

Указ Президента РФ от 01.05.2022 № 250

Чек-лист

Относится ли ваша организация к любому из указанных типов?

- федеральный орган исполнительной власти;
- высший исполнительный орган госвласти субъекта РФ;
- государственный фонд;
- госкорпорация (госкомпания);
- предприятие, созданное на основании федерального закона;
- стратегическое предприятие;
- стратегическое акционерное общество;
- системообразующая организация экономики (на уровне РФ или субъекта РФ);
- субъект критической информационной инфраструктуры (независимо от наличия значимых объектов КИИ),

Если да, то в соответствии с Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и подзаконными актами вам необходимо выполнить следующие задачи в области информационной безопасности (далее также — ИБ), сгруппированные по направлениям.

Органы управления организации по обеспечению информационной безопасности

- ☐ **Назначен** заместитель руководителя организации, ответственный за обеспечение ИБ.
- ☐ **Подготовлено и утверждено** положение о заместителе руководителя организации, ответственном за обеспечение ИБ, в соответствии с Постановлением Правительства РФ от 15.07.2022 № 1272.

  Примечание. Ответственным за обеспечение ИБ в субъектах РФ должен быть назначен вице-губернатор или заместитель мэра, а в министерствах — лицо в ранге заместителя министра.
- ☐ Заместитель руководителя организации, ответственный за обеспечение ИБ, **входит в состав коллегиальных органов** организации.

  Примечание. Наличие коллегиального органа организации определяется уставом организации. К коллегиальным органам относятся правление, дирекция, совет директоров и т. п.
- ☐ 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.
- ☐ Основополагающие документы организации в сфере ИТ, цифровизации и цифровой трансформации **проходят согласование** с заместителем руководителя организации, **ответственным за обеспечение ИБ**.
- ☐ **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.).

Подразделение, обеспечивающее информационную безопасность

- ◯ **Создано подразделение**, отвечающее за ИБ, или эти задачи возложены на иное подразделение.

  Примечание. Часто функция обеспечения ИБ возлагается на службу информационных технологий, а подразделение ИБ входит в его состав. Однако в условиях наличия в организации еще и подразделений по цифровизации или цифровой трансформации рекомендуется в целях исключения конфликтов выделение службы ИБ в отдельное подразделение.

- ◯ **Подготовлено и утверждено** (или актуализировано) положение о подразделении, обеспечивающем ИБ, в соответствии с Постановлением Правительства РФ от 15.07.2022 № 1272.

- ◯ Подразделение п**одчинено заместителю руководителя организации, ответственному за обеспечение ИБ**, или иным лицам из состава руководства организации при условии курирования со стороны руководителя организации.

Обеспечение информационной безопасности

- ◯ **Разработана и утверждена** политика организации в области информационной безопасности.
- ◯ **Определены цели** обеспечения информационной безопасности.
- ◯ **Сформулирован перечень** недопустимых событий и негативных последствий (ущерба) для организации.
- ◯ **Проведена оценка** возможности возникновения и реализации недопустимых событий путем моделирования целевых атак.
- ◯ **Проводятся мероприятия** по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).
- ◯ **Проводится контроль эффективности** (результативности) мероприятий по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).
- ◯ **Реализуются** организационные и технические меры в области ИБ, требования о реализации которых направляются ФСТЭК России и ФСБ России.
- ◯ **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.

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**.

  Обратите внимание: в тексте Указа стоит союз «и», а не «или», то есть привлекаемая организация должна обладать сразу двумя лицензиями.

Использование средств защиты информации

- ◯ **Проведена инвентаризация** используемых средств защиты информации и выделены все средства из недружественных государств.

  Примечание. В соответствии с Указом Президента РФ от 30.03.2022 № 166 требование о запрете использования иностранного ПО не зависит от статуса «дружественности» страны его происхождения и применяется к любому иностранному ПО, включая и средства защиты информации.

- ◯ **Проведена оценка** возможности перехода с используемых средств защиты информации из недружественных государств на иные решения (отечественные, open source или из дружественных государств).

  Примечание. В соответствии с требованиями ФСБ России и ФСТЭК России средства защиты информации, используемые на значимых объектах КИИ и в государственных информационных системах, а также средства обнаружения, предотвращения и ликвидации последствий компьютерных атак должны обладать действующей технической поддержкой, что может быть затруднительно в отношении решений open source.

- ◯ **Подготовлен план перехода** со средств защиты информации из недружественных государств к 1 января 2025 года.

  Примечание. В соответствии с Указом Президента РФ от 30.03.2022 года № 166 заказчикам согласно 223-ФЗ запрещена закупка любого иностранного ПО (включая и средства защиты информации) с 31 марта 2022 года независимо от статуса «дружественности» государства.

- ◯ О**существлено 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.

  Примечание. Выбор способа взаимодействия с НКЦКИ определяется организацией самостоятельно.

Если у вас остались вопросы, связанные с реализацией Указа Президента РФ от 01.05.2022 № 250, вы можете задать их по адресу pt@ptsecurity.com