания должностных лиц органа государственного контроля об устранении нарушений в части соблюдения требований по обеспечению безопасности персональных данных, выданные этими лицами в соответствии со своей компетенцией;

г) обеспечить с учетом требований пропускного режима беспрепятственный доступ проводящих проверку должностных лиц на территорию, в используемые при осуществлении деятельности оператора персональных данных здания, строения, сооружения, помещения и к информационным системам персональных данных;

д) принимать меры по устранению выявленных нарушений.

46. Руководитель оператора персональных данных или уполномоченное им должностное лицо, допустившие нарушение положений настоящих Правил, необоснованно препятствующие проведению проверки, уклоняющиеся от проведения проверки и (или) не выполняющие в установленный срок предписания органа государственного контроля об устранении выявленных нарушений требований по обеспечению безопасности персональных данных несут ответственность в соответствии с законодательством Российской Федерации.

47. В случае несогласия с фактами, изложенными в акте проверки и (или) предписании об устранении выявленного нарушения, руководитель оператора персональных данных или уполномоченное им должностное лицо вправе представить в течение 15 дней со дня получения акта проверки в проводивший проверку орган государственного контроля возражения в письменной форме в отношении акта проверки и (или) выданного предписания об устранении выявленного нарушения в целом или их отдельных положений. При этом оператор персональных данных вправе приложить к возражениям документы, подтверждающие обоснованность таких возражений, или их заверенные копии либо в согласованный срок передать их в орган государственного контроля.