ИМБА ИТ

Что требуется сделать и как соответствовать требованиям Указа 250

Попадает ли ваша организация под Указ 250?

Указ 250 распространяется на следующие организации:

- Органы государственной власти
- Высшие исполнительные органы государственной власти
- Государственные фонды
- Государственные корпорации
- Иные предприятия, созданные на основании ФЗ
- Стратегические предприятия и стратегические акционерные общества
- Системообразующие организации российской экономики
- Субъекты КИИ

Список сфер деятельности, в которых есть КИИ, на которых распространяется Указ 250

Субъектам КИИ являются:

- Государственные органы
- Государственные учреждения
- Российские юридические лица
- Российские ИП

Которым принадлежат ИС, ИТС, АСУ в следующих сферах деятельности:

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Банковская сфера и иные сферы финансового рынка
- Топливно-энергетический комплекс
- Атомная энергетика
- Оборонная промышленность
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность

Если ваша организация попадает в перечень выше, то на вас распространяется Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и в соответствии с ним вы должны выполнить следующие задачи по информационной безопасности (ИБ)

Органы управления по ИБ в компании

- Создано управление по обеспечению информационной безопасности.
- Выстроено взаимодействие с подрядчиками по вопросам обеспечения информационной безопасности.
- Обеспечена информационная безопасность.
- Используются средства защиты информации.
- Налажено взаимодействие с ГосСОПКА.

Создание управления по обеспечению информационной безопасности

- Назначен заместитель руководителя организации, ответственный за обеспечение ИБ.
- Подготовлено и утверждено положение о заместителе руководителя организации, ответственном за обеспечение ИБ.
- Заместитель руководителя организации, ответственный за обеспечение ИБ, обладает высшим образованием (не ниже уровня специалитета или магистратуры) в сфере ИБ или прошел профпереподготовку по программе длительностью не менее 360 часов, согласованной с ФСТЭК России или ФСБ России в соответствии с Приказом Министерства образования и науки от 19.10.2020 № 1316.
- Заместитель руководителя организации, ответственный за обеспечение ИБ, проходит повышение квалификации не менее одного раза в пять лет.
- Налажено регулярное информирование руководства организации о компьютерных инцидентах и текущем уровне ИБ в организации.
- Руководство организации ознакомлено с мерами ответственности за обеспечение ИБ (ст. 13.12, 13.12.1, 19.5 КоАП, ст. 274 и 274.1 УК РФ и др.).
- Создано подразделение, отвечающее за ИБ, или эти задачи возложены на иное подразделение.
- Подготовлено и утверждено (или актуализировано) положение о подразделении, обеспечивающем ИБ, в соответствии с Постановлением Правительства РФ от 15.07.2022 № 1272.
- Подразделение подчинено заместителю руководителя организации, ответственному за обеспечение ИБ, или иным лицам из состава руководства организации при условии курирования со стороны руководителя организации.

Взаимодействие с подрядчиками по вопросам обеспечения информационной безопасности

- Все привлекаемые к осуществлению мероприятий по ИБ организации (анализ защищенности, обучение, проектирование и т. п.) имеют лицензию ФСТЭК России на оказание услуг в области технической защиты конфиденциальной информации.
- Все привлекаемые для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты организации имеют аккредитацию ФСБ России в качестве центра государственной системы обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА).
- Все привлекаемые для оценки уровня защищенности организации имеют лицензии ФСБ России и ФСТЭК России.

Обеспечение информационной безопасности

- Разработана и утверждена политика организации в области информационной безопасности.
- Определены цели обеспечения информационной безопасности.
- Выполнены работы по оценке уровня защищенности информационной инфраструктуры в соответствии с «Типовым техническим заданием» Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Подробнее тут:

  Реализуются организационные и технические меры в области ИБ.
- Организованы работы по формированию навыков и повышению осведомленности работников организации в сфере ИБ.
- Организован контроль за соблюдением нормативных правовых актов в области ИБ.
- Организован контроль пользователей организации в части соблюдения ими конфиденциальности информации и правил работы со съемными носителями информации.
- Спланированы мероприятия по обеспечению ИБ в подведомственных организациях, филиалах, представительствах (при их наличии).
- Проводится контроль состояния ИБ, включая оценку защищенности, в подведомственных организациях, филиалах, представительствах (при их наличии).
- Проводятся регулярные практические учения по противодействию компьютерным атакам (киберучения).
- Проводится регулярный анализ и оценка новых угроз, способов и методов проведения компьютерных атак (процесс threat intelligence).
- Выстроен непрерывный процесс выявления и устранения угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств.
- Проведена оценка практической возможности использования нарушителями недостатков (уязвимостей) средств защиты информации и программного обеспечения (на примере наиболее критически важных).
- Выстроен непрерывный процесс обнаружения, предотвращения и ликвидация последствий компьютерных атак и реагирования на компьютерные инциденты.

Использование средств защиты информации

- Проведена инвентаризация используемых средств защиты информации и выделены все средства из недружественных государств.
- Проведена оценка возможности перехода с используемых средств защиты информации из недружественных государств на иные решения (отечественные, open source или из дружественных государств).
- Подготовлен план перехода со средств защиты информации из недружественных государств к 1 января 2025 года.
- Осуществлено пилотирование выбранных решений, пришедших на смену средствам защиты информации из недружественных государств.
- Выбранные средства защиты информации протестированы и внедрены.

Взаимодействие с ГосСОПКА

- Подготовлен и утвержден регламент взаимодействия с должностными лицами ФСБ России в рамках получения ими доступа, в том числе удаленного, в целях осуществления мониторинга.
- Осуществляется мониторинг защищенности информационных ресурсов, принадлежащих организации или используемых ею, в соответствии с порядком, утвержденным ФСБ России.
- Организовано взаимодействие с должностными лицами ФСБ России и ее территориальных органов по результатам мониторинга защищенности информационных ресурсов организации.
- Организовано взаимодействие с НКЦКИ напрямую (требуется отдельное соглашение с НКЦКИ), через аккредитацию службы ИБ в качестве центра ГосСОПКА или через взаимодействие с аккредитованными центрами ГосСОПКА.