ЗАТВЕРДЖЕНО
Наказ Держкомтелерадіо
20 січня 2025 року № 6
(в редакції від __ ___2026 року №_)

ПЛАН
заходів з кіберзахисту інформаційно-комунікаційної системи Державного комітету телебачення і радіомовлення України

1. План реагування на кібератаки/кіберінциденти

№ з/п	Етап	Опис
1.	Виявлення інциденту	Моніторинг систем, мереж та програмного забезпечення для своєчасного виявлення підозрілих дій або порушень
2.	Аналіз і класифікація	Збір та аналіз даних для визначення характеру, джерела та масштабу інциденту. Встановлення його критичності та потенційного впливу на організацію
3.	Ізоляція та стримування	Обмеження поширення інциденту шляхом ізоляції уражених систем, блокування шкідливого трафіку або облікових записів
4.	Усунення наслідків	Видалення шкідливого програмного забезпечення, відновлення систем із резервних копій, усунення вразливостей та відновлення нормального функціонування
5.	Розслідування	Проведення глибокого аналізу для визначення причин інциденту, шляхів його виникнення та відповідальних осіб. Документування зібраної інформації
6.	Повідомлення	Інформування керівництва організації, відповідних державних органів (наприклад, CERT-UA) та, за необхідності, зацікавлених сторін або постраждалих осіб
7.	Підвищення рівня захисту	Аналіз отриманого досвіду, оновлення політик безпеки, впровадження додаткових технічних засобів захисту та навчання для запобігання подібним інцидентам

2. План кіберзахисту ІКС Держкомтелерадіо за класом «Ідентифікація ризиків кібербезпеки» (ID)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
1.	Провести ідентифікацію інформаційних, програмних та апаратних ресурсів (програмних та апаратних компонентів, змінних (зовнішніх) пристроїв та носіїв інформації тощо)	Реалізовано частково. Ідентифіковано пристрої в ІКС Держкомтелерадіо та програмне забезпечення	Провести інвентаризацію програмних та апаратних засобів	відділ документообігу, контролю та цифрового розвитку	щороку	За результатами аналізу виявити та видалити апаратне та програмне забезпечення, що не використовується
2.	Аналіз вразливостей	Реалізовано частково. Проведено оцінку вразливостей ІКС Держкомтелерадіо	Виконувати оцінку вразливостей у системах та мережах	відділ документообігу, контролю та цифрового розвитку	постійно	Провести аналіз відкритих портів, визначити приналежність доступних сервісів та заблокувати/обмежити доступ до непотрібних мережевих служб
3.	Зменшення поверхні атаки	Реалізовано частково. Використовується ліцензійне програмне забезпечення	Видалення застарілого та неліцензійного програмного забезпечення	відділ документообігу, контролю та цифрового розвитку	постійно	Деінсталяція неліцензійного програмного забезпечення, заміна на безкоштовні аналоги за потреби
4.	Управління доступом	Реалізовано частково. Впроваджено	Впровадити використання механізмів для	відділ документообігу,	постійно	Обмежити функціональні можливості браузера для

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
		механізми розмежування доступу	розмежування доступу на основі рольової моделі (RBAC), надаючи права користувачам за принципом найменших привілеїв	контролю та цифрового розвитку		зберігання даних автентифікації, доступ до панелі управління та мережевих налаштувань на робочих станціях
5.	Контроль за використанням мережевих ресурсів	Реалізовано частково. Посилено політики контролю доступу до мережевих ресурсів	Посилити захист ІКС Держкомтелерадіо та запобігання ризикам витоку конфіденційної інформації	відділ документообігу, контролю та цифрового розвитку	постійно	Заборонити використання зовнішніх VPN-сервісів на робочих станціях, сервісних налаштувань, інсталяцію додатків, плагінів, розширень у веб браузерах для запобігання несанкціонованому доступу до ІКС
6.	Захист даних	Реалізовано частково. Організовано централізоване резервування інформаційних активів	Забезпечити централізоване резервування даних на окремих фізичних носіях, періодично тестувати бекапи на справність	відділ документообігу, контролю та цифрового розвитку	постійно	Резервне копіювання даних забезпечує їх збереження у випадку втрати
7.	Захист мережі	Реалізовано частково. Вжито заходи захисту мережі від сторонніх проникнень і кібератак	ІКС захищено від стороннього проникнення, забезпечено протидію різним атакам на мережеву інфраструктуру	відділ документообігу, контролю та цифрового розвитку	постійно	Оновлення правил для маршрутизації трафіку
8.	Захист кінцевих	Реалізовано частково.	Організувати захист та	відділ	постійно	Моніторинг та аналіз

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
	точок	Використовується актуальна версія ліцензійного антивірусного програмного забезпечення	оновлення антивірусного програмного забезпечення на кінцевих пристроях ІКС Держкомтелерадіо	документообігу, контролю та цифрового розвитку		подій на робочих станціях, серверах антивірусним програмним забезпеченням, налаштування автоматичного виявлення та блокування підозрілої активності
9.	Моніторинг систем	Реалізовано частково. Налаштовано моніторинг мережевого трафіку	Проведення аналізу мережевих з'єднань	відділ документообігу, контролю та цифрового розвитку	постійно	Виявлення та сповіщення про аномальну активність трафіку в ІКС Держкомтелерадіо
10.	Забезпечити підключення ІКС Держкомтелерадіо до державних систем виявлення та обміну інформацією про кіберінциденти	Реалізовано частково. З 2024 року в установленому порядку налагоджено інформаційну взаємодію з національними суб’єктами у сфері кібербезпеки, зокрема з CERT-UA, а також здійснюється обмін інформацією з використанням платформи MISP-UA	Розширення функціоналу взаємодії та забезпечення інтеграції з адаптованими програмними продуктами (платформою MISP-UA, системами управління подіями інформаційної безпеки (SIEM)) відповідно до постанови Кабінету Міністрів України від 26.11.2025 № 1533.	відділ документообігу, контролю та цифрового розвитку	постійно	З метою виявлення кіберзагроз у режимі реального часу та обміну інформацією

3. План кіберзахисту за класом «Кіберзахист» (PR)

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
1.	Забезпечити використання надійних паролів	Реалізовано частково. Впроваджена політика використання паролів	Зміна паролів не рідше 1 разу на 6 місяців	відділ документообігу, контролю та цифрового розвитку	постійно	Встановлені базові вимоги до складності паролів.
2.	Затвердити процедуру вчасного видалення облікових записів звільнених працівників	Реалізовано частково. Базова процедура видалення записів функціонує	Своєчасне видалення облікових записів звільнених працівників	відділ документообігу, контролю та цифрового розвитку	постійно	Своєчасне видалення або блокування облікових записів у встановлений термін після звільнення працівника
3.	Унеможливити отримання зловмисником прав доступу до привілейованих облікових даних адміністраторів або користувачів	Реалізовано частково. Впроваджено основні засоби захисту адміністративних облікових записів	Посилити контроль доступу до критичних систем	відділ документообігу, контролю та цифрового розвитку	постійно	Впровадження додаткових заходів контролю привілейованого доступу

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
4.	Здійснити розподіл мережі на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту	Реалізовано частково базову сегментація мережі	Налаштувати міжмережеві екрани для мінімізації ризиків	відділ документообігу, контролю та цифрового розвитку	постійно	Оновлення мережевого обладнання та правил маршрутизації
5.	Забезпечити виявлення невдалих спроб входу в систему та перевищення граничної кількості спроб введення пароля	Реалізовано частково. Обмежено кількість спроб входу в СЕД	Налаштувати автоматичне блокування	відділ документообігу, контролю та цифрового розвитку	постійно	Блокування доступу до СЕД у разі перевищення граничної кількості спроб

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
6.	Забезпечити криптографічний та технічний захист, кібербезпеку, кіберзахист та безпеку інформаційних технологій, а також здійснювати контроль за їх станом в апараті Держкомтелерадіо	Реалізовано частково	Постійний контроль за станом КЗІ, ТЗІ, оновлення засобів захисту, перевірка відповідності вимогам законодавства	відділ документообігу, контролю та цифрового розвитку	постійно	Здійснюється відповідно до вимог законодавства у сфері технічного та криптографічного захисту інформації, нормативних документів Адміністрації Держспецзв’язку та внутрішніх організаційно-розпорядчих документів Держкомтелерадіо

4. План заходів із забезпечення авторизації з безпеки ІКС та сертифікації відповідності

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
1.	Розробка цільового профілю безпеки ІКС Держкомтелерадіо	Не реалізовано	Розроблення проєкту цільового профілю безпеки ІКС Держкомтелерадіо на основі базового профілю, формування моделі загроз, визначення вимог безпеки	відділ документообігу, контролю та цифрового розвитку	I–II квартал 2026 року	Розроблення цільового профілю безпеки здійснюється на основі базового профілю безпеки системи, де обробляється відкрита

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
			та підготовка організаційно-розпорядчих документів			або конфіденційна інформація, затвердженого наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409, відповідно до Порядку авторизації з безпеки ІКС, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 р. № 712.
2.	Підготовка ІКС до проходження процедури авторизації	Не реалізовано	Реалізація організаційних та технічних заходів відповідно до затвердженого цільового профілю безпеки, проведення внутрішньої оцінки відповідності встановленим вимогам, усунення виявлених невідповідностей та організаційне забезпечення підготовки пакета документів для подання до органу оцінки відповідності	відділ документообігу, контролю та цифрового розвитку	II–III квартал 2026 року	Здійснюється у взаємодії з уповноваженими суб'єктами у сфері технічного та криптографічного захисту інформації

№ з/п	Завдання із кіберзахисту	Поточний стан виконання завдання (реалізовано/не реалізовано) та наявні ресурси	Заплановані заходи для виконання (реалізації) завдання	Відповідальні за виконання	Запланований термін виконання	Примітки (потреба у реалізації, проблемні питання, деталі реалізації тощо)
3.	Проходження процедури сертифікації та отримання сертифіката відповідності	Не реалізовано	Подання пакета документів до органу оцінки відповідності та організаційне забезпечення проходження процедури сертифікації відповідно до вимог законодавства	відділ документообігу, контролю та цифрового розвитку	III квартал 2026 року	Сертифікація здійснюється акредитованим органом оцінки відповідності
4.	Підтримання статусу авторизованої ІКС	Не реалізовано	Моніторинг відповідності встановленим вимогам безпеки, актуалізація документації, організаційне забезпечення проходження планових та позапланових перевірок	відділ документообігу, контролю та цифрового розвитку	постійно	Виконується відповідно до Порядку авторизації з безпеки ІКС (постанова КМУ № 712) та з урахуванням періодичності перевірок, визначених законодавством