Література

1. Tirulo A., Chauhan S., Shafie-khah M. LLM-Powered Threat Intelligence: Proactive Detection of Zero-Day Attacks in Electric Vehicle Cyber-Physical Systems. Sustainable Energy, Grids and Networks. 2025. P. 101877. URL: https://doi.org/10.1016/j.segan.2025.101877 (date of access: 06.10.2025).
2. Cybersecurity in vehicle-to-grid (V2G) systems: A systematic review / M. A. Razzaque et al. Applied Energy. 2025. Vol. 398. P. 126364. URL: https://doi.org/10.1016/j.apenergy.2025.126364 (date of access: 06.10.2025).
3. A Comprehensive Review of Vehicle-to-Grid (V2G) Technology as an Ancillary Services Provider / S. Alamgir et al. Results in Engineering. 2025. P. 106813. URL: https://doi.org/10.1016/j.rineng.2025.106813 (date of access: 06.10.2025).
4. xCarbon. VicOne. URL: https://vicone.com/products/xcarbon (date of access: 06.10.2025).

УДК 656.1.078:004.056

СУБ'ЄКТИ ПРОВЕДЕННЯ ОБОВ'ЯЗКОВОГО ТЕХНІЧНОГО КОНТРОЛЮ ТРАНСПОРТНИХ ЗАСОБІВ: СУТНІСТЬ ТА ОСОБЛИВОСТІ ДОТРИМАННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Віштак Інна Вікторівна, канд. техн. наук, доцент кафедра БЖДПБ,
Вінницький національний технічний університет,
e-mail: innavish322@gmail.com, ORCID: 0000-0001-5646-4996
Майданевич Леонід Олександрович, адвокат, канд. філос. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет,
e-mail: lmaidanevych@gmail.com, ORCID: 0000-0002-7364-8874

Актуальність теми роботи пов'язана з тим, що забезпечення технічного захисту інформації в інформаційно-комунікаційних системах суб'єктів проведення обов'язкового технічного контролю транспортних засобів є ключовою умовою дотримання вимог законодавства України у сфері безпеки дорожнього руху та цифрової безпеки. Недотримання встановлених стандартів призводить до ризику несанкціонованого доступу, втрати або викривлення даних про результати технічного контролю, що негативно впливає на функціонування Єдиного державного реєстру транспортних засобів та підриває довіру до державної системи контролю. У контексті цифрової трансформації та зростання кіберзагроз дана проблема набуває особливої актуальності.

Метою дослідження є визначення основних вимог та розробка практичних рекомендацій щодо приведення робочих місць суб'єктів обов'язкового технічного контролю у відповідність до норм законодавства України у сфері технічного захисту інформації.

Об’єктом дослідження є процес організації та функціонування робочих місць суб’єктів обов’язкового технічного контролю транспортних засобів.

Предметом дослідження є правові, технічні та організаційні аспекти забезпечення технічного захисту інформації в інформаційно-комунікаційних системах, що використовуються суб’єктами обов’язкового технічного контролю.

Обов’язковий технічний контроль транспортних засобів, які зареєстровані в територіальних органах Міністерства внутрішніх справ України та призначені для використання в транспортній системі, проводять спеціалізовані суб’єкти. Такими суб’єктами проведення обов’язкового технічного контролю транспортних засобів є юридичні особи та/або фізичні особи – підприємці, відомості про яких внесені до загальнодержавної бази даних про результати обов’язкового технічного контролю транспортних засобів, яка є складовою частиною Єдиного державного реєстру транспортних засобів в Україні.

Основною вимогою до таких суб’єктів є: щоб такі суб’єкти мали у власності або користуванні обладнання, що забезпечує перевірку технічного стану транспортних засобів на відповідність вимогам безпеки дорожнього руху та екологічним нормам.

Також, згідно Порядку формування загальнодержавної бази даних про результати обов’язкового технічного контролю транспортних засобів, доступу до неї та встановлення розміру плати за надання таких послуг (затвердженого постановою Кабінету Міністрів України від 31.05.2012 року за №512) – суб’єкти проведення обов’язкового технічного контролю транспортних засобів зобов’язані дотримуватися щоб робоче місце відповідало вимогам законодавства, зокрема у сфері технічного захисту інформації в інформаційно-комунікаційних системах (п.10 Порядку формування бази даних №512) [1].

Невідповідність робочого місця суб’єкта проведення обов’язкового технічного контролю вимогам законодавства у сфері **технічного захисту інформації (ТЗІ)** в інформаційно-комунікаційних системах може проявлятися у таких основних формах:

1. *Відсутність атестованої системи захисту інформації* (інформаційно-комунікаційна система (ІКС), у якій ведеться облік, зберігання та передача даних про результати обов’язкового технічного контролю (ОТК), не має атестата відповідності комплексної системи захисту інформації (КСЗІ), що вимагається законодавством України);
2. *Недотримання режиму доступу та ідентифікації* (робочі місця не забезпечені механізмами персоніфікованого доступу (логіни, паролі, електронні ключі, сертифікати КЕП); можливість доступу сторонніх осіб до інформації без належних повноважень);
3. *Використання несертифікованого або забороненого ПЗ і технічних засобів* (застосування програмного забезпечення чи технічних засобів, які не пройшли державну експертизу або не включені до переліків, дозволених для використання в ІКС з обмеженим доступом);
4. *Відсутність захисту каналів зв’язку та обробки інформації* (передача даних до реєстрів або до інших органів здійснюється без криптографічного захисту

(шифрування, КЕП тощо); використання відкритих або ненадійних каналів зв'язку);
5. *Недотримання вимог до приміщення та фізичного захисту* (робочі місця з доступом до ІКС розташовані у приміщеннях без належного контролю доступу; відсутні заходи щодо недопущення витоку інформації технічними каналами (електромагнітне випромінювання, підключення сторонніх пристроїв);
6. *Відсутність або неналежне ведення обліку та контролю* (не ведеться журнал обліку доступу до ІКС і результатів перевірок; відсутні процедури регулярного контролю стану захисту інформації);
7. *Невиконання вимог нормативних документів Держспецзв'язку* (порушення положень Закону України «Про захист інформації в інформаційно-комунікаційних системах», а також нормативно-правових актів Держспецзв'язку (зокрема, НД ТЗІ, стандартів КСЗІ) [2].

Таким чином, *невідповідність робочого місця* суб'єкта ОТК вимогам ТЗІ може полягати як у відсутності формально-правових документів (атестата КСЗІ), так і в технічних чи організаційних недоліках (незахищені канали, сторонній доступ, несертифіковані засоби, порушення режиму.

Найпоширеніші порушення, які виявляють під час перевірок робочих місць суб'єктів проведення обов'язкового технічного контролю (ОТК) у сфері технічного захисту інформації (за практикою Держспецзв'язку та суміжних аудитів):

Таблиця 1 – Найпоширеніші порушення та можливі наслідки

Порушення	***Порушена норма***	***Можливі наслідки***
Відсутність атестата комплексної системи захисту інформації (КСЗІ)	Закон України «Про захист інформації в ІКС» (ст. 8, 9); НД ТЗІ 2.5-004-99	Визнання системи незахищеною; заборона доступу до державних реєстрів; призупинення діяльності як суб'єкта ОТК
Використання незахищених каналів зв'язку для передачі даних	Закон України «Про захист інформації в ІКС» (ст. 10); НД ТЗІ 2.5-010-03	Перехоплення або викривлення даних; витік службової інформації; блокування обміну з реєстрами
Використання несертифікованого ПЗ та обладнання	Постанова КМУ № 373 від 29.03.2006; вимоги Держспецзв'язку [3]	Порушення ліцензійних і ТЗІ-вимог; потенційне впровадження шкідливого ПЗ; штрафи, припис щодо заміни
Відсутність персоніфікованого доступу (спільні логіни/паролі)	Закон «Про захист інформації в ІКС» (ст. 8); НД ТЗІ 2.5-008-99	Неможливість ідентифікувати винних у витоку даних; підвищений ризик

		несанкціонованого доступу; відповідальність
Фізична незахищеність приміщень (вільний доступ сторонніх)	наказ Адміністрації Держспецзв'язку № 53; НД ТЗІ 2.5-010-03	Несанкціонований доступ до обладнання; крадіжка носіїв з даними; загроза припинення атестації
Відсутність захисту від технічних каналів витоку (ЕМВ, носії)	НД ТЗІ 2.5-004-99, 2.5-010-03	Витік даних через побічні випромінювання; санкції Держспецзв'язку, відмова в сертифікації
Неорганізоване ведення журналів доступу, відсутність моніторингу	НД ТЗІ 2.5-008-99; внутрішні інструкції	Неможливість відстеження інцидентів; підвищений ризик маніпуляцій з даними; штрафи
Відсутність внутрішніх інструкцій та навчання персоналу з питань ТЗІ	Закон «Про захист інформації в ІКС» (ст. 7); НД ТЗІ 2.5-004-99	Недотримання правил захисту; людський фактор як головна загроза; зростання кількості інцидентів

Висновки

Отже, такі порушення кваліфікуються як *невідповідність вимогам законодавства України у сфері ТЗІ* (Закон «Про захист інформації в ІКС», підзаконні акти Держспецзв'язку, НД ТЗІ).

З метою відповідності робочого місця суб'єкта ОТК *вимогам законодавства України у сфері ТЗІ* пропонується вчиняти такі дії:

1. Документи у сфері ТЗІ (має бути атестат про акредитацію, КЕП та інші дозвільні документи; розроблені та затвердженні внутрішні положення/інструкції з ТЗІ; персонал має пройти відповідне навчання, інструктаж з питань ТЗІ).
2. Доступ та автентифікація (це процес перевірки прав користувача перед роботою з інформаційною системою: Ідентифікація – користувач вводить свій унікальний ідентифікатор (логін, номер сертифіката, токен тощо); Автентифікація – система перевіряє справжність користувача за паролем, електронним підписом, токеном чи багатофакторним методом (наприклад, пароль + смс/додаток); Авторизація – надається доступ тільки до тих ресурсів і функцій, які дозволені конкретному користувачу згідно з його правами).

3. Програмні та апаратні засоби (використовувати тільки сертифіковане та ліцензійне ПЗ; антивірус та засоби захисту оновлювати регулярно; дотримуватися заборони встановлювати сторонні та/або піратські ПЗ).
4. Порядок передачі та зберігання даних (вся передача даних здійснюється з криптографічним захистом; архіви та резервні копії зберігати в захищеному місці; розробити план відновлення даних у разі збою/кіберінцидену тощо).
5. Фізичний захист (робоче місце має бути належно захищено з контролем доступу (замки, охорона, відеоспостереження тощо); заборона доступу сторонніх осіб до програмних та апаратних засобів робочого місця; мінімізувати можливість підключення несанкціонованих носіїв до апаратних засобів робочого місця).
6. Контроль та аудит (регулярно перевіряти стан системи захисту інформації; вести журнал інцидентів та порушень; призначити відповідальну особу за ТЗІ у суб'єкта ОТК).

Література

1. Кабінет Міністрів України. (2012, 31 травня). *Постанова № 512 «Про затвердження Порядку формування загальнодержавної бази даних про результати обов'язкового технічного контролю транспортних засобів, доступу до неї та встановлення розміру плати за надання таких послуг»*. Київ. https://zakon.rada.gov.ua/go/512-2012-%D0%BF .
2. Верховна Рада України. (1994, 5 липня). *Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР*. Відомості Верховної Ради України, 31, ст. 286. https://zakon.rada.gov.ua/go/80/94-вр .
3. Кабінет Міністрів України. (2006, 29 березня). *Постанова № 373 «Деякі питання діяльності Адміністрації Державної служби спеціального зв'язку та захисту інформації»*. Офіційний вісник України, 13, ст. 857. https://zakon.rada.gov.ua/go/373-2006-п .