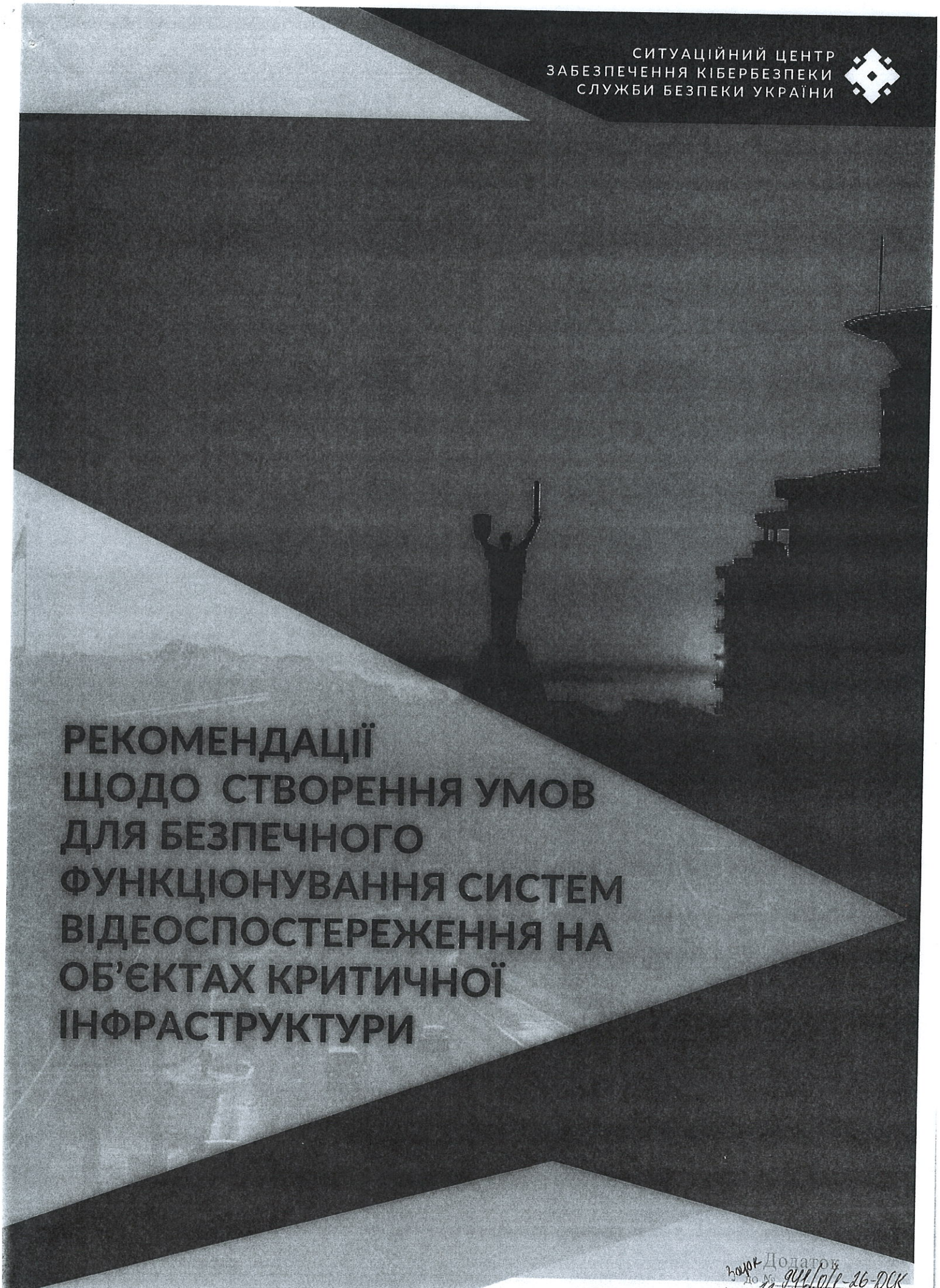
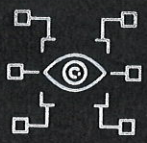
СИТУАЦІЙНИЙ ЦЕНТР
ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ
СЛУЖБИ БЕЗПЕКИ УКРАЇНИ



РЕКОМЕНДАЦІЇ ЩОДО СТВОРЕННЯ УМОВ ДЛЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



Етап побудови системи відеоспостереження на об'єкті критичної інфраструктури

1. Створити локальну мережу, фізично відокремлену від усіх інших систем та мереж об'єкту. Склад: камери відеоспостереження (за можливості уникати приладів китайського виробництва), DVR/NVR/VMS пристрої, Firewall з функцією VPN. Альтернативою може бути використання хмарних сервісів.
2. У разі віддаленого розміщення камер відеоспостереження та відсутності можливості організувати фізичні канали зв'язку або через Wi-Fi мережу доцільним є використання транспортних каналів мобільних операторів з локальною адресацією (GRE тунелі).
3. Адміністрування DVR/NVR/VMS пристроїв та доступ до камер відеоспостереження для перегляду відеоматеріалів має відбуватися лише з виокремлених операторських місць, розміщених в тій самій локальній мережі. Створення Video Management System (VMS) може забезпечити централізований доступ до камер та одночасно розмежування прав доступу до перегляду камер відеоконтенту.
4. Сховище для зберігання архівних відео повинно бути заведене в окрему локальну мережу, доступ до якої повинен бути лише в режимі перегляду. Адміністрування серверу здійснювати локально.
5. Доступ до DVR/NVR/VMS для перегляду камерам заборонити з мережі Інтернет напряму. Встановити окремий маршрутизатор з функціями фаєрволу, що буде фільтрувати доступ користувачів та термінувати їх до DVR/NVR/VMS пристроїв. У тому числі має бути впроваджено механізм 2FA авторизації. У разі можливості, організувати site-to-site VPN тунель між інфраструктурою об'єкту критичної інфраструктури та зацікавленими у отриманні доступу суб'єктом.
6. Налаштувати перелік пристроїв, що мають доступ до DVR/NVR/VMS за MAC адресою. Змінити впровадженні за умовчанням паролі на всіх пристроях та камерах, а також стандартні порти доступу за відомими протоколами. Доступ до камер та DVR/NVR/VMS, у тому числі GUI, має відбуватися за захищеними протоколами з шифруванням даних.
7. Впровадити логування підключень до DVR/NVR/VMS, закрити всі відкриті порти, що не використовуються, за можливості впровадити перелік білих IP адрес для підключення до Firewall, використання сильних паролів, що містять від 12 символів (великі і малі літери, цифри, спеціальні символи).

Етап експлуатації системи відеоспостереження на об'єкті критичної інфраструктури

1. Оновлення старих версій програмного забезпечення, яке використовується для функціонування DVR/NVR/VMS та камер-відеоспостереження. Виведення з експлуатації непідтримуваних виробниками пристроїв.
2. Систематична зміна паролів всім обліковим записам користувачів, у тому числі з адміністративними правами (наприклад 1 раз на 45 днів).
3. Постійний контроль та розмежуванням привілейованих облікових записів, сервісних та звичайних з правами користувача, у тому числі контроль за створенням нових облікових записів, зокрема локальних, та блокування/видалення облікових записів, які не використовуються.
4. Організовувати систематичні (наприклад 1 раз на рік) перевірки на предмет наявності вразливостей (пентестінг) системи відеоспостереження.
5. Відслідковувати та впроваджувати рекомендації виробників DVR/NVR/VMS пристроїв та камер з посилення рівня захищеності.