XVIII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
«РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ-2022)»
САНКТ-ПЕТЕРБУРГ, 26-28 ОКТЯБРЯ 2022

# *Нормативно-правовое регулирование государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации*

**АРКТИЧЕСКИЙ И АНТАРКТИЧЕСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ**

*СТОРОЖИК Виктор Сергеевич*

*кандидат технических наук, доцент*

# Доктрина информационной безопасности Российской Федерации

***утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646***

Национальные интересы в информационной сфере:

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации.

Основные информационные угрозы и состояние информационной безопасности:

2. наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

7. постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры.

9. мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

# Доктрина информационной безопасности Российской Федерации

***утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646***

Защита критической информационной инфраструктуры является одной из стратегических целей обеспечения информационной безопасности в области государственной и общественной безопасности.

Основные направления обеспечения информационной безопасности в области государственной и общественной безопасности:

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории РФ

# СИСТЕМА НПА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИИ РФ

**Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»**

**Федеральный закон от 26 июля 2017 г. № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием …»**

**Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в уголовный кодекс Российской Федерации в связи с принятием …»**

## Нормативные правовые акты Президента Российской Федерации

- Указ Президента РФ от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004г. № 1085»
- Указ Президента РФ от 22 декабря 2017г. №620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий КА на информационные ресурсы РФ»
- Указ Президента РФ от 2 марта 2018г. №98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»
- Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ»
- Указ Президента РФ от 14 апреля 2022 г. № 203 «О Межведомственной комиссии Совета Безопасности РФ по вопросам обеспечения технологического суверенитета в сфере развития КИИ РФ»
- Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

## Нормативные правовые акты Правительства Российской Федерации

- Постановление Правительства РФ от 8 февраля 2018 г. №127 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
- Постановление Правительства РФ от 17 февраля 2018 г. №162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ»
- Постановление Правительства РФ от 11 июня 2018г. № 808 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК» »
- Постановление Правительства РФ от 8 июня 2019г. № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ»
- Постановление Правительства РФ от 15 июля 2022г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение ИБ в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем ИБ органа (организации)»
- Постановление Правительства РФ от 22 августа 2022 г. № 1478 «Об утверждении требований к ПО, правил согласования закупок иностранного ПО и услуг, необходимых для этого ПО, и Правил перехода на преимущественное использование российского ПО, в том числе в составе ПАК»

## Нормативные правовые акты федеральных органов исполнительной власти

- Приказ ФСТЭК России от 21 декабря 2017г.№ 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ»
- Приказ ФСТЭК России от 22 декабря 2017г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости»
- Приказ ФСТЭК России от 25 декабря 2017г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ»
- Приказ ФСТЭК России от 11 декабря 2017г. № 229 «Об утверждении формы акта проверки»
- Приказ ФСТЭК России от 6 декабря 2017г №227 «Об утверждении порядка ведения реестра значимых объектов КИИ»
- Приказ ФСТЭК России от 28 мая 2020 г. № 75 «Об утверждении Порядка согласования субъектом КИИ РФ … подключения ЗО КИИ РФ к сети связи общего пользования»

- Приказ ФСБ России от 24 июля 2018 г. № 366 «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам»
- Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»
- Приказ ФСБ России от 19 июня 2019 г. №282 «Об утверждении порядка информирования ФСБ России о КИ, реагирования на них, принятии мер по ликвидации последствий КА, проведенных в отношении ЗО КИИ РФ»
- Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении порядка, технических условий, установки и эксплуатации средств предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагировании на КИ …»
- Приказ ФСБ России от 24 июля 2018 г. № 368«Об утверждении порядка обмена информации о компьютерных инцидентах и порядка получения информации субъектами КИИ»
- Приказ Минцифры России от 17 марта 2020 г. N 114 «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ»
- Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении требований к средствам предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на КИ»

- ФСТЭК России
- ФСБ России
- Минцифры России

## 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»

# Требования, выполнение которых проверяется в ходе проведения проверки



Части 2, 3 статьи 9, статьи 10 - 11 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Правила подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденные постановлением Правительства Российской Федерации от 8 июня 2019 г. № 743

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (в части требований к комиссии, рассмотрения всех необходимых объектов, в том числе создаваемых, актов категорирования, соблюдения сроков категорирования и представления в ФСТЭК России необходимых сведений, пересмотра категории значимости объектов)

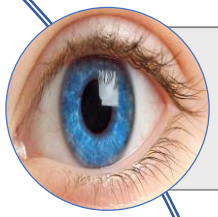
Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденных приказом ФСТЭК России от 21 декабря 2017 г. № 235

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239

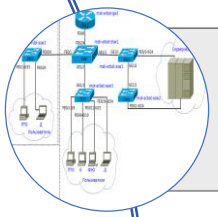
Пункты 6 - 10 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденного приказом ФСБ России от 19 июня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

# Проведение выездной проверки





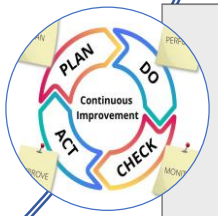
Визуальный осмотр технических средств объектов КИИ субъекта КИИ



Анализ схем вычислительных сетей субъекта КИИ

Оценка выполнения требований к силам обеспечения безопасности значимых объектов КИИ субъекта КИИ

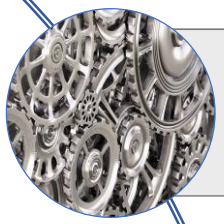
Оценка выполнения требований к ОРД субъекта КИИ по обеспечению безопасности значимых объектов КИИ субъекта КИИ



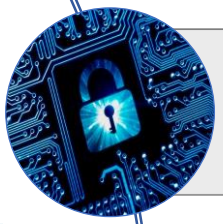

Проверка выполнения требований к функционированию системы обеспечения безопасности значимых объектов КИИ

# Проведение выездной проверки





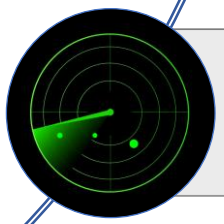
Проверка выполнения требований к функционированию значимых объектов КИИ



Проверка реализации организационных и технических мер по обеспечению безопасности значимых объектов КИИ

Проверка выполнения требований к созданию и модернизации значимых объектов КИИ (в случае наличия создаваемых и (или) модернизируемых значимых объектов КИИ)

Проверка выполнения требований к выводу из эксплуатации значимых объектов КИИ (в случае наличия выведенных и (или) выводимых из эксплуатации значимых объектов КИИ)



Проведение контрольных мероприятий с использованием средств контроля

# Общие положения

Состав комиссии: не менее 2 должностных лиц (плановая / внеплановая проверки).

Допускается проведение внеплановой проверки 1 должностным лицом *(основание: контроль выполнения предписания об устранении нарушения).*

Сроки проверок: не более 20 рабочих дней (плановая);
не более 10 рабочих дней (внеплановая).

Общий срок проверок в отношении одного субъекта КИИ, расположенного на территориях нескольких субъектов Российской Федерации, не может превышать 60 рабочих дней.

Информация об организации проверок, в том числе об их планировании, о проведении и результатах таких проверок, в органы прокуратуры *НЕ НАПРАВЛЯЕТСЯ*.

*Исключение: в органы прокуратуры направляются результаты внеплановых проверок, проведенных на основании требования прокурора в рамках проведения надзора за исполнением законов.*

# Организация плановой проверки

Предмет проверки: соблюдение субъектом КИИ требований по ОБИ.

Основание для осуществления плановой проверки — истечение 3 лет:

со дня внесения сведений об объекте КИИ в реестр значимых объектов КИИ;

со дня окончания последней плановой проверки значимого объекта КИИ.

План проведения плановых проверок на очередной год утверждается до 20.12.

Выписки из утвержденного ежегодного плана проведения плановых проверок направляются субъектам значимых объектов КИИ до 1.01.

Уведомление субъекта значимой КИИ проводится **не менее чем за 3 рабочих дня** до начала проведения плановой выездной проверки.

Содержание приказа о проведении проверки:

1. Наименование органа государственного контроля, номер и дата издания приказа.
2. Должности, ФИО должностных лиц, уполномоченных на проведение проверки.
3. Сведения о субъекте КИИ.
4. Сведения о лице, эксплуатирующем значимый объект КИИ.
5. Задачи проверки.
6. Дата начала и окончания проверки.
7. Срок проведения проверки.
8. Правовые основания проведения проверки.
9. Перечень мероприятий по контролю, необходимых для выполнения задач проверки.

# Организация внеплановой проверки

Предмет внеплановой проверки:

1. Соблюдение субъектом КИИ требований по ОБИ.
2. Выполнение предписания об устранении выявленного нарушения требований по ОБИ.
3. Проведение мероприятий по предотвращению негативных последствий на значимом КИИ, причиной которых является возникновение КИ.

Основание для осуществления внеплановой проверки:

1. Истечение срока выполнения предписания об устранении выявленного нарушения требований по ОБИ.
2. Возникновение компьютерного инцидента на значимом объекте КИИ, повлекшего негативные последствия.
3. Приказ, 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.

**Содержание приказа о проведении внеплановой проверки соответствует содержанию приказа о проведении плановой проверки**

Уведомление субъекта значимой КИИ не менее чем за 24 часа до начала проведения внеплановой выездной проверки *(направление копии приказа о проверке любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления).*

*ИСКЛЮЧЕНИЕ: Предоставлено право приступить к проведению внеплановой проверки* ***незамедлительно*** *в случае возникновения компьютерного инцидента на значимом объекте КИИ, повлекшего негативные последствия.*

# Проведение проверки

1. Проводится по месту нахождения субъекта КИИ.
2. Начинается с предъявления служебных удостоверений членами комиссии.
3. Передается под расписку копия приказа о проведении проверки, заверенная печатью органа государственного контроля.
4. Комиссии должна быть предоставлена возможность ознакомиться с документами, связанными с предметом и задачами проверки, а также обеспечен беспрепятственный доступ (с учетом требований пропускного режима) на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения и к значимым объектам КИИ.
5. Для оценки эффективности принимаемых мер комиссией используются сертифицированные по ТБИ программные и аппаратно-программные средства контроля, в том числе имеющиеся у субъекта КИИ.

*(Возможность и порядок использования средств контроля с учетом особенностей функционирования значимого объекта КИИ согласовывается с руководителем субъекта КИИ или уполномоченным им должностным лицом).*

# Ограничения при проведении проверки

Члены проверочной комиссии ФСТЭК России не вправе:

1. Проверять выполнение требований по ОБИ, если они 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 документов и информации, если они не относятся к предмету 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 сроки проведения 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.

# Обязанности должностных лиц при проведении проверки

1. Своевременно и в полной мере исполнять полномочия по предупреждению, выявлению и пресечению нарушений субъектом КИИ требований по ОБИ.
2. Соблюдать права и законные интересы субъекта КИИ.
3. Проводить проверку на основании приказа, в соответствии с ее предметом и задачами, а также во время исполнения служебных обязанностей и при предъявлении служебных удостоверений и копии приказа.
4. Не препятствовать руководителю субъекта КИИ присутствовать и давать разъяснения по вопросам, относящимся к предмету проверки.
5. Предоставлять руководителю субъекта КИИ информацию и документы, относящиеся к предмету проверки.
6. Знакомить руководителя субъекта КИИ с результатами проверки.
7. Соблюдать сроки проверки.
8. Не требовать от субъекта КИИ документы (сведения), представление которых не предусмотрено законодательством.
9. Пройти в первый день проверки инструктаж по соблюдению техники безопасности при нахождении на территории, на котором расположен объект КИИ *(если такой инструктаж обязателен).*
10. Осуществить запись о проведенной проверке в журнале учета проверок (при его наличии).

# Меры, принимаемые в отношении фактов нарушения субъектом КИИ требований по ОБИ

Комиссия выдает предписание субъекту КИИ об устранении выявленного нарушения требований по ОБИ 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.

Должностные лица, проводившие проверку, **обязаны принять меры** по контролю за устранением выявленного нарушения, его предупреждению и предотвращению.

В случае невозможности выполнения субъектом КИИ (по причинам, от него не зависящим) предписания об устранении выявленного нарушения требований по ОБИ: руководитель органа государственного контроля при поступлении мотивированного обращения субъекта КИИ вправе продлить срок выполнения указанного предписания, но не более чем на один год.

Уведомление субъекта КИИ о продлении срока предписания осуществляется в течение 30 дней со дня регистрации такого обращения.

# Обязанности и права субъекта КИИ

Руководитель субъекта КИИ при проведении проверки обязан:

1. Непосредственно присутствовать при проведении проверки и давать пояснения.
2. Предоставить комиссии возможность ознакомиться с документами, связанными с задачами и предметом проверки.
3. Выполнять предписания об устранении нарушений требований по ОБИ.
4. Обеспечить с учетом требований пропускного режима беспрепятственный доступ комиссии на территорию и к значимым объектам КИИ.
5. Провести в первый день проверки инструктаж по соблюдению техники безопасности при нахождении на территории, на котором расположен объект КИИ.
6. Принимать меры по устранению выявленных нарушений.

Руководитель субъекта КИИ при проведении проверки имеет право:

1. Получать информацию, которая относится к предмету проверки.
2. Знакомиться с результатами проверки (указывать в акте проверки о своем ознакомлении, согласии или несогласии с ними, а также отдельными действиями должностных лиц органа государственного контроля).
3. Обжаловать действия (бездействие) должностных лиц органа государственного контроля, повлекшие за собой нарушение прав субъекта КИИ в административном и (или) судебном порядке.

# Права субъекта КИИ по завершении проверки

В случае несогласия с фактами, изложенными в акте проверки или предписании об устранении выявленного нарушения, руководитель субъекта КИИ вправе представить в течение 15 дней с даты получения акта проверки **в орган государственного контроля,** проводивший проверку, возражения в письменной форме.

Субъект КИИ вправе приложить к возражениям документы (их заверенные копии), подтверждающие обоснованность таких возражений, либо в согласованный срок передать их в орган государственного контроля.

До истечения срока выполнения предписания об устранении нарушений **руководитель субъекта КИИ** вправе обратиться с мотивированным обращением **к руководителю органа государственного контроля**, выдавшему предписание об устранении нарушений, о продлении срока выполнения предписания.

# Ответственность субъекта КИИ

**Руководитель субъекта КИИ** допустивший нарушение положений Правил, необоснованно препятствующий проведению проверки (уклоняющийся от ее проведения), не выполняющий в установленный срок предписания об устранении нарушений **несет ответственность** в соответствии с законодательством Российской Федерации.

## КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ

### Пункт 6 статьи 13.12

Нарушение требований о защите информации (за исключением информации, составляющей ГТ), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 настоящей статьи,

влечет наложение административного штрафа:

| | |
|---|---|
| на граждан | от 500 до 1000 рублей; |
| на должностных лиц | от 1000 до 2000 рублей; |
| на юридических лиц | от 10 000 до 15 000 рублей. |

### Пункт 2 статьи 19.5

Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа -

влечет наложение административного штрафа

на должностных лиц в размере от 5 000 до 10 000 рублей или дисквалификацию на срок до трех лет;

на юридических лиц - от 200 000 до 500 000 рублей.


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

# П Р И К А З

«11» декабря 2017 г. Москва № 229

**Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации**

---

В соответствии с пунктом 5 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736)
**П Р И К А З Ы В А Ю :**

Утвердить прилагаемую форму акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ**
**ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

**В.СЕЛИН**

# Оформление результатов проверки

1. По результатам проверки составляется акт проверки (по утвержденной форме).
2. В случае выявления нарушения требований по ОБИ выдается предписание об устранении выявленного нарушения с указанием срока его устранения.
3. К акту проверки прилагаются протоколы по результатам контрольных мероприятий, предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.
4. Акт проверки оформляется непосредственно после ее завершения в 3-х экземплярах:
   - ✓ 1 экземпляр акта вручается руководителю субъекта КИИ;
   - ✓ 2 экземпляр акта направляется в ФСТЭК России;
   - ✓ 3 экземпляр акта направляется в территориальное управление ФСТЭК России, проводившее проверку.
5. В случае проведения внеплановой проверки на основании требования прокурора **копия акта** проверки с **копиями приложений** высылается в соответствующий орган прокуратуры.

Результаты проверки, содержащие информацию, составляющую государственную, коммерческую, служебную и иную охраняемую законом тайну, оформляются с соблюдением требований законодательства Российской Федерации.

# Содержание Акта проверки

а) дата и место составления акта проверки;

б) наименование органа государственного контроля;

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

г) продолжительность и место проведения проверки;

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

е) сведения о субъекте КИИ;

ж) фамилия, имя и отчество руководителя субъекта КИИ или уполномоченного им должностного лица, присутствовавших при проведении проверки;

з) сведения о лице, эксплуатирующем значимый объект КИИ;

и) сведения о проверяемом значимом объекте КИИ;

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

л) сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у субъекта КИИ указанного журнала;

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

н) сведения об ознакомлении или отказе от ознакомления с актом проверки руководителя субъекта КИИ или уполномоченного им должностного лица.

Спасибо за внимание!