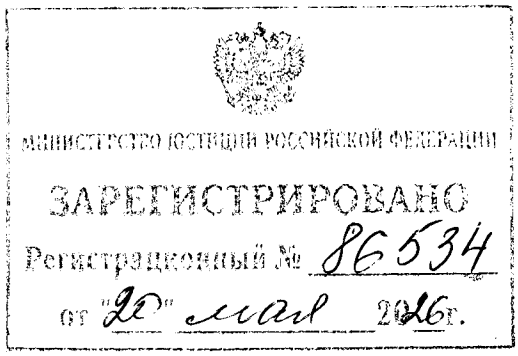
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

22 апреля 2026 года **Москва** № 161



Об утверждении Порядка аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Требований к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам

В соответствии с подпунктом «а» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

П Р И К А З Ы В А Ю:

утвердить:

Порядок аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение № 1 к настоящему приказу);

Требования к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам (приложение № 2 к настоящему приказу).

Директор А.Бортников

Приложение № 1
к приказу ФСБ России
от 22 апреля 2026 г.
№ 161

Порядок
аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

I. Общие положения

1. Аккредитация центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) проводится ФСБ России силами Центра защиты информации и специальной связи ФСБ России (далее – аккредитующий орган) посредством оценки соответствия органов (организаций) требованиям к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам, приведенным в приложении № 2 к настоящему приказу (далее – Требования).

2. Аккредитация центров ГосСОПКА проводится в целях осуществления ими деятельности (далее – направление деятельности) по:

а) обнаружению компьютерных атак и регистрации компьютерных инцидентов;

б) реагированию на компьютерные инциденты и ликвидации их последствий;

в) предупреждению компьютерных атак на информационные ресурсы;

г) координации субъектов ГосСОПКА[1] в рамках деятельности, указанной в подпунктах «а» – «в» настоящего пункта, а также по анализу и выработке мер по повышению защищенности информационных ресурсов.

---

[1] Пункт 3 раздела 3 ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения», утвержденного и введенного в действие приказом Росстандарта от 29 ноября 2022 г. № 1375-ст (М.: Стандартинформ, 2022).

3. По результатам аккредитации выдается аттестат аккредитации (рекомендуемый образец приведен в приложении № 1 к настоящему Порядку) и размещается информация в информационно-телекоммуникационной сети «Интернет» по адресу: https://gossopka.ru либо в адрес органа (организации) направляется уведомление об отказе в аккредитации.

II. Процедура аккредитации и порядок приостановления процедуры аккредитации

4. Для получения аккредитации орган (организация), претендующий (претендующая) на аккредитацию центра ГосСОПКА (далее – соискатель), должен (должна) представить в аккредитующий орган заявление на аккредитацию центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – заявление на аккредитацию) (рекомендуемый образец приведен в приложении № 2 к настоящему Порядку) с приложением к нему документов и сведений об органе (организации), предусмотренных пунктом 6 настоящего Порядка (далее – документы и сведения), а также обеспечить прохождение проверки знаний и навыков работников соискателя, предусмотренной подпунктом «б» пункта 9 настоящего Порядка.

5. Заявление на аккредитацию должно содержать следующие сведения:

полное и сокращенное (при наличии) наименования органа (организации);

основной государственный регистрационный номер;

идентификационный номер налогоплательщика;

адрес в пределах места нахождения органа (организации);

направление (направления) деятельности, по которому (которым) соискатель планирует получить аккредитацию;

перечень прилагаемых документов и сведений;

номер (номера) телефона (телефонов) органа (организации);

адрес (адреса) электронной почты органа (организации) (при наличии).

6. Для получения аккредитации соискатель с заявлением на аккредитацию должен представить следующие документы и сведения:

а) декларацию о соответствии органа (организации) требованиям к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам (далее – декларация) (рекомендуемый образец приведен в приложении № 3 к настоящему Порядку);

б) сведения о единоличном исполнительном органе (руководителе государственного органа):

наименование должности руководителя;

фамилия, имя, отчество (при наличии);

серия и номер документа, удостоверяющего личность;

в) документы, подтверждающие наличие по месту осуществления заявленного (заявленных) направления (направлений) деятельности помещений, не являющихся объектами жилого назначения, принадлежащих соискателю на праве собственности или ином законном основании, предусматривающем право владения и пользования, в которых созданы условия для размещения работников и технических средств для осуществления заявленного (заявленных) направления (направлений) деятельности и права на которые зарегистрированы в Едином государственном реестре недвижимости[1];

г) копии документов, подтверждающих наличие у соискателя в штате по основному месту работы работников, соответствующих Требованиям:

трудовые договоры работников соискателя;

трудовые книжки или сведения о трудовой деятельности работников соискателя;

---

[1] Статья 1 Федерального закона от 13 июля 2015 г. № 218-ФЗ «О государственной регистрации недвижимости».

документы государственного образца (дипломы, аттестаты, свидетельства) об образовании (о переподготовке, повышении квалификации) в соответствии с Общероссийским классификатором специальностей по образованию ОК 009-2016, принятым и введенным в действие приказом Росстандарта от 8 декабря 2016 г. № 2007-ст, работников соискателя;

документы, подтверждающие наличие у работников соискателя, занятых в проведении работ со сведениями, составляющими государственную тайну, формы допуска в соответствии с Требованиями;

д) копии положения о центре ГосСОПКА и состава сил центра ГосСОПКА, разработанных в соответствии с пунктом 6 Требований;

е) сведения о технической оснащенности центра ГосСОПКА в соответствии с Требованиями;

ж) копия лицензии, выданной соискателю на проведение работ, связанных с использованием сведений, составляющих государственную тайну[1];

з) копии лицензий на осуществление деятельности в области защиты информации (при наличии)[2];

и) документы, содержащие результаты работы за последний год, в соответствии с заявленным (заявленными) направлением (направлениями) деятельности (при наличии).

7. Заявление на аккредитацию, документы и сведения, указанные в пункте 6 настоящего Порядка, соискатель должен направить в аккредитующий орган по почте заказным письмом с уведомлением о вручении либо вручить его лично под подпись сотруднику аккредитующего органа. Указанные документы должны быть заверены подписью руководителя соискателя либо уполномоченного им лица и печатью соискателя (при наличии).

---

[1] Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

[2] Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

В случае если заявление на аккредитацию, декларация или документы и сведения подписаны уполномоченным руководителем соискателя лицом, то соискателем прилагаются заверенные копии документов, подтверждающих полномочия указанного лица.

8. Аккредитующий орган должен провести процедуру аккредитации в отношении соискателя в срок, не превышающий 65 рабочих дней со дня приема заявления на аккредитацию и прилагаемых к нему документов и сведений.

9. В ходе процедуры аккредитации аккредитующий орган должен:

а) провести проверку комплектности документов и полноты сведений, представленных соискателем, в срок, не превышающий 10 рабочих дней со дня приема заявления на аккредитацию. В случае отсутствия замечаний аккредитующий орган должен уведомить соискателя о завершении данной проверки посредством направления уведомления по адресу (адресам) электронной почты, указанному (указанным) в заявлении на аккредитацию;

б) провести проверку знаний и навыков работников соискателя согласно заявленному (заявленным) направлению (направлениям) деятельности на предмет соответствия главе III Требований и проверку достоверности сведений, представленных в аккредитующий орган для прохождения процедуры аккредитации, в том числе посредством межведомственного взаимодействия, в срок, не превышающий 50 рабочих дней со дня завершения проверки, указанной в подпункте «а» настоящего пункта.

При наличии технической возможности получение информации от федеральных органов исполнительной власти осуществляется в электронном виде, в том числе посредством использования системы межведомственного электронного взаимодействия[1], а также доступа к информационным ресурсам.

Проверка знаний и навыков работников соискателя проводится по месту его нахождения. В случае, когда такая проверка по месту нахождения

---

[1] Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия».

соискателя невозможна, место ее проведения согласовывается с аккредитующим органом. При наличии у органа (организации) технической возможности и по согласованию с аккредитующим органом допускается проведение проверки знаний и навыков работников соискателя удаленно с использованием технической инфраструктуры аккредитующего органа.

Для проверки знаний и навыков соискатель должен обеспечить присутствие по месту ее проведения не менее 50 процентов работников по каждому заявленному направлению деятельности и не менее минимально достаточного количества работников, предусмотренного главой III Требований, а также руководителя и заместителя руководителя центра ГосСОПКА.

Проверка знаний и навыков считается пройденной в случае если по каждому заявленному направлению деятельности не менее 75 процентов присутствовавших при проверке знаний и навыков работников соискателя, а также руководитель и заместитель руководителя центра ГосСОПКА правильно выполнили не менее 75 процентов тестовых заданий;

в) проверить в отношении соискателя факт отзыва аккредитации в соответствии с подпунктами «а» – «в» пункта 23 настоящего Порядка в течение 3 лет, предшествующих дню подачи заявления на аккредитацию;

г) проверить сведения о том, что лицо, имеющее право действовать без доверенности от имени соискателя, не является лицом, имевшим право действовать без доверенности от имени органа (организации), в отношении которого (которой) была отозвана аккредитация центра ГосСОПКА в соответствии с подпунктами «а» – «в» пункта 23 настоящего Порядка в течение 3 лет, предшествующих дню подачи заявления на аккредитацию;

д) принять решение о приостановлении процедуры аккредитации в случае, указанном в пункте 10 настоящего Порядка;

е) принять решение об аккредитации или отказе в аккредитации центра ГосСОПКА в срок, не превышающий 5 рабочих дней со дня завершения проверки, проведенной в соответствии с подпунктом «б» настоящего пункта.

10. В случае неполучения в рамках межведомственного взаимодействия информации, необходимой для проверки достоверности сведений, представленных в аккредитующий орган для прохождения процедуры аккредитации, в срок, установленный подпунктом «б» пункта 9 настоящего Порядка, аккредитующий орган должен принять решение о приостановлении процедуры аккредитации и в течение 5 рабочих дней со дня принятия такого решения известить соискателя посредством направления уведомления о приостановлении процедуры аккредитации по почте заказным письмом, а также по адресу (адресам) электронной почты, указанному (указанным) в заявлении на аккредитацию.

11. Приостановление процедуры аккредитации осуществляется на срок, не превышающий 30 рабочих дней со дня принятия решения о приостановлении процедуры аккредитации.

12. Неполучение запрашиваемой в ходе межведомственного взаимодействия информации в сроки, установленные настоящим Порядком для проведения и приостановления процедуры аккредитации, не является основанием для отказа в аккредитации центра ГосСОПКА.

13. Уведомление об отказе в аккредитации направляется аккредитующим органом в адрес соискателя по почте заказным письмом, а также по адресу (адресам) электронной почты, указанному (указанным) в заявлении на аккредитацию, не позднее 5 рабочих дней со дня принятия решения об отказе в аккредитации.

14. Основаниями для отказа в аккредитации являются:

а) представление в неполном объеме в аккредитующий орган заявления на аккредитацию, декларации, документов и сведений, предусмотренных настоящим Порядком;

б) нарушение соискателем процедуры аккредитации, предусмотренной настоящей главой;

в) несоответствие соискателя Требованиям;

г) наличие в заявлении на аккредитацию, декларации, документах и сведениях, представленных соискателем, недостоверной информации;

д) отзыв аккредитации соискателя в соответствии с подпунктами «а» – «в» пункта 23 настоящего Порядка в течение 3 лет, предшествующих дню подачи заявления на аккредитацию;

е) наличие сведений о том, что лицо, имеющее право действовать без доверенности от имени соискателя, является лицом, имевшим право действовать без доверенности от имени органа (организации), в отношении которого (которой) была отозвана аккредитация центра ГосСОПКА в соответствии с подпунктами «а» – «в» пункта 23 настоящего Порядка в течение 3 лет, предшествующих дню подачи заявления на аккредитацию.

15. Повторная подача заявления на аккредитацию после отказа в аккредитации в соответствии с подпунктом «а» пункта 14 настоящего Порядка допускается не ранее чем через 5 рабочих дней, а в случаях, предусмотренных подпунктами «б» – «е» пункта 14 настоящего Порядка, – не ранее чем через 50 рабочих дней со дня принятия решения об отказе в аккредитации.

16. Внесение записи об аккредитации центра ГосСОПКА в информационно-телекоммуникационной сети «Интернет» по адресу: https://gossopka.ru, а также направление уведомления об аккредитации центра ГосСОПКА по адресу (адресам) электронной почты органа (организации), указанному (указанным) в заявлении на аккредитацию, осуществляется на следующий рабочий день после дня принятия решения об аккредитации центра ГосСОПКА.

17. Аттестат аккредитации центра ГосСОПКА направляется в адрес органа (организации), в котором (которой) он создан, по почте заказным письмом либо вручается представителю органа (организации) под подпись не позднее 5 рабочих дней со дня принятия решения об аккредитации центра ГосСОПКА.

III. Порядок приостановления действия и отзыва аккредитации центров ГосСОПКА

18. Аккредитующий орган должен незамедлительно принять решение о приостановлении действия аккредитации в случае выявления факта (фактов) несоответствия аккредитованного центра ГосСОПКА Требованиям или представления недостоверной информации органом (организацией) на этапе процедуры аккредитации центра ГосСОПКА и вынести предписание об устранении нарушения в рамках осуществления контроля за деятельностью аккредитованных центров ГосСОПКА[1]. Технические ошибки в документах и сведениях, допущенные органом (организацией), не могут считаться фактом представления недостоверной информации.

19. Аккредитующий орган в день принятия решения о приостановлении действия аккредитации центра ГосСОПКА должен направить по адресу (адресам) электронной почты органа (организации), в котором (которой) функционирует центр ГосСОПКА, предписание об устранении нарушения, содержащее информацию об основаниях и о сроке приостановления действия аккредитации, и внести изменения в запись об аккредитации центра ГосСОПКА в информационно-телекоммуникационной сети «Интернет» по адресу: https://gossopka.ru.

20. Приостановление аккредитации центра ГосСОПКА осуществляется на срок, не превышающий 40 рабочих дней со дня принятия решения о приостановлении аккредитации центра ГосСОПКА.

21. Орган (организация), в котором (которой) функционирует центр ГосСОПКА, в течение 30 рабочих дней после дня принятия решения о приостановлении действия аккредитации должен (должна) представить в аккредитующий орган информацию и (или) документы, подтверждающие устранение нарушений, на основании которых было принято решение о приостановлении действия аккредитации центра ГосСОПКА.

---

[1] Подпункт «г» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Вышеуказанные документы должны быть заверены подписью руководителя органа (организации) либо уполномоченного им лица и печатью органа (организации) (при наличии) и направлены по почте заказным письмом с уведомлением о вручении либо вручены лично под подпись сотруднику аккредитующего органа.

В случае если указанные в абзаце первом настоящего пункта документы подписаны уполномоченным руководителем органа (организации) лицом, то орган (организация) прилагает заверенные копии документов, подтверждающих полномочия указанного лица.

Проверка информации и (или) документов, подтверждающих устранение нарушений, осуществляется аккредитующим органом в срок, не превышающий 10 рабочих дней со дня их получения.

22. В случае если органом (организацией), в котором (которой) функционирует центр ГосСОПКА, в срок не представлены информация и документы в соответствии с пунктом 21 настоящего Порядка либо в случае если по итогам проверки представленных информации и документов причины, вследствие которых было принято решение о приостановлении аккредитации, не устранены, аккредитующим органом принимается решение об отзыве аккредитации.

23. Отзыв аккредитации центра ГосСОПКА осуществляется аккредитующим органом на основании:

а) истечения срока приостановления действия аккредитации центра ГосСОПКА в соответствии с пунктом 20 настоящего Порядка;

б) повторного выявления аккредитующим органом факта (фактов) несоответствия аккредитованного центра ГосСОПКА Требованиям в течение одного года со дня вручения предписания об устранении нарушения;

в) выявления аккредитующим органом фактов осуществления деятельности центром ГосСОПКА по направлению (направлениям), по которому (которым) он не был аккредитован;

г) получения аккредитующим органом заявления от аккредитованного центра ГосСОПКА об отзыве аккредитации по его инициативе;

д) ликвидации органа (организации), в котором (которой) функционирует аккредитованный центр ГосСОПКА.

24. В случае отзыва аккредитации центра ГосСОПКА в соответствии с подпунктами «а» – «в» пункта 23 настоящего Порядка аккредитующий орган должен направить по почте заказным письмом, а также по адресу (адресам) электронной почты органа (организации), в котором (которой) функционирует центр ГосСОПКА, уведомление об отзыве аккредитации и внести изменения в запись об аккредитации центра ГосСОПКА в информационно-телекоммуникационной сети «Интернет» по адресу: https://gossopka.ru в течение 5 рабочих дней со дня наступления основания для отзыва аккредитации.

Отзыв аккредитации в соответствии с подпунктами «г» и «д» пункта 23 настоящего Порядка осуществляется без уведомления органа (организации), в котором (которой) был создан центр ГосСОПКА, посредством внесения изменений в запись об аккредитации центра ГосСОПКА в информационно-телекоммуникационной сети «Интернет» по адресу: https://gossopka.ru.

Приложение № 1
к Порядку аккредитации центров
государственной системы обнаружения,
предупреждения и ликвидации
последствий компьютерных атак
на информационные ресурсы
Российской Федерации (пункт 3)

Рекомендуемый образец

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ И СПЕЦИАЛЬНОЙ СВЯЗИ ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

АТТЕСТАТ АККРЕДИТАЦИИ

**ЦЕНТРА
ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ**

№ _____
(номер)

Срок действия: _____ лет
(не более 5 (пяти) лет)

Настоящий аттестат аккредитации удостоверяет, что

_____
(полное (сокращенное (при наличии) наименование органа (организации)

_____
(адрес в пределах места нахождения органа (организации)

_____
(ИНН органа (организации)

аккредитован (аккредитована, аккредитовано)
в качестве центра ГосСОПКА и может осуществлять деятельность по:

_____

(обнаружению компьютерных атак и регистрации компьютерных инцидентов;
реагированию на компьютерные инциденты и ликвидации их последствий;
предупреждению компьютерных атак на информационные ресурсы;
координации деятельности подразделений субъектов ГосСОПКА)

Регистрационный номер
центра ГосСОПКА

№ _____

Должность
уполномоченного должностного лица

Дата выдачи: _____ _____ 20___ г.

_____ _____
(подпись) **(инициалы, фамилия)**

Приложение № 2
к Порядку аккредитации центров
государственной системы обнаружения,
предупреждения и ликвидации
последствий компьютерных атак
на информационные ресурсы
Российской Федерации (пункт 4)

Рекомендуемый образец

Заместителю руководителя
Научно-технической службы –
начальнику Центра защиты
информации и специальной
связи ФСБ России

_____
(фамилия, инициалы)

_____
(почтовый адрес)

Заявление на аккредитацию центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

_____
(полное (сокращенное (при наличии) наименование юридического лица, ИНН, ОГРН)

_____
(адрес в пределах места нахождения)

просит аккредитовать центр ГосСОПКА _____
(наименование органа (организации)

по следующему (следующим) направлению (направлениям) деятельности:

_____
(направление (направления) деятельности)

С проведением процедуры аккредитации ознакомлен, с проведением в отношении центра ГосСОПКА и органа (организации) проверок

и размещением информации о центре ГосСОПКА в информационно-телекоммуникационной сети «Интернет» по адресу: https://gossopka.ru согласен.

К заявлению прилагаю:

1. _____

2. _____

№№. _____

Способ получения аттестата аккредитации _____
(заказным письмом (лично)

Информация для получения уведомлений от аккредитующего органа о прохождении процедуры аккредитации:

адрес (адреса) электронной почты (при наличии): _____

номер (номера) телефона (телефонов): _____

Согласен получать уведомления об отказе в аккредитации, о приостановлении аккредитации центра ГосСОПКА и по другим вопросам в рамках аккредитации центра ГосСОПКА по электронной почте по адресу (адресам), указанному (указанным) в настоящем заявлении.

_____
(должность руководителя органа (организации)

_____ _____ _____
либо уполномоченного им лица) (подпись) (инициалы, фамилия)

____ _____ 20__ г.

Приложение № 3
к Порядку аккредитации центров
государственной системы обнаружения,
предупреждения и ликвидации
последствий компьютерных атак
на информационные ресурсы
Российской Федерации
(подпункт «а» пункта 6)

Рекомендуемый образец

Декларация о соответствии

_____
(полное (сокращенное (при наличии) наименование органа (организации)

требованиям к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам

_____ подтверждает,
(полное (сокращенное (при наличии) наименование органа (организации)

что соответствует требованиям к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккредитованным центрам.

1. _____ не находится
(полное (сокращенное (при наличии) наименование органа (организации)

под юрисдикцией иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия[1], прямо или косвенно подконтрольный им либо аффилированный с ними.

2. Руководитель _____,
(полное (сокращенное (при наличии) наименование органа (организации)

руководитель центра ГосСОПКА и его заместитель отсутствуют в реестре иностранных агентов[2].

---

[1] Перечень иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, утвержденный распоряжением Правительства Российской Федерации от 5 марта 2022 г. № 430-р.

[2] Статья 5 Федерального закона от 14 июля 2022 г. № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием».

3. _____ подтверждает,
(полное (сокращенное (при наличии) наименование органа (организации)

что у руководителя центра ГосСОПКА и его заместителя отсутствуют судимости и (или) факты уголовного преследования либо прекращено уголовное преследование по реабилитирующим основаниям.

_____
(должность руководителя органа (организации)

_____ _____ _____
либо уполномоченного им лица) (подпись) (инициалы, фамилия)

____ _____ 20__ г.

Приложение № 2
к приказу ФСБ России
от 22 апреля 2026 г.
№ 161

Требования
к центрам государственной системы обнаружения,
предупреждения и ликвидации последствий компьютерных атак
на информационные ресурсы Российской Федерации,
а также к аккредитованным центрам

I. Общие положения

1. Центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) должен создаваться в органе (организации), который (которая) не находится под юрисдикцией иностранных государств, прямо или косвенно подконтрольных им либо аффилированных с ними.

2. Центр ГосСОПКА должен создаваться в органе (организации), имеющем (имеющей) лицензию ФСБ России на право осуществления работ, связанных с использованием сведений, составляющих государственную тайну[1].

3. При осуществлении своей деятельности центр ГосСОПКА должен руководствоваться в том числе методическими документами Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ)[2].

Центр ГосСОПКА должен обеспечить информационную безопасность в соответствии с требованиями, приведенными в приложении № 1 к настоящим Требованиям.

---

[1] Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

[2] Подпункт 4.3 пункта 4 Положения о Национальном координационном центре по компьютерным инцидентам, утвержденного приказом ФСБ России от 24 июля 2018 г. № 366 (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109), с изменениями, внесенными приказом ФСБ России от 24 декабря 2025 г. № 540 (зарегистрирован Минюстом России 25 декабря 2025 г., регистрационный № 84777) (далее – Положение № 366).

4. Деятельность центра ГосСОПКА должна осуществляется в соответствии с аттестатом аккредитации по следующим направлениям:

а) обнаружение компьютерных атак и регистрация компьютерных инцидентов;

б) реагирование на компьютерные инциденты и ликвидация их последствий;

в) предупреждение компьютерных атак на информационные ресурсы;

г) координация субъектов ГосСОПКА[1] в рамках деятельности, указанной в подпунктах «а» – «в» настоящего пункта, а также анализ и выработка мер по повышению защищенности информационных ресурсов.

5. Для осуществления своей деятельности центр ГосСОПКА должен выполнять следующие функции:

непрерывное автоматизированное взаимодействие с НКЦКИ;

инвентаризация информационных ресурсов;

проведение мероприятий по оценке защищенности информационных ресурсов от компьютерных атак, в том числе методом тестирования на проникновение;

выявление уязвимостей информационных ресурсов;

анализ угроз информационной безопасности;

прием сообщений о признаках компьютерных инцидентов от персонала и пользователей информационных ресурсов;

анализ событий информационной безопасности;

регистрация компьютерных инцидентов;

реагирование на компьютерные инциденты;

ликвидация последствий компьютерных инцидентов;

установление причин возникновения компьютерных инцидентов;

анализ результатов ликвидации последствий компьютерных инцидентов;

---

[1] Пункт 3 раздела 3 ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения», утвержденного и введенного в действие приказом Росстандарта от 29 ноября 2022 г. № 1375-ст (М.: Стандартинформ, 2022).

формирование предложений по повышению уровня защищенности информационных ресурсов;

выполнение информационных заданий, поступающих от НКЦКИ, в части отработки сценариев действий по реагированию на компьютерные инциденты, а также представление в НКЦКИ запрашиваемой информации и материалов в части деятельности по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты (далее – ОКА и РКИ).

Центр ГосСОПКА должен выполнять указанные функции в соответствии с осуществляемым (осуществляемыми) направлением (направлениями) деятельности, которое (которые) приведено (приведены) в приложении № 2 к настоящим Требованиям.

6. Для осуществления своей деятельности центр ГосСОПКА должен иметь следующие документы, утвержденные руководителем органа (организации), в котором (которой) он создается, либо уполномоченным им лицом:

положение о центре ГосСОПКА, содержащее основные цели его создания, направления деятельности, функции и описание всех типов (видов) взаимодействия и субъектов такого взаимодействия, в том числе НКЦКИ, ФСБ России, субъектов критической информационной инфраструктуры Российской Федерации, организаций, не являющихся субъектами критической информационной инфраструктуры Российской Федерации, в отношении которых осуществляются мероприятия по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, подразделений органа (организации), в котором (которой) создан центр ГосСОПКА;

состав сил центра ГосСОПКА, содержащий перечень работников с указанием фамилий, имен, отчеств (при наличии) работников, занимаемые ими должности, данные об образовании (о квалификации) и опыте работы, а также возложенные на них функции.

7. Присвоение наименования центру ГосСОПКА должно осуществляться посредством добавления к словам «центр ГосСОПКА» названия органа (организации), в рамках которого (которой) он функционирует. Допускается добавление слов «ведомственный», «корпоративный» или «отраслевой» перед словами «центр ГосСОПКА» в случае организации центра по ведомственному, корпоративному или отраслевому принципу[1].

II. Требования к технической оснащенности центров ГосСОПКА

8. Центр ГосСОПКА для проведения работ по заявленным направлениям деятельности должен соответствовать требованиям к технической оснащенности центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, приведенным в приложении № 3 к настоящим Требованиям. Центру ГосСОПКА запрещается использовать средства, странами происхождения которых являются иностранные государства и территории, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия[2], либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

9. В случае использования при осуществлении своей деятельности средств управления событиями информационной безопасности, платформ реагирования на компьютерные инциденты, платформ анализа информации киберразведки и средств обмена информацией, предназначенных для

---

[1] Пункт 6 раздела 3 ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения», утвержденного и введенного в действие приказом Росстандарта от 29 ноября 2022 г. № 1375-ст.

[2] Перечень иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, утвержденный распоряжением Правительства Российской Федерации от 5 марта 2022 г. № 430-р.

непрерывного автоматизированного взаимодействия с НКЦКИ, такие средства и платформы должны соответствовать Требованиям к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе к средствам, предназначенным для поиска признаков компьютерных атак, утвержденным приказом ФСБ России от 26 декабря 2025 г. № 554[1].

III. Требования к кадровому обеспечению

10. Руководитель, заместитель руководителя и работники центра ГосСОПКА должны иметь гражданство Российской Федерации, не имея гражданства другого государства.

11. Руководитель центра ГосСОПКА и его заместитель должны соответствовать одному из следующих требований:

иметь высшее образование (специалитет или магистратура) в области информационной безопасности, стаж работы в сфере информационной безопасности или информационных технологий не менее 5 лет и не менее 3 лет опыта работы на руководящих должностях в данных сферах;

иметь высшее образование (специалитет или магистратура), пройти профессиональную переподготовку в области информационной безопасности (срок – не менее 360 часов)[2], стаж работы в сфере информационной безопасности или информационных технологий не менее 5 лет и не менее 3 лет опыта работы на руководящих должностях в данных сферах.

12. Руководитель центра ГосСОПКА и его заместитель должны иметь допуск к работе со сведениями, составляющими государственную тайну.

---

[1] Зарегистрирован Минюстом России 30 декабря 2025 г., регистрационный № 84874.

[2] Пункт 17 Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности, утвержденного приказом Минобрнауки России от 19 октября 2020 г. № 1316 (зарегистрирован Минюстом России 2 ноября 2020 г., регистрационный № 60696) с изменениями, внесенными приказом Минобрнауки России от 4 сентября 2024 г. № 579 (зарегистрирован Минюстом России 20 сентября 2024 г., регистрационный № 79533) (далее – Порядок № 1316). В соответствии с пунктом 2 приказа Минобрнауки России от 19 октября 2020 г. № 1316 данный акт действует до 1 января 2027 г.

13. Допускается совмещать должность заместителя руководителя центра ГосСОПКА с должностью начальника одного из его подразделений. Совмещение других должностей в центре ГосСОПКА не допускается.

14. Начальник подразделения по обнаружению компьютерных атак и регистрации компьютерных инцидентов должен соответствовать одному из следующих требований:

иметь высшее образование в области информационной безопасности и стаж работы по данному направлению деятельности не менее 2 лет;

иметь высшее образование, пройти профессиональную переподготовку в области информационной безопасности (срок – не менее 360 часов)[1] и стаж работы по данному направлению деятельности не менее 2 лет.

15. Сотрудники подразделения по обнаружению компьютерных атак и регистрации компьютерных инцидентов должны соответствовать одному из следующих требований:

иметь высшее или среднее профессиональное образование в области информационной безопасности;

иметь высшее образование, пройти профессиональную переподготовку в области информационной безопасности (срок – не менее 360 часов)[1];

иметь высшее или среднее профессиональное образование в области математики и механики, или информатики и вычислительной техники, или компьютерных и информационных наук и стаж работы в области информационной безопасности не менее одного года.

16. В подразделении по обнаружению компьютерных атак и регистрации компьютерных инцидентов должно быть не менее одного начальника подразделения и 5 сотрудников.

17. Для работы в подразделении по обнаружению компьютерных атак и регистрации компьютерных инцидентов допускается принимать на работу работников без опыта, имеющих образование в области математики и механики, или информатики и вычислительной техники, или компьютерных

---

[1] Пункт 17 Порядка № 1316.

и информационных наук, или студентов образовательных организаций высшего образования на последнем году обучения, проходящих обучение по направлению информационной безопасности, из расчета не более одного работника без опыта или студента на 3 сотрудников подразделения.

18. Начальники подразделений по реагированию на компьютерные инциденты и ликвидации их последствий, предупреждению компьютерных атак на информационные ресурсы и координации подразделений субъектов ГосСОПКА должны соответствовать одному из следующих требований:

иметь высшее образование в области информационной безопасности и стаж работы по данному направлению деятельности не менее 3 лет;

иметь высшее образование, пройти профессиональную переподготовку в области информационной безопасности (срок – не менее 360 часов)[1] и стаж работы по данному направлению деятельности не менее 3 лет.

19. Сотрудники подразделений по реагированию на компьютерные инциденты и ликвидации их последствий, предупреждению компьютерных атак на информационные ресурсы и координации подразделений субъектов ГосСОПКА должны соответствовать одному из следующих требований:

иметь высшее образование в области информационной безопасности;

иметь высшее образование, пройти профессиональную переподготовку в области информационной безопасности (срок – не менее 360 часов)[1];

иметь высшее образование в области математики и механики, или информатики и вычислительной техники, или компьютерных и информационных наук и стаж работы в области информационной безопасности не менее одного года.

20. В подразделениях по реагированию на компьютерные инциденты и ликвидации их последствий, предупреждению компьютерных атак на информационные ресурсы и координации подразделений субъектов ГосСОПКА должно быть не менее одного начальника подразделения и 2 сотрудников.

---

[1] Пункт 17 Порядка № 1316.

21. Центр ГосСОПКА должен обеспечить наличие в штате работников, владеющих знаниями нормативных правовых актов Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА, национальных стандартов, международных стандартов и методических документов НКЦКИ[1] в части, касающейся обеспечения информационной безопасности и ОКА и РКИ, а также навыками ОКА и РКИ в соответствии с методическими документами НКЦКИ[1].

22. Работники центра ГосСОПКА должны проходить повышение квалификации не реже одного раза в 3 года (срок – не менее 40 часов)[2].

IV. Требования к аккредитованным центрам ГосСОПКА

23. Аккредитованный центр ГосСОПКА обязан обеспечивать:

а) выполнение функций в соответствии с направлением (направлениями) деятельности, указанным (указанными) в аттестате аккредитации центра ГосСОПКА, и методическими документами НКЦКИ[1];

б) взаимодействие с НКЦКИ по вопросам ОКА и РКИ посредством использования технической инфраструктуры НКЦКИ, в том числе направление в НКЦКИ информации о компьютерных инцидентах в срок не позднее 3 часов с момента обнаружения компьютерного инцидента, связанного с функционированием значимого объекта критической информационной инфраструктуры Российской Федерации[3], и не позднее

---

[1] Подпункт 4.3 пункта 4 Положения № 366.

[2] Пункт 17 Порядка № 1316.

[3] Статья 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

24 часов с момента обнаружения компьютерного инцидента, связанного с функционированием иных информационных ресурсов, в отношении которых центр ГосСОПКА обеспечивает обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты (далее – зона ответственности);

в) при осуществлении направления деятельности по обнаружению компьютерных атак и регистрации компьютерных инцидентов на информационные ресурсы или реагированию на компьютерные инциденты и ликвидации их последствий круглосуточный режим работы;

г) при проведении мероприятий по оценке защищенности информационных ресурсов, находящихся в зоне ответственности аккредитованного центра ГосСОПКА, от компьютерных атак, в том числе методом тестирования на проникновение, предварительное уведомление об этом НКЦКИ не позднее чем за 5 календарных дней до планируемого дня их проведения, а также направление в адрес НКЦКИ результатов указанных мероприятий. В случае если решение о проведении указанных мероприятий принимается менее чем за 5 календарных дней до планируемого дня их проведения допускается информировать НКЦКИ в день проведения таких мероприятий;

д) при осуществлении направления деятельности по реагированию на компьютерные инциденты и ликвидации их последствий направление в НКЦКИ в срок не позднее 3 календарных дней со дня начала проведения таких мероприятий промежуточных отчетов о проводимых мероприятиях, а также не позднее 5 календарных дней со дня завершения таких мероприятий – итоговых отчетов о результатах реагирования на компьютерные инциденты и ликвидации их последствий;

е) передачу в НКЦКИ сведений об оказании третьим лицам услуг по выявлению признаков компьютерных атак, мониторингу информационной безопасности, анализу событий информационной безопасности, выявлению уязвимостей в программном обеспечении, анализу сведений об угрозах

информационной безопасности, восстановлению работоспособности информационных ресурсов (в случае ее нарушения), фиксации следов вредоносного воздействия компьютерной атаки, установлению причин возникновения компьютерных инцидентов и устранению их последствий, проведению оценки защищенности информационных ресурсов, в том числе методом тестирования на проникновение, организации и проведению учений и тренировок (в том числе с использованием учебно-тренировочных центров) в течение 5 календарных дней со дня возникновения основания об оказании таких услуг, а по запросу НКЦКИ представление результатов проводимых мероприятий.

Указанные сведения должны содержать полное (сокращенное (при наличии) наименование юридического лица или фамилию, имя, отчество (при наличии) индивидуального предпринимателя, которому оказывались указанные услуги, индивидуальный номер налогоплательщика (ИНН), код причины постановки на учет (КПП), дату оказания услуг);

ж) представление в НКЦКИ сведений о состоянии защищенности, а также о выявляемых компьютерных атаках и компьютерных инцидентах в информационных ресурсах, находящихся в зоне ответственности центра ГосСОПКА, не реже одного раза в квартал;

з) направление в адрес владельцев информационных ресурсов, находящихся в зоне ответственности центра ГосСОПКА, информации, получаемой от НКЦКИ, для информирования владельцев информационных ресурсов, а также рекомендаций по устранению угроз информационной безопасности;

и) выполнение информационных заданий НКЦКИ, связанных с мероприятиями по ОКА и РКИ, а также предписаний об устранении нарушений, выявляемых ФСБ России в ходе контроля деятельности аккредитованных центров ГосСОПКА[1];

---

[1] Подпункт «г» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

к) проведение по уведомлению силами НКЦКИ мероприятий по оценке защищенности информационных ресурсов центра ГосСОПКА от компьютерных атак, в том числе методом тестирования на проникновение, своих информационных ресурсов. В случае выявления недостатков в обеспечении информационной безопасности информационных ресурсов центра ГосСОПКА или защите обрабатываемой в них информации центр ГосСОПКА в 6-месячный срок со дня завершения указанных мероприятий должен устранить выявленные недостатки либо реализовать компенсирующие меры, позволяющие минимизировать вызванные этими недостатками угрозы информационной безопасности. Об окончании указанных работ центр ГосСОПКА должен проинформировать НКЦКИ;

л) бесперебойную работу своих информационных ресурсов, задействованных в выполнении функций центра ГосСОПКА, а также их информационную безопасность и защиту обрабатываемой в них информации в соответствии с требованиями, приведенными в приложении № 1 к настоящим Требованиям;

м) хранение информации о компьютерных инцидентах и связанных с ними событиях (электронные журналы, инвентаризационная информация, сведения о выявленных уязвимостях, сетевой трафик) не менее 3 лет со дня их обнаружения;

н) необходимое минимально достаточное количество работников в соответствии с главой III настоящих Требований;

о) информирование органов (организаций), в отношении которых аккредитованный центр ГосСОПКА выполняет свои функции, в случае приостановления или отзыва аккредитации центра ГосСОПКА.

24. Включение информационных ресурсов в зону ответственности аккредитованного центра ГосСОПКА и исключение из нее должно осуществляться с уведомлением об этом НКЦКИ.

25. Уведомление НКЦКИ о включении (об исключении) информационных ресурсов в зону (из зоны) ответственности аккредитованного центра ГосСОПКА должно осуществляться в течение 24 часов с момента возникновения (прекращения) основания, в соответствии с которым информационные ресурсы включаются в зону ответственности (исключаются из зоны ответственности) аккредитованного центра ГосСОПКА.

26. Центр ГосСОПКА должен ежегодно проводить оценку защищенности своих информационных ресурсов от компьютерных атак (в соответствии с методическими документами НКЦКИ[1]) силами другого центра ГосСОПКА, аккредитованного по направлению деятельности «предупреждение компьютерных атак на информационные ресурсы», с представлением отчетности в НКЦКИ. В случае выявления недостатков в обеспечении информационной безопасности центр ГосСОПКА, в отношении информационных ресурсов которого проводились указанные мероприятия, в 6-месячный срок со дня их завершения должен устранить выявленные недостатки либо реализовать компенсирующие меры, позволяющие минимизировать вызванные этими недостатками угрозы информационной безопасности, и проинформировать об этом НКЦКИ.

27. В случае если при увольнении работников центра ГосСОПКА их количество не соответствует количеству, установленному главой III настоящих Требований, то руководитель центра ГосСОПКА обязан проинформировать об этом Центр защиты информации и специальной связи ФСБ России в срок, не превышающий 10 календарных дней со дня наступления такого события, и в течение 3 месяцев со дня наступления такого события устранить несоответствие с уведомлением Центра защиты информации и специальной связи ФСБ России.

---

[1] Подпункт 4.3 пункта 4 Положения № 366.

28. При выявлении ошибок в работе средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, центр ГосСОПКА должен уведомить об этом производителя этих средств в срок не позднее 5 календарных дней со дня выявления таких ошибок, включив в данное уведомление предложения по совершенствованию этих средств (при наличии). Копию указанного уведомления центр ГосСОПКА должен направить в НКЦКИ.

29. Руководителю, заместителю руководителя и работникам центра ГосСОПКА запрещается:

исполнять свои должностные обязанности, в том числе посредством удаленного доступа, из-за пределов территории Российской Федерации, дипломатических представительств и (или) консульских учреждений Российской Федерации, за исключением случаев выполнения мероприятий по реагированию на компьютерные инциденты или оценке защищенности информационных ресурсов от компьютерных атак, в том числе методом тестирования на проникновение, проводимых в отношении информационных ресурсов Российской Федерации, расположенных за пределами территории Российской Федерации;

передавать информацию о компьютерных атаках и компьютерных инцидентах, а также выявленных уязвимостях информационных ресурсов и об угрозах информационной безопасности сторонним органам (организациям) и физическим лицам (за исключением случаев уведомления производителей программного обеспечения об уязвимостях в их продуктах);

не представлять в НКЦКИ и (или) искажать направляемую в НКЦКИ информацию о компьютерных атаках, компьютерных инцидентах, результатах их последствий, результатах проведения мероприятий по оценке защищенности информационных ресурсов от компьютерных атак, в том числе методом тестирования на проникновение, включая сведения о выявленных

уязвимостях информационных ресурсов и об угрозах информационной безопасности;

препятствовать выполнению сотрудниками ФСБ России контрольных мероприятий[1].

30. Центру ГосСОПКА запрещается осуществлять деятельность по направлению (направлениям), по которому (которым) он не аккредитован.

[1] Подпункт «г» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Приложение № 1
к Требованиям к центрам
государственной системы
обнаружения, предупреждения
и ликвидации последствий
компьютерных атак
на информационные ресурсы
Российской Федерации, а также
к аккредитованным центрам
(пункты 3 и 23)

Требования по обеспечению информационной безопасности информационных ресурсов центров ГосСОПКА и защите обрабатываемой в них информации

1. В информационных ресурсах центра ГосСОПКА должны обеспечиваться:

сохранность и неизменность обрабатываемой информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения (далее – целостность информации);

защита информации от действий пользователей, приводящих в том числе к уничтожению, модификации и блокированию информации (далее – неправомерные действия).

2. Обеспечение информационной безопасности информационных ресурсов центра ГосСОПКА и защиты обрабатываемой в них информации должно осуществляться силами центра ГосСОПКА.

3. Объектами защиты информационных ресурсов центра ГосСОПКА должны являться программно-аппаратные средства (в том числе автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи), программные средства (общесистемное и прикладное программное обеспечение), системы управления базами данных, машинные носители информации, средства защиты информации, конфигурация информационных систем и информационно-телекоммуникационных сетей.

4. Защита информации, содержащейся в информационных ресурсах центра ГосСОПКА, должна осуществляться посредством применения совокупности организационных и технических мер, направленных на обеспечение целостности указанной информации и исключение в отношении нее неправомерных действий.

5. Принимаемые организационные и технические меры по обеспечению информационной безопасности информационных ресурсов центра ГосСОПКА и защиты обрабатываемой в них информации не должны приводить к нарушению функционирования информационных ресурсов, входящих в зону ответственности центра ГосСОПКА.

6. Методы и способы обеспечения информационной безопасности информационных ресурсов центра ГосСОПКА и защиты обрабатываемой в них информации должны определяться руководством центра ГосСОПКА и соответствовать настоящим требованиям.

7. Достаточность принимаемых мер, направленных на обеспечение информационной безопасности информационных ресурсов центра ГосСОПКА и защиты обрабатываемой в них информации, должна оцениваться центром ГосСОПКА при проведении мероприятий по их разработке, внедрению и контролю за их выполнением.

8. При организации размещения информационных ресурсов центра ГосСОПКА должны обеспечиваться их сохранность, включая сохранность машинных носителей информации и средств защиты информации, а также исключаться возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. В информационных ресурсах центра ГосСОПКА должны быть обеспечены:

поддержание целостности и доступности информации;

проведение мероприятий, направленных на предотвращение неправомерных действий в отношении информации, предупреждение

наступления негативных последствий в результате нарушения порядка доступа к информации, а также обнаружение фактов неправомерных действий в отношении информации;

недопущение воздействия на информационные ресурсы центра ГосСОПКА, в результате которого может быть нарушено его функционирование;

возможность восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий;

проведение мероприятий по постоянному контролю за обеспечением их защищенности.

10. Организация информационной безопасности информационных ресурсов центра ГосСОПКА должна включать разработку и внедрение механизмов обеспечения информационной безопасности центра ГосСОПКА, а также обеспечение информационной безопасности информационных ресурсов центра ГосСОПКА в ходе их эксплуатации.

11. Разработка механизмов обеспечения информационной безопасности центра ГосСОПКА должна включать:

анализ угроз информационной безопасности;

проектирование информационной безопасности центра ГосСОПКА, в том числе по результатам анализа угроз информационной безопасности;

разработку документации по обеспечению информационной безопасности.

12. Внедрение механизмов обеспечения информационной безопасности центра ГосСОПКА должно включать:

принятие организационных мер по обеспечению информационной безопасности;

установку и настройку средств защиты информации в соответствии с эксплуатационной и технической документацией;

проверку эффективности информационной безопасности центра ГосСОПКА и устранение недостатков.

13. Обеспечение информационной безопасности информационных ресурсов центра ГосСОПКА должно включать:

определение лиц, ответственных за обеспечение информационной безопасности информационных ресурсов центра ГосСОПКА;

управление информационной безопасностью центра ГосСОПКА, конфигурацией и обновлениями средств защиты информации и других программно-аппаратных и программных средств, задействованных в обеспечении информационной безопасности центра ГосСОПКА;

резервирование информации, обрабатываемой в информационных ресурсах, задействованных в обеспечении информационной безопасности центра ГосСОПКА;

контроль за обеспечением информационной безопасности информационных ресурсов центра ГосСОПКА и соблюдением условий по использованию средств защиты информации и других программно-аппаратных и программных средств, задействованных в обеспечении информационной безопасности центра ГосСОПКА;

анализ изменения угроз информационной безопасности и уязвимостей информационных ресурсов, возникающих в ходе их эксплуатации, и принятие мер по их устранению;

выявление фактов несоблюдения условий использования средств защиты информации и других программно-аппаратных и программных средств, задействованных в обеспечении информационной безопасности центра ГосСОПКА, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационных ресурсов центра ГосСОПКА, а также разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений.

14. Контроль доступа пользователей к информационным ресурсам центра ГосСОПКА должен осуществляться с использованием автоматизированных средств регистрации в электронном журнале. Содержание электронного журнала должно проверяться работниками, ответственными за обеспечение

информационной безопасности центра ГосСОПКА, не реже одного раза в месяц.

15. При обнаружении нарушений порядка доступа к информации руководитель центра ГосСОПКА обязан организовать работу по выявлению причин нарушений и устранению этих причин. Посредством использования механизмов обеспечения информационной безопасности должно обеспечиваться восстановление информации в срок до 8 часов.

16. При обеспечении информационной безопасности информационных ресурсов должны использоваться:

средства антивирусной защиты, сертифицированные ФСБ России[1];

средства обнаружения компьютерных атак, сертифицированные ФСБ России[1];

средства фильтрации и блокирования сетевого трафика, в том числе средства межсетевого экранирования, сертифицированные ФСБ России[1];

средства криптографической защиты информации (электронной подписи, при этом средства электронной подписи обязательно должны применяться к публикуемому информационному наполнению), сертифицированные ФСБ России[1];

средства регистрации действий пользователей информационных ресурсов центра ГосСОПКА;

средства резервирования технических и программных средств, дублирования носителей и массивов информации;

сертифицированные системы обеспечения гарантированного электропитания (источников бесперебойного питания).

---

[1] Подпункт 5.4 пункта 5 приложения 1 к Положению о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ – ГТ), утвержденному приказом ФСБ России от 13 ноября 1999 г. № 564 (зарегистрирован Минюстом России 27 декабря 1999 г., регистрационный № 2028).

Приложение № 2
к Требованиям к центрам
государственной системы
обнаружения, предупреждения
и ликвидации последствий
компьютерных атак
на информационные ресурсы
Российской Федерации, а также
к аккредитованным центрам (пункт 5)

Соответствие функций, выполняемых центром государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, направлению осуществляемой им деятельности

Функции центра ГосСОПКА	Направления деятельности центра ГосСОПКА			
	Обнаружение компьютерных атак и регистрация компьютерных инцидентов	Реагирование на компьютерные инциденты и ликвидация их последствий	Предупреждение компьютерных атак на информационные ресурсы	Координация деятельности подразделений субъектов ГосСОПКА
1	2	3	4	5
Непрерывное автоматизированное взаимодействие с НКЦКИ	+	+	+	+
Инвентаризация информационных ресурсов	+	+	+	+
Оценка защищенности информационных ресурсов от компьютерных атак	–	–	+	–
Выявление уязвимостей информационных ресурсов	–	+	+	–

1	2	3	4	5
Анализ угроз информационной безопасности	–	+	+	+
Прием сообщений о признаках компьютерных инцидентов от персонала и пользователей информационных ресурсов	+	+	–	–
Анализ событий информационной безопасности	+	+	–	–
Регистрация компьютерных инцидентов	+	+	–	–
Реагирование на компьютерные инциденты	–	+	–	–
Ликвидация последствий компьютерных инцидентов	–	+	–	–
Установление причин возникновения компьютерных инцидентов	–	+	–	–
Анализ результатов ликвидации последствий компьютерных инцидентов	–	+	–	+
Формирование предложений по повышению уровня защищенности информационных ресурсов	+	+	+	+
Выполнение информационных заданий, поступающих от НКЦКИ, в части отработки сценариев действий по реагированию на компьютерные инциденты, а также своевременное представление в НКЦКИ запрашиваемой информации и материалов в части деятельности по ОКА и РКИ	+	+	+	+

Приложение № 3
к Требованиям к центрам
государственной системы
обнаружения, предупреждения
и ликвидации последствий
компьютерных атак
на информационные ресурсы
Российской Федерации, а также
к аккредитованным центрам
(пункт 8)

Требования к технической оснащенности центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Средства, необходимые центру ГосСОПКА для осуществления своей деятельности	Направления деятельности центра ГосСОПКА			
	Обнаружение компьютерных атак и регистрация компьютерных инцидентов	Реагирование на компьютерные инциденты и ликвидация их последствий	Предупреждение компьютерных атак на информационные ресурсы	Координация деятельности подразделений субъектов ГосСОПКА
1	2	3	4	5
Средство обмена информацией, предназначенное для непрерывного автоматизированного взаимодействия с НКЦКИ	+	+	+	+
Система управления событиями информационной безопасности	+	+	–	–
Платформа реагирования на компьютерные инциденты	+	+	–	+
Платформа анализа информации киберразведки	+	+	–	+

1	2	3	4	5
Система выявления и реагирования на инциденты на конечных устройствах пользователей или решение, выполняющее аналогичные функции	–	+	–	–
Средство динамического анализа загружаемых файлов	+	+	–	–
Сканер уязвимостей	–	+	+	–
Система автоматизированного анализа сетевого трафика либо системы, выполняющие аналогичные функции	+	+	+	–
Средство антивирусной защиты	–	+	–	–