



ДЕРЖАВНА РЕГУЛЯТОРНА СЛУЖБА УКРАЇНИ

НАКАЗ

від _____ 2024

Київ

№ _____

Про внесення змін до наказу ДРС від 02.12.2022
№ 209 «Про затвердження Переліку відомостей,
що становлять службову інформацію
у Державній регуляторній службі України»
(зі змінами)

Відповідно до вимог постанови Кабінету Міністрів України від 19.10.2016
№ 736 «Про затвердження Типової інструкції про порядок ведення обліку,
зберігання, використання і знищення документів та інших матеріальних носіїв
інформації, що містять службову інформацію» (зі змінами) та з метою
оптимізації Переліку відомостей, що становлять службову інформацію у
Державній регуляторній службі України,

НАКАЗУЮ:

1. Доповнити Перелік відомостей, що становлять службову інформацію у
Державній регуляторній службі України (далі - ДРС), затверджений наказом
ДРС від 02.12.2022 № 209 (зі змінами), новими пунктами:

« 13. Технічний захист інформації.

13.1. Відомості про планування, організацію запровадження заходів,
фактичний стан, наявність недоліків в організації захисту інформації щодо
окремого об'єкта інформаційної діяльності, інформаційної, електронної
комунікаційної, інформаційно-комунікаційної системи, де циркулює (або
передбачена циркуляція) інформація, вимога щодо захисту якої встановлена
законодавством, крім тих, що становлять державну таємницю.

13.2. Відомості про зміст заходів, склад засобів комплексу технічного
захисту інформації або комплексної системи захисту інформації, призначених
для захисту інформації, вимога щодо захисту якої встановлена законодавством
(крім тих, що становлять державну таємницю), на конкретному об'єкті
інформаційної діяльності або в конкретній інформаційній (автоматизованій),
електронній комунікаційній чи інформаційно-комунікаційній системі.

13.3. Відомості про організацію та аналіз заходів оцінки стану захищеності державних інформаційних ресурсів в інформаційних (автоматизованих), електронних комунікаційних чи інформаційно-комунікаційних системах, а також про результати цієї оцінки та результати державної експертизи у сфері технічного захисту інформації, крім тих, що становлять державну таємницю.

13.4. Відомості про взаємодію із суб'єктами владних повноважень, військовими формуваннями, підприємствами, установами та організаціями незалежно від форм власності з питань організації технічного захисту інформації, вимога щодо захисту якої встановлена законом, крім тих, що становлять державну таємницю.

13.5. Відомості про організацію заходів щодо створення комплексної системи захисту інформації в інформаційних (автоматизованих), електронних комунікаційних чи інформаційно-комунікаційних системах, що містяться у протоколах, звітах, підготовлених та оформлених за результатами нарад і зустрічей з представниками органів державної влади, підприємств, установ.

13.6. Відомості про склад та структуру, результати державної експертизи комплексних систем захисту інформації в інформаційно-комунікаційних системах, заходи, які здійснюються при її проведенні, способи (методи) і порядок проведення цих заходів, що містяться в матеріалах державних експертиз у сфері технічного захисту інформації (що не становить державної таємниці), а також узагальнені відомості щодо виданих/зареєстрованих атестатів відповідності комплексних систем захисту інформації в інформаційнокомунікаційних системах вимогам нормативних документів.

13.7. Відомості про зміст проектів нормативно-правових актів і нормативних документів у сфері технічного захисту інформації, а також матеріалів, що їх супроводжують у процесі розроблення до затвердження документів і введення їх в дію, якщо необхідність цього визнана розробником.

14. Криптографічний захист інформації.

14.1. Відомості (за окремими показниками) про: зміст, стан, наявність недоліків в організації чи забезпеченні безпеки, плани розвитку системи криптографічного захисту службової інформації, порядок застосування (роботи) засобів криптографічного захисту службової інформації, результати розробки, виробництва, досліджень та експлуатації цих засобів і порядок забезпечення режиму безпеки під час їх проведення, крім тих, що становлять державну таємницю.

14.2. Відомості про взаємодію з органами державної влади, підприємствами, установами та організаціями у сфері криптографічного захисту службової та секретної інформації, якщо ці відомості не становлять державної таємниці.

14.3. Відомості про порядок використання, поводження, технічні характеристики ключових документів до засобів криптографічного захисту службової інформації.

14.4. Відомості про криптографічні системи або засоби криптографічного захисту службової інформації, якщо вони розкривають їх криптографічну схему (схему захисту, принципи побудови або криптографічні параметри).

14.5. Відомості про номенклатуру, кількість засобів криптографічного захисту службової інформації, місця їх розташування.

14.6. Відомості про номенклатуру, тактико-технічні характеристики засобів криптографічного захисту секретної інформації, якщо ці відомості не становлять державної таємниці.

14.7. Відомості (зміст, структура та повна назва) про нормативно-правові акти та нормативні документи з питань криптографічного захисту секретної та службової інформації, якщо ці відомості не становлять державної таємниці.

14.8. Відомості про особливості схемотехнічної та конструктивної побудови, криптографічні та спеціальні вимоги, механізми захисту та системи блокування, які наведено у відомчих нормативно-правових актах, нормативних документах з питань криптографічного захисту службової інформації.

14.9. Відомості про порядок, програми, методики, протоколи та звіти тематичних досліджень засобів спеціального зв'язку, засобів криптографічного захисту службової та секретної інформації, якщо вони не становлять державної таємниці.

14.10. Відомості про стан, планування, організацію і здійснення контролю за станом криптографічного захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законодавством, якщо ці відомості не становлять державної таємниці.

15. Кіберзахист.

15.1. Відомості про планування, організацію запровадження та зміст заходів, фактичний стан, наявність недоліків в організації кіберзахисту, а також рекомендації щодо підвищення рівня кіберзахисту.

15.2. Відомості про структуру та склад програмних та апаратних компонентів об'єкта інформаційної інфраструктури, їх налаштування, порядок взаємодії, журнали реєстрації подій (логи) компонентів об'єкта інформаційної інфраструктури, виявлення, запобігання, припинення кібератак та кіберінцидентів, а також усунення їх наслідків. »

2. Управлінню комунікацій та міжнародного співробітництва забезпечити оприлюднення цього наказу на офіційному вебсайті ДРС.

3. Контроль за виконанням цього наказу залишаю за собою.

**Голова Державної регуляторної
служби України**

Олексій КУЧЕР