Указ Президента РФ от 01.05.2022 N 250

Реализация требований законодательства РФ в области ИБ

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Указ Президента РФ от 01.05.2022 N 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Описание указа

1 мая 2022 г. вышел Указ Президента Российской Федерации N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Данный Указ направлен на повышение уровня информационной безопасности (ИБ). Рассмотрим основные моменты из Указа N 250.

Следующим организациям необходимо принять ряд мер по повышению уровня безопасности информационных ресурсов:

- федеральным органам исполнительной власти
- высшим исполнительным органам государственной власти субъектов РФ
- государственным фондам
- государственным корпорациям (компаниям) и иным организациям, созданным на основании федеральных законов
- стратегическим предприятиям
- стратегическим акционерным обществам (согласно Указу Президента РФ от 04.08.2004 N 1009 «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ»)
- системообразующим организациям российской экономики
- юридическим лицам, являющимся субъектами критической информационной инфраструктуры (КИИ) (Все субъекты критической информационной инфраструктуры, независимо от того, обладают они значимыми или незначимыми объектами КИИ)

На руководителя возлагается персональная ответственность за обеспечение информационной безопасности соответствующих органов.

Полномочия по обеспечению ИБ возлагаются на заместителя руководителя организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Необходимо создать структурное подразделение, ответственное за обеспечение ИБ, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить такие функции на существующее подразделение.

В соответствии с подпунктом «а» пункта 3 Указа N 250 утверждено: Постановление Правительства от 15 июля 2022 года N 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающим информационную безопасность органа (организации)».

Подробнее

К мероприятиям по обеспечению информационной безопасности органа (организации) могут привлекаться сторонние организации, исключительно имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

К мероприятиям по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, исключительно аккредитованные центры ГосСОПКА.

Согласно Приказу ФСБ России от 1 ноября 2022 г. N 543 «Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. N 250», вступил в силу 13 декабря 2022 г., переходный период, составляет 3 года со дня вступления в силу этого приказа, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в интересах органов и организаций, которые попадают под действие Указа Президента РФ от 1 мая 2022 г. N 250 на основании заключенных с ФСБ России соглашений о сотрудничестве в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Требования указа

Обеспечивать беспрепятственный доступ органам ФСБ (в том числе удаленный) к принадлежащим органам (организациям) либо используемым ими информационным ресурсам, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети Интернет.

Обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются на регулярной основе в органы (организации) с учетом меняющихся угроз в информационной сфере.

Органам (организациям), указанным в (Распоряжение Правительства РФ от 22.06.2022 N 1661-р «Об утверждении перечня ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России»), необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России.

Подробнее

Органам (организациям) провести инвентаризацию используемых средств защиты информации, разработать план перехода к 01.01.2025 на использование отечественных средств защиты информации. С 1 января 2025 г. органам (организациям) запрещается использовать СЗИ, происходящие из недружественных государств, либо производителями которых являются организации. находящиеся под их юрисдикцией, прямо или косвенно подконтрольные им либо аффилированные с ними.

Список недружественных стран

(согласно Распоряжение Правительства РФ от 05.03.2022 N 430-р (ред. от 29.10.2022) «Об утверждении перечня иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, российских юридических и физических лиц»):

1. Австралия
2. Албания
3. Андорра
4. Багамские Острова
5. Великобритания (включая коронные владения Британской короны и Британские заморские территории)
6. Государства-члены Европейского союза
7. Исландия
8. Канада
9. Лихтенштейн
10. Микронезия
11. Монако
12. Новая Зеландия
13. Норвегия
14. Республика Корея
15. Сан-Марино
16. Северная Македония
17. Сингапур
18. Соединенные Штаты Америки
19. Тайвань (Китай)
20. Украина
21. Черногория
22. Швейцария
23. Япония

Сопоставление требований и реализации

Согласно требованиям, описанным в пункте 6 Указа N 250, в организациях, на которые распространяются требования указа, запрещено использовать иностранное ПО и СЗИ на значимых объектах КИИ. Для выполнения данного требования «Лаборатория Касперского» предлагает сертифицированные продукты.

СЗИ проходят процедуру оценки соответствия, имеют сертификаты соответствия требованиям по защите информации

Все разрабатываемое ПО находится в Едином реестре российского ПО

«Лаборатория Касперского» предоставляет решения для выполнения требований по защите информации

«Лаборатория Касперского» оказывает услуги по оценке уровня защищенности согласно требованиям Указа N 250

1 Запрещено использовать иностранное ПО и СЗИ на значимых ОКИИ (пункт 6 Указа N 250)

Продукт	Соответствует требованиям
Kaspersky Unified Monitoring and Analysis Platform	4 Уровень доверия
Kaspersky Anti Targeted Attack	4 Уровень доверия, СОВ уровня сети 4 класса защиты
Kaspersky EDR Expert	4 Уровень доверия, СОВ уровня узла 4 класса защиты, средство антивирусной защиты типов «Б» и «В» 4 класса защиты
Kaspersky Endpoint Security	2-4 Уровень доверия, средства антивирусной защиты типов «Б», «В» и «Г» 2-4 классов защиты
Kaspersky Web Traffic Security	2 Уровень доверия, средство антивирусной защиты типа «Б» 2 класса защиты
Kaspersky Industrial CyberSecurity for Networks / Nodes	4 Уровень доверия, СОВ уровня сети 4 класса защиты / 3 Уровень доверия, средство антивирусной защиты типа «В» 3 класса защиты

2 Необходимо обеспечить реализацию организационных и технических мер по защите информации (подпункт «е» пункта 1 Указа N 250)

Согласно требованиям описанным в подпункте «е» пункта 1 Указа N 250 в организациях на которые распространяются требования указа необходимо обеспечить реализацию организационных и технических мер. Для выполнения данного требования «Лаборатория Касперского» предлагает следующие продукты:

Продукт	Выполняемый набор мер
 Kaspersky Unified Monitoring and Analysis Platform	Непрерывный мониторинг и реагирование на инциденты информационной безопасности
	Сбор и анализ сетевого трафика
	Автоматизированное реагирование на инциденты ИБ
	Инвентаризация / категоризация активов
	Оценка возможности возникновения недопустимых событий
	Обогащение событий информационной безопасности
	Предоставление отчетности
 Kaspersky Anti Targeted Attack	Анализ собранных объектов сетевого трафика
	Проверка файлов на наличие скрытого вредоносного функционала
	Создание правил автоматического реагирования на конечных станциях
	Фиксация факта обнаружения вторжения, уведомление администратора безопасности
	Анализ почтового трафика на наличие вредоносного ПО
	Анализ подозрительных файлов на конечных станциях пользователей
	Эмуляция работы подозрительного ПО в изолированной среде

Kaspersky EDR Expert	Автоматический анализ подозрительных событий на конечных рабочих станциях
	Изоляция хоста на уровне сети
	Возможность запуска произвольного скрипта исполняемого файла
	Запрет запуска заданного ПО на конечной рабочей станции
	Автоматический сбор данных для проведения расследования инцидента ИБ
	Централизованный поиск вредоносного ПО на конечных рабочих станциях
	Эмуляция работы подозрительного ПО в изолированной среде
	Визуализация дерева событий полученных с рабочих станций для расследования инцидентов ИБ
Kaspersky Security для бизнеса	Автоматическое антивирусное сканирование в режиме реального времени
	Антивирусное сканирование подключаемых устройств
	Автоматическая блокировка действий вредоносных программ
	Автоматическая блокировка баннеров и всплывающих окон при работе с Web страницами
	Контроль используемого ПО / запуска ПО на рабочих станциях / серверах
	Работа с разными типами ОС (Linux / Windows)
Kaspersky Web Traffic Security	Автоматическое обнаружение и лечение вирусов в любых файлах и вложениях
	Автоматическая блокировка вредоносных и фишинговых сайтов
	Проверка репутации файлов с использованием облачных сервисов
	Гибкая настройка правил доступа к ресурсам по различным критериям
	Контроль используемых веб-обозревателей
	Предоставление инструментария в расследовании инцидентов информационной безопасности

Kaspersky Industrial CyberSecurity

- Анализ уязвимостей и их устранение
- Регистрация событий безопасности
- Мониторинг безопасности
- Контроль и анализ сетевого трафика
- Комплексная защита конечных узлов
- Обнаружение и предотвращение компьютерных атак
- Информирование о компьютерных инцидентах

3 Необходимо произвести оценку уровня защищенности системы (пункт 4 Указа N 250)

Согласно требованиям, описанным в пункте 4 Указа N 250, организациям необходимо провести оценку уровня защищенности инфраструктуры / информационных систем. Для выполнения данного требования «Лаборатория Касперского» предлагает сервисы по анализу защищенности. Также оперативную информацию по уровню защищенности предоставляют предлагаемые продукты.

Продукты и услуги	Оценка защищенности
Kaspersky Anti Targeted Attack Kaspersky EDR Expert	• Оценка защищенности почтовой инфраструктуры / веб доступа / рабочих станций • Базовый отчет защищенности
Kaspersky Unified Monitoring and Analysis Platform Kaspersky Symphony XDR	• Оценка защищенности инфраструктуры в целом • «Обзор угроз»

Продукты и услуги

Оценка защищенности

Kaspersky EDR Expert

Kaspersky Security для бизнеса

- Оценка защищенности конечных рабочих станций
- «Выявленные угрозы ИБ»

Kaspersky Security Assessment

Kaspersky Security Awareness

- Анализ защищенности приложения
- Анализ защищенности инфраструктуры
- Выявление и консолидация недопустимых событий ИБ
- Оценка осведомленности сотрудников в вопросах ИБ
- Проверка практической возможности использования уязвимостей
- Разработка маршрутной карты по модернизации информационной инфраструктуры
- Оценка мер противодействия

Kaspersky Industrial CyberSecurity

- Оценка защищенности автоматизированной системы управления технологическими процессами
- Отчет о безопасности системы

Kaspersky Automated Security Awareness Platform

Повышение осведомленности пользователей в области информационной безопасности

4 Прочие требования Указа N 250

«Лаборатория Касперского» предлагает комплексный подход к выполнению требований Указа N 250. Комплексное предложение включает в себя продукты и услуги на схеме ниже.

Выполнение требований Указа N 250

Консалтинг

Kaspersky SOC Consalting — Оценка существующего SOC заказчика

Kaspersky Security Assessment — Анализ защищенности инфрастуктуры / приложений

Поставка и внедрение средств защиты

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Anti Targeted Attack

Kaspersky EDR Expert

Kaspersky Symphony XDR

Kaspersky Industrial CyberSecurity

И другие средства защиты

Автоматизация расследования за счет использования средств защиты

Анализ состояния имеющихся продуктов «Лаборатории Касперского»

Рекомендации по конфигурации продуктов «Лаборатории Касперского»

Тренинги для специалистов по IT-безопасности

Цифровая криминалистика

Анализ вредоносного ПО

Реагированиена инциденты

Эффективное обнаружение угроз

Тренинги по основам кибербезопасности

Обучение пользователей — Kaspersky Automated Security Awareness Platform

Узнать подробнее о продуктах и сервисах «Лаборатории Касперского»

Подробнее

Остались вопросы?

Задайте их нашим специалистам, и мы обязательно вам ответим regulhub@kaspersky.com.
За более подробной информацией можно обратиться к нам на сайт

Подробнее

www.kaspersky.ru