



АГЕНТСТВО ПО ДОРОЖНОМУ ХОЗЯЙСТВУ РЕСПУБЛИКИ ДАГЕСТАН

ГКУ РД «ДОРОЖНЫЙ КОНТРОЛЬ»

П Р И К А З

«06» июня 2017 г.

№ 26

г. Махачкала

О сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них в ГКУ РД «Дорожный контроль»

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», **п р и к а з ы в а ю :**

1. Утвердить перечень сотрудников, ответственных за выявление инцидентов информационной безопасности и реагирование на них в ГКУ РД «Дорожный контроль» (Приложение № 1).
2. Утвердить регламент выявления инцидентов информационной безопасности и реагирование на них в ГКУ РД «Дорожный контроль» (Приложение № 2).
3. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель

Т.М. Азаев

Перечень сотрудников, ответственных за выявление инцидентов информационной безопасности и реагирование на них
в ГКУ РД «Дорожный контроль»

№ п/п	ФИО сотрудника	Должность
1.	Бутаев Герман Нурудинович	Ведущий инженер отдела информационных технологий ГКУ РД «Дорожный контроль»

Регламент выявления инцидентов информационной безопасности и реагирование на них в ГКУ РД «Дорожный контроль»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент устанавливает порядок действий по управлению инцидентами информационной безопасности в государственном казенном учреждении Республики Дагестан «Дорожный контроль» (далее – Учреждение).

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

2. ПОРЯДОК ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ

2.1. 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 Министерства;
- информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

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

2.3. 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.

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

2.5. 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.

**Лист ознакомления
с Регламентом выявления инцидентов информационной безопасности и реагирование на
них в ГКУ РД «Дорожный контроль»**

№ п/п	Ф.И.О.	Должность	Дата	Подпись
1.	Бугаев Г.Н.	Ведущий инженер ОИТ	06.07.07г.	