В соответствии с Федеральным законом № 390-ФЗ «О безопасности» организациям рекомендуется разработать и внедрить следующие документы для обеспечения комплексной системы безопасности:

1. **Политика безопасности организации**: определяет общие принципы и подходы к обеспечению безопасности в организации.
2. **Положение об обеспечении безопасности**: детализирует меры и процедуры, направленные на защиту различных аспектов деятельности организации.
3. **План мероприятий по обеспечению безопасности**: содержит конкретные действия, сроки и ответственных лиц за реализацию мер безопасности.
4. **Приказы о назначении ответственных за безопасность**: документы, назначающие сотрудников, ответственных за различные направления безопасности (информационная, физическая, экономическая и т.д.).
5. **Инструкции для сотрудников по вопросам безопасности**: руководства, описывающие обязанности и действия сотрудников в различных ситуациях, связанных с безопасностью.
6. **План реагирования на чрезвычайные ситуации**: определяет порядок действий при возникновении инцидентов, угрожающих безопасности организации.
7. **Отчеты и акты по результатам проверок и аудитов безопасности**: документы, фиксирующие результаты внутренних и внешних проверок системы безопасности.
8. **Журналы учета инцидентов безопасности**: регистрация всех происшествий, связанных с нарушением безопасности, и принятых мер по их устранению.
9. **Планы обучения и повышения квалификации сотрудников в области безопасности**: программы, направленные на повышение осведомленности и компетентности персонала в вопросах безопасности.
10. **Договоры с контрагентами, содержащие требования по обеспечению безопасности**: соглашения, включающие обязательства сторон по соблюдению мер безопасности при взаимодействии.

Эти документы помогут организации соответствовать требованиям законодательства и обеспечить эффективную защиту от различных угроз.

**Дополнения к списку документов по ФЗ № 390-ФЗ "О безопасности"**

Для комплексного выполнения требований закона можно добавить следующие документы:

**I. Организационные документы**

1. **Реестр угроз безопасности организации**:
   * Перечень возможных угроз (физических, информационных, экономических) с их вероятностью и последствиями.
2. **Акт категорирования объектов безопасности**:
   * Определение степени значимости объектов организации для национальной и корпоративной безопасности.
3. **Документ о порядке взаимодействия с государственными органами**:
   * Регламент информирования уполномоченных органов в случае выявления критических угроз или инцидентов.
4. **Регламент управления доступом**:
   * Устанавливает правила предоставления и контроля доступа сотрудников к объектам и ресурсам.

**II. Документы для обеспечения информационной безопасности**

1. **Инструкция по работе с конфиденциальной информацией**:
   * Регламентирует порядок работы с данными, которые не подлежат разглашению.
2. **Положение о порядке мониторинга информационных систем**:
   * Описывает методы и средства контроля за использованием информационных ресурсов.
3. **Журнал учета носителей информации**:
   * Регистрация всех физических и цифровых носителей, содержащих конфиденциальную информацию.
4. **Политика по защите критической информационной инфраструктуры (КИИ)**:
   * Документ для организаций, относящихся к объектам КИИ, регламентирующий защиту информационных систем.

**III. Документы для физической безопасности**

1. **План физической охраны объектов**:
   * Описание мер физической защиты объектов, включая контроль доступа, видеонаблюдение, сигнализацию.
2. **Инструкция по пропускному режиму**:
   * Регламент контроля доступа сотрудников и посетителей на территорию организации.
3. **Акт проверки состояния технических средств физической защиты**:
   * Результаты регулярной оценки состояния систем видеонаблюдения, сигнализации и других средств физической безопасности.

**IV. Документы по реагированию на инциденты**

1. **План антикризисного управления**:
   * Детализированный алгоритм действий в случае возникновения чрезвычайных ситуаций или угроз.
2. **Протокол реагирования на инциденты безопасности**:
   * Описание последовательности действий сотрудников при обнаружении инцидентов (например, утечка данных, кибератака).
3. **Журнал инцидентов безопасности**:
   * Учет всех случаев нарушения безопасности с датой, описанием и мерами реагирования.

**V. Обучение и контроль персонала**

1. **Программа обучения по вопросам безопасности**:
   * Документ, описывающий содержание и порядок проведения обучения для сотрудников.
2. **Протоколы инструктажа сотрудников**:
   * Подтверждение, что сотрудники ознакомлены с процедурами безопасности и своими обязанностями.
3. **План проведения учебных тревог**:
   * График и сценарии тренингов для отработки действий при угрозах (пожар, утечка информации, физическое вторжение).

**VI. Документы для внешнего взаимодействия**

1. **Соглашения с подрядчиками о соблюдении мер безопасности**:
   * Устанавливает обязательства сторон в отношении обеспечения безопасности при взаимодействии.
2. **Договоры с провайдерами услуг безопасности**:
   * Условия предоставления услуг охраны, мониторинга и других функций.
3. **Протоколы проверок подрядчиков**:
   * Результаты проверок выполнения контрагентами требований по безопасности.

**VII. Постоянный мониторинг и аудит**

1. **План внутреннего аудита безопасности**:
   * Устанавливает порядок проведения регулярных проверок системы безопасности.
2. **Отчет о результатах аудита системы безопасности**:
   * Документ, фиксирующий выявленные несоответствия и рекомендации по их устранению.
3. **План модернизации системы безопасности**:
   * Содержит предложения по улучшению и актуализации мер безопасности в организации.

**VIII. Дополнительные рекомендации**

1. **Паспорт безопасности объектов**:
   * Подробное описание объектов организации с указанием мер защиты.
2. **Документ о резервировании и восстановлении данных**:
   * Регламентирует порядок создания резервных копий и восстановления информации после инцидентов.
3. **Протоколы взаимодействия с экстренными службами**:
   * Алгоритмы связи и совместных действий с пожарными, полицией, службой МЧС.

**Итог**

Эти дополнения охватывают более широкий спектр аспектов безопасности, включая физическую, информационную, кадровую и кризисную составляющие. Это обеспечит комплексное выполнение требований ФЗ-390 и защиту всех ключевых активов организации. Если требуется помощь в разработке шаблонов этих документов, дайте знать!

**Подсчет документов, необходимых для организации в соответствии с ФЗ № 390-ФЗ "О безопасности"**

На основании перечисленных выше документов, вот итоговый перечень с подсчетом:

**I. Организационные документы *(7 документов)***

1. Политика безопасности организации.
2. Положение об обеспечении безопасности.
3. План мероприятий по обеспечению безопасности.
4. Приказ о назначении ответственных за безопасность.
5. Акт категорирования объектов безопасности.
6. Регламент управления доступом.
7. Документ о порядке взаимодействия с государственными органами.

**II. Документы по информационной безопасности *(7 документов)***

1. Инструкция по работе с конфиденциальной информацией.
2. Положение о порядке мониторинга информационных систем.
3. Политика по защите критической информационной инфраструктуры (КИИ).
4. Журнал учета носителей информации.
5. Паспорт безопасности информационных систем.
6. Протокол тестирования систем защиты данных.
7. План модернизации систем защиты.

**III. Документы по физической безопасности *(4 документа)***

1. План физической охраны объектов.
2. Инструкция по пропускному режиму.
3. Акт проверки состояния технических средств защиты.
4. Протокол взаимодействия с экстренными службами.

**IV. Документы по реагированию на инциденты *(5 документов)***

1. План антикризисного управления.
2. Протокол реагирования на инциденты.
3. Журнал инцидентов безопасности.
4. Отчет о расследовании инцидентов.
5. Протокол тестирования антикризисного плана.

**V. Документы по управлению рисками *(3 документа)***

1. Реестр угроз безопасности организации.
2. План управления рисками.
3. Отчет о регулярной оценке рисков.

**VI. Документы для обучения и контроля персонала *(5 документов)***

1. Программа обучения по вопросам безопасности.
2. Протоколы инструктажа сотрудников.
3. План проведения учебных тревог.
4. Отчет о результатах обучения сотрудников.
5. Регламент внутреннего контроля действий сотрудников.

**VII. Документы по взаимодействию с подрядчиками и внешними организациями *(3 документа)***

1. Соглашения с подрядчиками о соблюдении мер безопасности.
2. Протоколы проверок подрядчиков.
3. Договоры с провайдерами услуг безопасности.

**VIII. Документы по мониторингу и аудиту *(4 документа)***

1. План внутреннего аудита безопасности.
2. Отчет о результатах аудита системы безопасности.
3. Протокол тестирования резервных копий.
4. Протокол имитации реальных атак (пентесты).

**Итоговый подсчет**

**Итого: 38 документов**.

Эти документы охватывают все ключевые аспекты безопасности, включая физическую, информационную и кадровую составляющие. Если требуется помощь с конкретным документом, например, шаблон или инструкция, сообщите!