САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ**

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
**РЕГИОНАЛЬНАЯ ИНФОРМАТИКА**

## Сборник трудов

# РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## Выпуск 11

Санкт-Петербург
2022

УДК (002:681):338.98

Р32

**Региональная информатика и информационная безопасность.**

**Р32** Сборник трудов. Выпуск 11 / СПОИСУ. – СПб., 2022. – 645 с.

ISBN 978-5-00182-048-2

В сборник включены статьи участников Санкт-Петербургской международной конференции «Региональная информатика» и Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», проведенных при поддержке Правительства Санкт-Петербурга, объединенных в рубрики: Государственная политика в сфере информатизации и информационной безопасности; Теоретические проблемы информатики и информатизации; Телекоммуникационные сети и технологии; Информационная безопасность; Правовые аспекты информатизации и информационной безопасности; Информационно-психологическая безопасность; Информационные технологии на транспорте; Информационные технологии в образовании, Информационные технологии в медицине и здравоохранении; Информационные технологии в экологии; Информационные технологии управления объектами морской техники и морской инфраструктуры, Информационные технологии в дизайне, печати и медиаиндустрии; Информационные технологии в социокомпьютинге; Информационные технологии в критических инфраструктурах; Молодежная научная школа «интеллектуальные безопасные информационные системы и технологии».

Сборник статей предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений, специализирующихся в вопросах информатизации, связи, информационной безопасности и защиты информации.

**УДК (002:681):338.98**

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

ISBN 978-5-00182-048-2

Публикуется в авторской редакции

Подписано в печать 30.11.2022. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 74,5. Тираж 400 экз. Заказ № 17956
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-048-2


ST. PETERSBURG INTERREGIONAL CONFERENCE
**INFORMATION SECURITY OF RUSSIAN REGIONS**

ST. PETERSBURG INTERNATONAL CONFERENCE
**REGIONAL INFORMATICS**

## Proceedings

# REGIONAL INFORMATICS AND INFORMATION SECURITY

## The Issue No 11

**St. Petersburg**
**2022**

УДК 004.056

# ОРГАНИЗАЦИЯ ГОСУДАРСТВЕННОГО КОНТРОЛЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Сторожик Виктор Сергеевич**
Арктический и антарктический научно-исследовательский институт
Беринга, ул., 38, Санкт-Петербург, 199397, Россия
e-mail: vstorozhik@yandex.ru

**Аннотация.** Рассматриваются особенности реализации требований нормативных правовых актов, определяющих организацию государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

**Ключевые слова:** автоматизированная система управления; безопасность; государственный контроль; значимый объект; информационная система; критическая информационная инфраструктура; проверка; субъект; угроза безопасности информации; уязвимость; эффективность.

# ORGANIZATION OF STATE CONTROL IN THE FIELD OF SECURITY OF SIGNIFICANT OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

**Storozhik Viktor**
Arctic and Antarctic Research Institute
38 Bering St, St. Petersburg, 199397, Russia
e-mail: vstorozhik@yandex.ru

**Abstract.** The features of the implementation of the requirements of regulatory legal acts defining the organization of state control in the field of ensuring the security of significant objects of critical information infrastructure of the Russian Federation are considered.

**Keywords:** automated control system; security; state control; significant object; information system; critical information infrastructure; verification; subject; threat to information security; vulnerability; efficiency.

Введение. В Доктрине информационной безопасности Российской Федерации к основным национальным интересам в информационной сфере отнесено обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры (КИИ) в условиях проведения компьютерных атак [1].

В Стратегии национальной безопасности Российской Федерации указано, что использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российский информационных ресурсов, включая объекты КИИ, к воздействию из-за рубежа, а также поставлена задача повышения защищенности и устойчивости функционирования информационной инфраструктуры [2].

В докладе Президента Российской Федерации 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» указано: «Количество кибератак на российскую информационную инфраструктуру все последние годы постоянно растет... По сути, против России развязана настоящая агрессия, война в информационном пространстве.» [3].

В рамках реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4] Постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162 утверждены Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ [5].

Значимыми объектами КИИ являются объекты, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов КИИ, [4, 6, 7, 8, 9].

Мероприятия по государственному контролю в области обеспечения безопасности значимых объектов КИИ проводятся Федеральной службой по техническому и экспортному контролю (ФСТЭК России) и её территориальными органами в целях проверки соблюдения требований по обеспечению безопасности субъектами КИИ, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ.

Задачами государственного контроля в области обеспечения безопасности значимых объектов КИИ являются:

1. Оценка организации обеспечения безопасности значимых объектов КИИ и состояния систем их безопасности.

2. Оценка организации и проведения работ субъектами КИИ по обеспечению безопасности принадлежащих им значимых объектов КИИ в ходе их создания и эксплуатации.

3. Оценка эффективности принимаемых мер по обеспечению безопасности значимых объектов КИИ, принадлежащих субъектам КИИ.

4. Осуществление методического руководства по отдельным направлениям деятельности субъектов КИИ при обеспечении безопасности принадлежащих им значимых объектов КИИ.

Полномочия по осуществлению государственного контроля в области обеспечения безопасности значимых объектов КИИ распределяются следующим образом:

– ФСТЭК России контролирует субъекты КИИ федеральных органов исполнительной власти и подведомственных им учреждений, государственных корпораций и управляющих компаний интегрированных структур;

– территориальные органы ФСТЭК России контролируют субъекты КИИ органов власти субъектов Российской Федерации и подведомственных им учреждений, компаний, входящих в интегрированные структуры и самостоятельные субъекты КИИ, не имеющие ведомственной подчиненности, в том числе индивидуальных предпринимателей.

Государственный контроль в области обеспечения безопасности значимых объектов КИИ осуществляется путем проведения плановых и внеплановых выездных проверок. Плановая (внеплановая) проверка проводится по месту нахождения субъекта КИИ, лица, эксплуатирующего значимый объект КИИ, и значимого объекта КИИ.

Особое внимание при проведении выездной проверки обращается на соблюдение:

1. Требований частей 2 и 3 статьи 9, статей 10 и 11 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4];

2. Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденных постановлением Правительства Российской Федерации от 8 июня 2019 г. № 743 [10];

3. Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (в части требований к комиссии по категорированию, рассмотрения всех подлежащих категорированию объектов КИИ (в том числе создаваемых), актов категорирования, соблюдения сроков категорирования и представления необходимых сведений в ФСТЭК России, пересмотра категории значимости объектов КИИ) [8];

4. Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденных приказом ФСТЭК России от 21 декабря 2017 г. № 235 [11, 12];

5. Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239 [13, 14];

6. Пунктов 6 - 10 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденного приказом ФСБ России от 19 июня 2019 г. № 282 [15].

Основаниями для осуществления плановой выездной проверки являются истечение трех лет со дня:

а) внесения сведений об объекте КИИ в реестр значимых объектов КИИ;

б) окончания осуществления последней плановой проверки в отношении значимого объекта КИИ.

Ежегодный план проведения плановых проверок утверждается директором ФСТЭК России до 20 декабря года, предшествующего году проведения плановых проверок.

Выписки из утвержденного ежегодного плана проведения плановых проверок направляются субъектам КИИ территориальными органами ФСТЭК России до 1 января года проведения плановых проверок.

О проведении плановой проверки субъект КИИ уведомляется органом государственного контроля не менее чем за три рабочих дня до начала ее проведения посредством направления копии приказа органа государственного контроля о проведении плановой проверки любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

Плановая выездная проверка проводится на основании утвержденного ежегодного плана проведения плановых проверок и приказа органа государственного контроля о проведении проверки.

Основаниями для осуществления внеплановой проверки являются:

а) истечение срока выполнения субъектом КИИ выданного органом государственного контроля предписания об устранении выявленного нарушения требований по обеспечению безопасности;

б) возникновение компьютерного инцидента на значимом объекте КИИ, повлекшего негативные последствия;

в) приказ 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.

Предметом внеплановой выездной проверки является соблюдение субъектом КИИ требований по обеспечению безопасности, выполнение предписания органа государственного контроля, а также проведение мероприятий по предотвращению негативных последствий на значимом объекте КИИ, причиной которых является возникновение компьютерного инцидента.

О проведении внеплановой выездной проверки субъект КИИ уведомляется органом государственного контроля не менее чем за 24 часа до начала её проведения, за исключением случая возникновения компьютерного инцидента на значимом объекте КИИ, повлекшего негативные последствия, когда органу государственного контроля предоставлено право приступить к проведению внеплановой проверки незамедлительно.

Проверка проводится должностными лицами ФСТЭК России и/или её территориальных органов, которые указаны в приказе о проведении проверки. Состав комиссии при проведении плановой (внеплановой) проверки включает не менее 2 должностных лиц. Допускается проведение внеплановой проверки одним должностным лицом в случае, если её основанием является истечение срока выполнения субъектом КИИ выданного органом государственного контроля предписания об устранении выявленного нарушения.

Срок проведения плановой выездной проверки не должен превышать 20 рабочих дней, а внеплановой - более 10 рабочих дней. Общий срок выездной проверки в отношении одного субъекта КИИ, расположенного на территориях нескольких субъектов Российской Федерации, не должен превышать 60 рабочих дней.

В процессе проведения выездной проверки члены комиссии осуществляют:

1. Визуальный осмотр технических средств объектов КИИ субъекта КИИ;
2. Анализ схем вычислительных сетей субъекта КИИ;
3. Оценку выполнения требований к силам обеспечения безопасности значимых объектов КИИ субъекта КИИ;
4. Оценку выполнения требований к организационно-распорядительным документам субъекта КИИ по обеспечению безопасности принадлежащих им значимых объектов КИИ;
5. Проверку выполнения требований к функционированию системы обеспечения безопасности значимых объектов КИИ;
6. Проверку выполнения требований к функционированию значимых объектов КИИ;
7. Проверку корректности реализации организационных и технических мер по обеспечению безопасности значимых объектов КИИ;
8. Проверку выполнения требований к созданию и модернизации значимых объектов КИИ (в случае наличия создаваемых и (или) модернизируемых значимых объектов КИИ);
9. Проверку выполнения требований к выводу из эксплуатации значимых объектов КИИ (в случае наличия выведенных и (или) выводимых из эксплуатации значимых объектов КИИ);
10. Проведение контрольных мероприятий для оценки эффективности принимаемых мер во исполнение требований по обеспечению безопасности с использованием сертифицированных по требованиям безопасности информации программных и аппаратно-программных средств контроля, в том числе имеющихся у субъекта КИИ. Возможность и порядок использования таких средств контроля с учетом особенностей функционирования значимого объекта КИИ согласовывается с руководителем субъекта КИИ или уполномоченным им должностным лицом.

Руководитель субъекта КИИ (уполномоченное им должностное лицо) обязан присутствовать при проведении мероприятий проверки и давать пояснения комиссии по вопросам проверки, предоставить комиссии возможность ознакомиться с документами, связанными с предметом и задачами проверки, а также обеспечить с учетом требований пропускного режима беспрепятственный доступ комиссии на территорию, в используемые здания, сооружения, помещения и к значимым объектам КИИ, в первый день проверки провести инструктаж комиссии по соблюдению техники безопасности на объектах КИИ, а также устранять выявленные комиссией нарушения.

При проверке корректности реализации организационных и технических мер по обеспечению безопасности значимых объектов КИИ должностными лицами органа государственного контроля оцениваются как принципы реализации мер (полнота и достаточность, гибкость, минимизация влияния мер на обеспечиваемый процесс, планирование реализации мер, реализация «бесплатных» мер, не требующих материальных затрат, регламентация мер), так и способы реализации мер (с использованием организационных решений и режимных мероприятий, с организацией физической защиты, при помощи архитектурных и технических решений, с использованием встроенных и наложенных средств защиты информации).

Члены комиссии ФСТЭК России не вправе:

1. Проверять выполнение тех требований по обеспечению безопасности информации, которые не относятся к полномочиям ФСТЭК России;
2. Проводить проверку в случае отсутствия при ее проведении руководителя субъекта КИИ или уполномоченного им должностного лица (за исключением внеплановой проверки значимого объекта КИИ из-за компьютерного инцидента, повлекшего негативные последствия);
3. Требовать представления от руководителя субъекта КИИ (уполномоченного им должностного лица) документов и информации, которые не относятся к предмету выездной проверки, а также изымать оригиналы таких документов;
4. Распространять информацию (охраняемую законом тайну), полученную в результате проведения проверки (за исключением случаев, предусмотренных законодательством Российской Федерации);
5. Превышать установленные приказом сроки проведения выездной проверки;
6. Осуществлять выдачу субъектам КИИ предписаний или предложений о проведении за их счет мероприятий по контролю.
7. Осуществлять действия с техническими средствами обработки информации, в результате которых может быть нарушено и (или) прекращено функционирование значимого объекта КИИ.

По результатам проверки составляется акт проверки по форме, утвержденной приказом ФСТЭК России от 11 декабря 2017 г. № 229 [16]. К акту проверки прилагаются протоколы по результатам контрольных мероприятий, предписания субъекту КИИ об устранении выявленных нарушений (в случае выявления нарушений требований по обеспечению безопасности информации) с указанием сроков их устранения и иные связанные с результатами проверки документы или их копии. Акт проверки оформляется в 3-х экземплярах, один из которых с приложениями вручается руководителю субъекта КИИ или уполномоченному им должностному лицу. Акт проверки, содержащий сведения,

составляющие государственную и иную охраняемую законом тайну, должен быть оформлен с соблюдением требований законодательства Российской Федерации [17-19]. В случае проведения внеплановой проверки на основании требования прокурора 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.

В случае выявления при проведении проверки нарушения требований по обеспечению безопасности комиссия выдает предписание субъекту КИИ об устранении выявленного нарушения требований по обеспечению безопасности с указанием срока его устранения, который устанавливается в том числе с учетом утвержденных и представленных субъектом КИИ программ (планов) по модернизации (дооснащению) значимого объекта КИИ.

В случае несогласия с фактами, изложенными в акте проверки и (или) предписании об устранении выявленного нарушения, руководитель субъекта КИИ (уполномоченное должностное лицо) вправе представить в течение 15 дней с даты получения акта проверки в 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 субъект КИИ вправе приложить к возражениям документы, подтверждающие обоснованность таких возражений, или их заверенные копии либо в согласованный срок передать их в орган государственного контроля.

Орган государственного контроля осуществляет контроль за устранением выявленного нарушения. По мотивированному обращению субъекта КИИ (в случае невозможности выполнения предписания по причинам, не зависящим от субъекта КИИ) орган государственного контроля вправе продлить срок выполнения предписания об устранении выявленного нарушения до одного года.

Заключение. Руководитель субъекта КИИ (уполномоченное им должностное лицо), допустившие нарушение положений Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ [5], 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, несут ответственность в соответствии с законодательством Российской Федерации [20-21].

## СПИСОК ЛИТЕРАТУРЫ


1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства».
4. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
6. Положение о Федеральной службе по техническому и экспортному контролю (утв. Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 «Вопросы Федеральной службе по техническому и экспортному контролю»).
7. Указ Президента Российской Федерации от 25 ноября 2017 г. № 569 «О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
9. Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».
10. Постановление Правительства Российской Федерации от 8 июня 2019г. № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры Российской Федерации».
11. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
12. Приказ ФСТЭК России от 27 марта 2019 г. № 64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235».
13. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60).
14. Приказ ФСТЭК России от 26 марта 2019 г. № 60 «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239».
15. Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятии мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».
16. Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
17. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне».
18. Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».
19. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. Указа Президента Российской Федерации от 13.07.2015 № 357).
20. Федеральный закон от 13.06.1996 № 63-ФЗ «Уголовный кодекс Российской Федерации» (ред. от 25.03.2022).
21. Федеральный закон от 30.12.2001 N 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (ред. от 16.04.2022, с изм. от 17.05.2022) (с изм. и доп., вступ. в силу с 27.04.2022).