**Совет депутатов Вачского муниципального округа Нижегородской области**

# РАСПОРЯЖЕНИЕ

от 27.01.2023 г. № 22-х

О назначении ответственных за выявление инцидентов информационной безопасности и реагирование на них в Совете депутатов Вачского муниципального округа Нижегородской области

В целях обеспечения безопасности защищаемой информации, не содержащей сведения, в целях выполнения требований приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»:

1. Назначить ответственными за выявление инцидентов информационной безопасности и реагирование на них в Совете депутатов Вачского муниципального округа Нижегородской области (далее – Совет депутатов):

- Специалиста 1 категории администрации Вачского муниципального округа Нижегородской области (по согласованию) – Калинину Ирину Владимировну;
- Начальника отдела Совета депутатов – Антонову Наталью Владимировну.

2. Утвердить Регламент выявления инцидентов информационной безопасности и реагирования на них в Совете депутатов, в соответствии с приложением 1 к настоящему распоряжению.

3. Настоящее распоряжение вступает в силу со дня его подписания.

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Председатель Совета депутатов С.Е. Липов

С распоряжением ознакомлен: специалист 1 категории Калинина И.В. _____

С распоряжением ознакомлен: начальник отдела Антонова Н.В. _____

Приложение
к распоряжению Совета депутатов
Вачского муниципального округа
Нижегородской области
от 27.01.2023 года № 22-х

**Регламент**
**выявления инцидентов информационной безопасности и реагирования на них в Совете депутатов Вачского муниципального округа Нижегородской области**

Настоящий Регламент устанавливает порядок действий по управлению инцидентами информационной безопасности в Совете депутатов Вачского муниципального округа Нижегородской области (далее – Совет депутатов).

Под инцидентом информационной безопасности (далее – инцидент) понимается событие или совокупность событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

В качестве источников информации об инцидентах могут использоваться: журналы и оповещения системного и прикладного программного обеспечения информационных систем, обрабатывающих защищаемую информацию, не содержащую сведения, составляющие государственную тайну (далее ИС);

- журналы и оповещения системы защиты информации (далее СЗИ);
- оповещения средств обнаружения вторжений;
- информация, получаемая от сотрудников администрация;
- информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

При обнаружении инцидента сотрудник, ответственный за выявления инцидентов информационной безопасности и реагирование на них в администрация (далее – Ответственный за управление инцидентами) должен оповестить ответственного за обеспечение безопасности персональных данных и за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах администрация (далее – Ответственный за обеспечение безопасности защищаемой информации).

Ответственный за управление инцидентами должен провести анализ инцидента информационной безопасности в целях выявления факта или предпосылки негативного воздействия на защищаемую информацию, не содержащую сведения, составляющие государственную тайну (далее – защищаемая информация). В ходе анализа инцидента по возможности следует выявить следующие показатели:

- факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее – угрозы);
- опасность угрозы;
- области, перечни информационных ресурсов, затрагиваемые воздействием угрозы;
- потенциальные нарушители, цели и причины реализации угрозы;
- перечень мер по локализации и остановке распространения действия угрозы.

Ответственный за управление инцидентами оповещает Ответственного за обеспечение безопасности защищаемой информации о ходе и результатах реагирования на инциденты.

Ответственный за управление инцидентами составляет предложения Ответственному за обеспечение безопасности защищаемой информации о недопущении повторных инцидентов. При необходимости Ответственный за обеспечение безопасности защищаемой информации обеспечивает реализацию данных предложений.