**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий Дисциплина:**

«Управление информационной безопасностью»

**ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №2**

«Перечень организационно-распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры»

**Выполнили:**

Шепелев Всеволод Александрович, студент группы N33511

(подпись)

Удинцев Максим Валерьевич, студент группы N33511

(подпись)

**Проверила:**

Михайличенко Ольга Викторовна

Санкт-Петербург

2022

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc98618881)

[**1 Состав системы документов. Классификация ОРД. Основные отличия политики, регламента, инструкции** 4](#_Toc98618882)

[**2 Анализ требований 187-ФЗ и его подзаконных актов** 6](#_Toc98618883)

[**3 Перечень документов и ОРД** 8](#_Toc98618884)

[ЗАКЛЮЧЕНИЕ 12](#_Toc98618885)

# ВВЕДЕНИЕ

**Цель работы.**

Сформировать перечень документов по безопасности значимых объектов критической информационной инфраструктуры (КИИ), разрабатываемых субъектом КИИ во исполнение Федерального закона № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» (далее - 187-ФЗ) и его подзаконных актов.

**Задачи.**

1. Определить виды документов, входящих в состав системы документов. Привести классификацию ОРД. Определить основные отличия политики, регламента, инструкции.
2. Провести анализ требований 187-ФЗ и его подзаконных актов в части требований к ОРД по безопасности значимых объектов.
3. Сформировать перечень документов и ОРД, определяющих порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов КИИ.

# **1 Состав системы документов. Классификация ОРД. Основные отличия политики, регламента, инструкции**

Система документов ИБ - объединенная целевой направленностью упорядоченная совокупность документов, регламентирующих деятельность организации, ее ДОО в области обеспечения ИБ, взаимосвязанных по функционально-целевому назначению, сфере действия, области распространения, периоду действия, а также едиными требованиями к их оформлению.

В состав системы документов входят следующие виды документов:

* основополагающие документы;
* организационно-распорядительные документы;
* документы системы стандартизации организации;
* информационно-справочные документы.

Различают следующие виды ОРД:

* организационные документы - определяют требования к организационной структуре СОИБ;
* распорядительные документы:
  1. Приказы - решение организационных и других направлений деятельности в области ИБ.
  2. Распоряжения - решение оперативных вопросов обеспечения ИБ.
  3. Планы (графики, программы) - точный перечень, последовательность и объем работ или мероприятий по обеспечению ИБ.
* иные документы, устанавливающие правила:

1. Положения – системно связанные между собой правила по вопросам, отнесенным к обеспечению ИБ.
2. Частные политики – устанавливают требования к процессам обеспечения ИБ.
3. Регламент – устанавливает правила организации какого-либо процесса обеспечения и управления ИБ, порядок действий по исполнению функций или процедур процесса.
4. Инструкции – устанавливают правила в определенном виде деятельности по обеспечению ИБ, порядок осуществления действий

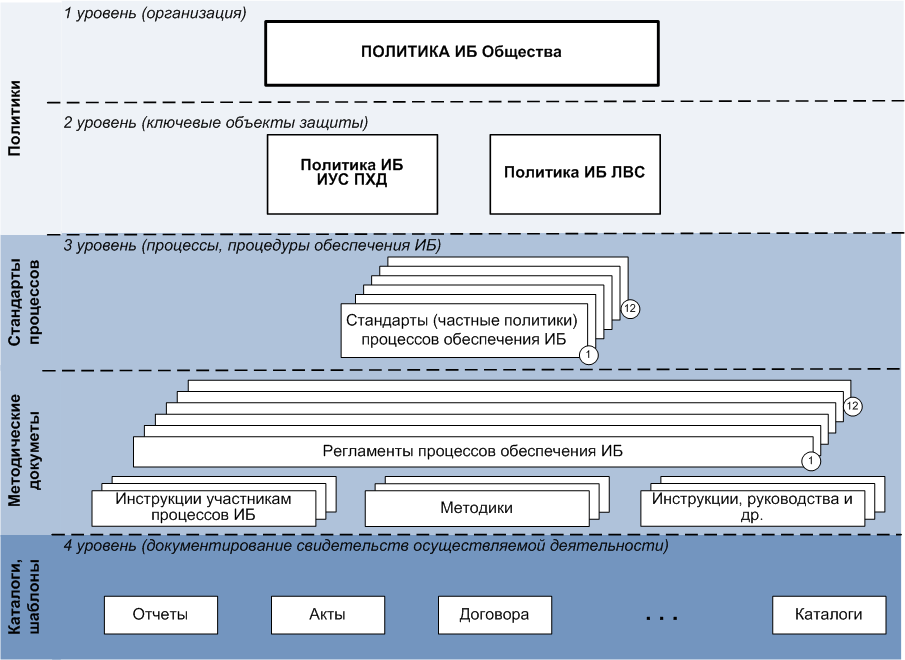


Рисунок 1 - Общая структура системы ОРД в области ИБ

**Вывод.**

Документ организационно-распорядительный - вид письменного документа, в котором фиксируют решение административных и организационных вопросов, а также вопросов управления, взаимодействия, обеспечения и регулирования деятельности органов власти, учреждений, предприятий, организаций, их подразделений и должностных лиц. Они оформляются по определенным требованиям, которые сведены в ГОСТ.

# **2 Анализ требований 187-ФЗ и его подзаконных актов**

1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 N187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» который распространяется на субъектов критической информационной инфраструктуры. Для выполнения требований законодательства организациям – субъектам КИИ необходимо выполнить следующие задачи:

* + 1. Руководитель организации – субъекта КИИ – создает комиссию по категорированию, в обязанности которой входит выявление критических процессов субъекта.
    2. Комиссией определяются объекты КИИ – информационные системы, сети и автоматизированные системы, которые связаны с этими процессами.
    3. Перечень объектов КИИ владелец согласовывает с регулятором в установленной сфере (Минэнерго для ТЭК и нефтехимической промышленности, Министерство связи и массовых коммуникаций для телеком-операторов и т. д.) и затем отправляет в ФСТЭК России.
    4. В течение года с момента согласования субъект КИИ осуществляет категорирование объектов КИИ:
* При выборе категории объект оценивается по уровню влияния на показатели значимости. Итоговая оценка ставится по максимальному значению среди критериев.
* Объекту могут быть присвоены три категории значимости. Либо комиссия признает, что объект КИИ не является значимым.
  + 1. Результаты категорирования фиксируются в акте, который утверждает руководитель субъекта КИИ, далее согласовываются с отраслевым регулятором и направляются в ФСТЭК России.
    2. Субъект КИИ должен создать систему безопасности значимых объектов КИИ. В нее входят:
* Люди (руководитель субъекта КИИ, уполномоченное лицо по контролю функционирования системы, сотрудники профильных структурных подразделений, сотрудники подразделений, ответственных за обеспечение безопасности)
* Средства защиты информации
* Организационная документация (общесистемные документы, правила безопасной работы сотрудников и регламенты действий при нештатных ситуациях)
* Документы планирования (порядок приемки и проведения испытаний, порядок взаимодействия подразделений и т. д.)
  + 1. Для каждого значимого объекта КИИ должны быть реализованы меры по обеспечению безопасности.

После внесения в реестр объектов КИИ или после последней проверки ФСТЭК России 1 раз в 3 года проводит новую проверку объектов КИИ на соответствие требованиям законодательства.

По результатам проверки возможны санкции в соответствии с действующим законодательством. Не реже 1 раза в 5 лет осуществляется пересмотр установленной категории объекта КИИ.

Выделим требования к ОРД:

* Согласно ФСТЭК 235 части 4 ОРД должны определять:

1. Цели и задачи обеспечения безопасности ЗО.
2. Основные угрозы ИБ и категории нарушителей.
3. Основные организационные и технические мероприятия по обеспечению безопасности ЗО.
4. Состав и структуру системы безопасности
5. Планы мероприятий по обеспечению безопасности ЗО.
6. Модели угроз ИБ в отношении ЗО.
7. Порядок реализации отдельных мер по обеспечению безопасности ЗО.
8. Порядок проведения испытаний средств защиты информации.
9. Порядок реагирования на компьютерные инциденты.
10. Порядок информирования и обучения работников.
11. Порядок взаимодействия подразделений субъекта КИИ при решении задач обеспечения безопасности.
12. Правила безопасной работы работников субъекта КИИ.
13. Действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций.

* Состав и формы ОРД по безопасности ЗО определяются субъектом КИИ с учетом особенностей его деятельности.
* Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте КИИ, сведения о присвоенной объекту категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
* максимальный срок категорирования не должен превышать одного года с момента согласования перечня объектов.
* Единый акт по результатам категорирования подписывается членами комиссии и утверждается руководителем субъекта КИИ
* Срок передачи во ФСТЭК сведений о результатах категорирования равен десяти дням со дня утверждения.

**Вывод.**

Проанализировав требования к ОРД по безопасности ЗО КИИ можно однозначно установить, что регуляторы ставят перед собой цель по повышению общего уровня безопасности объектов, входящих в реестр ЗО КИИ. Для этого создаются соответствующие НПА. В ОРД должна быть отражена вся важная для обеспечения безопасности информация. Это позволяет обеспечить устойчивое функционирование ЗО КИИ.

# **3 Перечень документов и ОРД**

Руководствуясь требованиями 187 и 235 ФЗ, мы составили следующий перечень ОРД по обеспечению безопасности ЗО КИИ (таблица 1).

Таблица 1 – перечень ОРД субъекта КИИ.

| Норма законодательства | Разрабатываемые документы |
| --- | --- |
| ФЗ-187 | |
| Сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты КИИ в письменном виде в десятидневный срок со дня принятия ими соответствующего решения направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ Российской Федерации, по утвержденной им форме (ч. 5 ст. 7). | **Сведения** о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. |
| Разрабатывать и осуществлять мероприятия по обеспечению безопасности критической инфраструктуры (пункт 4 ч 1 ст. 9) значимого объекта информационной | **План** проведения мероприятий по обеспечению безопасности значимых объектов КИИ. |
| Незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (пункт 1 ч 2 ст. 9) | **План** реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак |
| В случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность. (пункт 3 ч 2 ст. 9) | **Приказы** по внедрению, приемке и эксплуатации средств  **Порядок** хранения и учета средств. |
| Реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры. (пункт 3 ч 3 ст. 9) | **План** реагирования на компьютерные инциденты |
| Приказ ФСТЭК № 235 | |
| Руководитель субъекта КИИ или уполномоченное им лицо, на которое возложены функции обеспечения безопасности ЗО КИИ (далее - уполномоченное лицо), создает систему безопасности, организует и контролирует ее функционирование. (пункт 8). | **Политика** информационной безопасности значимых объектов критической информационной инфраструктуры. |
| Руководитель субъекта КИИ определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов КИИ в зависимости от количества значимых объектов КИИ, а также особенностей деятельности субъекта КИИ. (пункт 9). |
| Руководитель субъекта КИИ создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ (далее - структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение безопасности значимых объектов КИИ (далее - специалисты по безопасности). (пункт 10). |
| Субъект КИИ должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации. (пункт 15). | **Регламент** по повышению осведомленности персонала по вопросам обеспечения безопасности значимых объектов КИИ. |
| Средства защиты информации должны применяться в соответствии c инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на средства защиты информации. (пункт 20). | **Эксплуатационная документация** на средства защиты информации. |
| Порядок применения средств защиты информации определяется субъектом КИИ в ОРД по безопасности значимых объектов с учетом особенностей деятельности субъекта КИИ. (пункт 22). | **Порядок** по применению средств защиты информации. |
| Субъектом КИИ в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности ЗО КИИ. (пункт 23). | **Порядок и правила** обеспечения безопасности значимых объектов КИИ. |
| Постановление Правительства РФ от 8 февраля 2018 г. № 127 | |
| Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию (пункт 11): | **Приказ** о создании комиссии. |
| Комиссия по категорированию в ходе своей работы определяет процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ; | **Перечень** процессов в рамках функций (полномочий) или видов деятельности. |
| Комиссия по категорированию в ходе своей работы выявляет объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов; | **Перечень** объектов КИИ, подлежащих категорированию. |
| Комиссия по категорированию в ходе своей работы рассматривает возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации; | **Перечень** возможных действий нарушителей в отношении объектов КИИ. |
| Комиссия по категорированию в ходе своей работы анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ; | **Перечень** угроз безопасности и уязвимостей программного обеспечения объектов КИИ. |
| Комиссия по категорированию в ходе своей работы устанавливает каждому из объектов КИИ одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости. | **Акт** категорирования объектов КИИ |
| Приказ ФСТЭК №239 | |
| Разработка организационных и технических мер по обеспечению безопасности ЗО осуществляется субъектом КИИ и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по созданию (модернизации) значимого объекта и (или) обеспечению его безопасности, в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта и должна включать (пункт 11):  а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии); | **Модель угроз** безопасности информации для объекта КИИ или группы объектов КИИ. |
| б) проектирование подсистемы безопасности значимого объекта; | **Техническое задание.**  **Технический проект.** |
| в) разработку рабочей (эксплуатационной) документации на значимый объект КИИ (в части обеспечения его безопасности). | Эксплуатационная документация уже описана выше |
| Установка и настройка средств защиты информации должна проводиться в соответствии с проектной и рабочей (эксплуатационной) документацией | **Акт** установки средств защиты. |
| Предварительные испытания значимого объекта и его подсистемы безопасности должны проводиться в соответствии с программой и методиками предварительных испытаний… | **Программа и методики** предварительных испытаний работоспособности подсистемы безопасности значимого объекта |
| Опытная эксплуатация значимого объекта и его подсистемы безопасности должна проводиться в соответствии с программой и методиками опытной эксплуатации… | **Программа и методики** опытной эксплуатации |
| В ходе приемочных испытаний значимого объекта и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности настоящим Требованиям | **Программа и методики** приемочных испытаний.  **Акт** приемки значимого объекта в эксплуатацию.  **Приказ** о вводе в действие значимого объекта и его подсистемы безопасности. |

**Вывод.**

Проведя анализ и собрав требования 187, 235 и 239 ФЗ мы составили примерный список организационно-распорядительной документации субъекта КИИ. Это далеко не исчерпывающий перечень и, конечно, в действительности потребуется значительно больше документов.

# ЗАКЛЮЧЕНИЕ

В ходе практической работы был сформулирован перечень ОРД, необходимый для соответствия 187-ФЗ и его подзаконным актам. Организационные документы необходимы для регламентирования деятельности организации. Именно с их помощью фиксируются права и обязанности работников и работодателей, закрепляется их взаимная ответственность. Любые действия в организации формального характера должны соответствующим образом отражаться на бумаге. Поэтому они необходимы любой организации. Этот перечень поможет субъектам КИИ не упустить из виду важные аспекты построения защищённой системы.