Проверка ФСТЭК по обеспечению безопасности КИИ в ПАО МГТС

27.03.2024

Директор департамента информационной безопасности
Блок безопасности Корпоративный центр Группы МТС

Хрусталев Александр Александрович

Этапы подготовки и проведения проверки*

№ п/п	Наименование этапа	Мероприятия **
1	Получена выписка из ежегодного плана проверок До 1 января года планируемой проверки	1. Запросить предварительный перечень вопросов; 2. Провести самоаудит по пунктам требований нормативных документов (235, 239 приказы ФСТЭК, 250 Указ Президента…); 3. Подготовить и реализовать план устранения выявленных в ходе самоаудита недостатков; 4. Подготовить ответы по перечню вопросов с приложением подтверждающих документов.
2	Получена копия приказа о проведении проверки Не менее чем за 3 рабочих дня до начала проверки	1. Получить перечень вопросов; 2. Подготовить и согласовать план проверки (встреча с руководством, даты объезда площадок и работы с документами…); 3. Организовать рабочие места для проверяющих; 4. Подготовить недостающие ответы (в случае изменения перечня вопросов).
3	Начало проверки	1. Встреча с руководителем субъекта КИИ, на которой будут предъявлены служебные удостоверения должностных лиц органа госконтроля и передана под роспись копия приказа о проведении проверки;
4	Объезд площадок	1. Объезд площадок в соответствии с планом, опрос персонала, демонстрация используемых механизмов обеспечения безопасности и дача необходимых пояснений.
5	Оценка эффективности применяемых мер	1. Сканирование объектов на уязвимости; 2. Обоснование невозможности эксплуатации выявленных уязвимостей (в случае выявления).
6	Работа с документами	1. Анализ проверяющими предоставленных документов и ответов на вопросы; 2. Подготовка ответов, разъяснений и материалов по дополнительным запросам.
7	Оформление результатов проверки	1. Подготовка акта по результатам проверки; 2. Подготовка предписания об устранении выявленных нарушений (при выявлении). 3. Встреча с руководителем субъекта КИИ для вручения под роспись акта проверки и предписания.
8	Устранение выявленных нарушений	1. Подготовка и согласование плана устранения нарушений; 2. Устранение нарушений в соответствии с планом; 3. Подготовка отчета об устранении нарушений.

* Правила проведения проверки определены ПП от 17.02.2018 №162

** Перечень мероприятий в целом сформирован по опыту прохождения проверки в МГТС и носит рекомендательный/информационный характер

На что следует обратить внимание (#1):

01

Модели угроз и нарушителя
Модели угроз и нарушителя должны быть актуальны и соответствовать по содержанию требованиям 239 приказа. На основании моделей МУиН с учетом требований 239 приказа должны быть разработаны профили защиты.

02

Создание системы безопасности
Создание системы безопасности должно быть завершено. Должна быть разработана организационно-распорядительная, проектная и рабочая документация. Технические средства системы безопасности должны быть введены в эксплуатацию и обеспечивать выполнение требований 235 и 239 приказов ФСТЭК. Должно осуществляться планирование мероприятий по обеспечению безопасности и контроль выполнения плана.

03

Подключение к ГосСОПКА
Должно быть выполнено подключение к ГосСОПКА и организовано взаимодействие в части информирования о компьютерных инцидентах и принятых мерах по ликвидации последствий компьютерных атак.

04

Выполнение требований 250 Указа и ПП №1272
- о заместителе руководителя по обеспечению безопасности;
- о структурном подразделении по безопасности;
- в части квалификационных требований.

05

Выполнение требований ПП №127
- в части соблюдения правил категорирования;
- в части соблюдения сроков предоставления информации.

На что следует обратить внимание (#2):

06

Создание и вывод из эксплуатации объектов КИИ
Процессы создания новых и вывода из эксплуатации существующих объектов критической информационной инфраструктуры должны соответствовать требованиям 239 приказа.

07

Переход на использование отечественных СЗИ
Переход на отечественные СЗИ должен быть завершен до конца текущего года. Использование СЗИ, не обеспеченных поддержкой производителя (даже если только на территории РФ), в том числе встроенных в прикладное и системное ПО, является нарушением требований п.21 235 приказа и п. 31 239 приказов.
Использование неподдерживаемых СЗИ не может рассматриваться как компенсирующая мера!

08

Обучение персонала
- должно осуществляться на регулярной основе и обеспечивать достаточный уровень знаний и навыков безопасной работы;
- персонал должен быть ознакомлен с ОРД по безопасности;
- должны проводиться тренировки по действиям в нештатных ситуациях и при компьютерных инцидентах.

09

Обеспечение физической безопасности
Должна быть определена контролируемая зона, для которой должны выполняться основные меры физической защиты, такие как пропускной режим, фиксация выдачи ключей от помещений и шкафов, СКУД, видеонаблюдение, опечатывание корпусов и неиспользуемых интерфейсов и т.д.

10

Достаточность мер по обеспечению безопасности
Оценка достаточности мер по обеспечению безопасности должна проводиться на постоянной основе и учитывать появление новых угроз.
В качестве основных инструментов могут использоваться:
- анализ архитектурно-технических решений с учетом актуальных угроз и потенциала нарушителя;
- проведение инструментального контроля;
- проведение внешних аудитов и пентестов.

Спасибо за внимание!