НАЦІОНАЛЬНЕ АГЕНТСТВО З ПИТАНЬ ЗАПОБІГАННЯ КОРУПЦІЇ

НАКАЗ

02.04.2020 № 127/20

Зареєстровано в Міністерстві юстиції України
22 квітня 2020 р.
за № 370/34653

Про затвердження Вимог до захисту анонімних каналів зв'язку, через які здійснюються повідомлення про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України «Про запобігання корупції»

Відповідно до пункту 10 частини першої статті 7, пункту 5 частини першої статті 12, частини четвертої статті 53 Закону України «Про запобігання корупції» **НАКАЗУЮ:**

1. Затвердити Вимоги до захисту анонімних каналів зв'язку, через які здійснюються повідомлення про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України «Про запобігання корупції», що додаються.

2. Департаменту запобігання та виявлення корупції подати в установленому порядку цей наказ на державну реєстрацію до Міністерства юстиції України.

3. Контроль за виконанням цього наказу залишаю за собою.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова	**О. Новіков**
ПОГОДЖЕНО: Голова Державної служби спеціального зв'язку та захисту інформації України Заступник Міністра цифрової трансформації України	 В. Петров Л. Рабчинська

	ЗАТВЕРДЖЕНО **Наказ Національного агентства з питань запобігання корупції** **02 квітня 2020 року № 127/20**
	Зареєстровано в Міністерстві юстиції України **22 квітня 2020 р.** **за № 370/34653**

ВИМОГИ
до захисту анонімних каналів зв'язку, через які здійснюються повідомлення про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України«Про запобігання корупції»

I. Загальні положення

1. Ці Вимоги визначають умови створення та функціонування захищених анонімних каналів зв'язку, через які здійснюються повідомлення про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону України «Про запобігання корупції» (далі - Закон), та які застосовуються спеціально уповноваженими суб'єктами у сфері протидії корупції, державними органами, органами влади Автономної Республіки Крим, органами місцевого самоврядування, юридичними особами публічного права та юридичними особами, зазначеними у частині другій статті 62 Закону.

2. У цих Вимогах терміни вживаються у таких значеннях:

анонімний канал зв'язку - канали онлайн-зв'язку, анонімні гарячі лінії, електронні поштові скриньки та інші канали зв'язку, через які викривач може повідомити інформацію про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону;

повідомлення - повідомлення про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень Закону, отримане через анонімні канали зв'язку;

оператор - посадова або службова особа установи, яка приймає та/або розглядає повідомлення;

установа - спеціально уповноважений суб'єкт у сфері протидії корупції, державний орган, орган влади Автономної Республіки Крим, орган місцевого самоврядування, юридична особа публічного права та юридична особа, зазначена у частині другій статті 62 Закону.

II. Типи захищених анонімних каналів зв'язку

1. Типи захищених анонімних каналів зв'язку:

канал отримання повідомлень із використанням офіційного вебсайту установи;

канал отримання повідомлень із використанням електронних поштових скриньок;

канал отримання голосових повідомлень із використанням технології IP-телефонії (анонімна гаряча лінія);

канал отримання голосових повідомлень із використанням телефонної мережі загального користування (анонімна гаряча лінія).

III. Організаційні засади забезпечення захисту анонімних каналів зв'язку

1. Захист анонімних каналів зв'язку здійснюється шляхом побудови інформаційно-телекомунікаційної системи (далі - ІТС) із застосуванням комплексної системи захисту інформації, що має забезпечувати конфіденційність та гарантувати анонімність особи, яка здійснює повідомлення. Комплексна система захисту інформації повинна мати атестат відповідності.

2. ІТС складається із таких систем:

система отримання повідомлень із використанням офіційного вебсайту установи;

система отримання повідомлень з використанням електронної поштової скриньки;

система отримання голосових повідомлень (анонімна гаряча лінія) на основі технології IP-телефонії.

3. У разі використання телефонної мережі загального користування для лінії фіксованого телефонного зв'язку в межах зони нумерації (місцевий телефонний зв'язок) установа забезпечує виділення окремих телефонних апаратів, які повинні бути розміщені у спеціально виділеному приміщенні. Доступ до таких телефонних апаратів повинні мати лише оператори.

4. У системах ІТС не повинні застосовуватися функції моніторингу дій та ідентифікації особи, яка здійснила повідомлення. В документації на ІТС повинно бути визначено перелік інформації, що зберігається в ІТС, щодо особи, яка здійснила повідомлення.

5. Ідентифікація, автентифікація та авторизація операторів здійснюється з використанням персонального логіна та пароля або кваліфікованого електронного підпису. Дії оператора з даними ІТС та відвідування ним ІТС підлягають моніторингу. Якщо установа використовує мережу телефонного зв'язку загального користування, ідентифікація, автентифікація та авторизація операторів не здійснюється.

Керівник Департаменту запобігання та виявлення корупції	**С. Деркач**