навчання [електронне видання]. Х.: НТУ "ХПІ", 2024. Харків. 132 с. https://repository.kpi.kharkov.ua/handle/KhPI-Press/75508 .

УДК 004.056:339.543

ОБ'ЄКТИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ МИТНОГО ПОСТУ ТА СТУПЕНІ ЇЇ УШКОДЖЕННЯ

Віра Сокольцова

Дніпровський національний університет ім. Олеся Гончара, м. Дніпро, Україна

Науковий керівник: В. Ю. Клим,
канд.тех.наук, доцент
Дніпровський національний університет ім. Олеся Гончара

Після руйнівного впливу митний пост може повернутися до роботи лише тоді, коли відновлено його комплексну систему захисту інформації (КСЗІ). Будівлю й обладнання можна замінити, проте обробляти митні декларації, платежі та персональні дані без працездатної і перевіреної КСЗІ не можна. Тому відновлення митного посту доцільно розглядати насамперед як відновлення його КСЗІ.

Мета дослідження полягає в визначенні об’єктів КСЗІ та систематизації ступенів ушкодження для подальшого обґрунтування алгоритму відновлення КСЗІ митного посту після фізичного втручання (руйнівного впливу). Об’єктом дослідження є комплексна система захисту інформації митного посту. Предметом дослідження є засоби відновлення КСЗІ після фізичного руйнівного впливу.

Для досягнення поставленої мети насамперед було проаналізовано нормативно-правову базу України. Окремого акту, який регламентував би відновлення КСЗІ після фізичного руйнування, в Україні немає, тому дослідження спирається на кілька груп джерел. Базовим є Закон України «Про захист інформації в інформаційно-комунікаційних системах», який відносить до об’єктів захисту як інформацію, так і програмне забезпечення для її обробки, покладає відповідальність за захист на власника системи та вимагає обробляти державні інформаційні ресурси в системах із КСЗІ [1]. Митні пости працюють у Єдиній автоматизованій інформаційній системі Держмитслужби (ЄАІС) [2], а отже, підпадають під ці вимоги. Закон України «Про критичну інфраструктуру» доповнює їх вимогою забезпечувати стійкість об’єктів, порушення роботи яких впливає на безпеку держави [3]. З цих норм випливає ключова вимога: повернення посту до обробки інформації допустиме лише після відновлення і перевірки КСЗІ, а не одразу після ремонту обладнання.

Національні норми доповнюють міжнародні стандарти та настанови. Найбільше до теми дослідження стосуються контролі ISO/IEC 27001:2022 A.5.29 (безпека під час критичної події) [4] і A.7.1 (фізичні межі безпеки) [5]. Стандарти ISO 22301 і ISO 22313 вводять показники відновлення MTPD, MBCO, RTO та RPO [6], керівництва NIST SP 800-34 [7] і SP 800-61 Rev. 3 [8] описують планування відновлення інформаційних систем і реагування на інциденти, а Настанови Всесвітньої митної організації (ВМО) пропонують митним адміністраціям цикл «готовність – реагування – відновлення» [9]. Крім того, оскільки фізичний рівень КСЗІ залежить від стану споруд, враховано Порядок № 473 щодо невідкладних робіт з ліквідації наслідків пошкодження будівель [10] та порядок їх обстеження [11]: доки за результатами обстеження не прийнято рішення, повертати обладнання в пошкоджену серверну не можна.

Визначивши нормативні вимоги, необхідно встановити, що саме підлягає відновленню, тобто саме об’єкти КСЗІ. Оскільки фізичний вплив зачіпає різні об’єкти КСЗІ по-різному, тому основні інформаційні ресурси митного посту згруповано за структурними підрозділами, які з ними працюють безпосередньо. Для кожної групи визначено критичні властивості інформації (конфіденційність, цілісність, доступність, автентичність, які позначено відповідними буквами К, Ц, Д, А) та загрози, що виникають після фізичного втручання.

В таблиці 1 зведена інформація по об'єктах КСЗІ митного посту та загрозах для них після фізичного втручання. Аналіз таблиці 1 показує, що найбільш уразливими до фізичного впливу є інформаційний відділ і відділ комунікацій: для їхніх даних критичні всі три основні властивості – конфіденційність, цілісність і доступність.

Таблиця 1 Об'єкти КСЗІ митного посту та загрози їм після фізичного втручання

Підрозділ	**Дані / активи**	**Критичні властивості**	**Що загрожує після фізичного втручання**
Інформаційний відділ	Бази митних декларацій, електронні журнали перевірок, архіви платежів	К, Ц, Д	Недоступність ЄАІС, викрадення локальних копій
Архів	Електронні й паперові декларації, акти перевірок, протоколи порушень	Ц, А	Знищення вогнем, втрата, підміна документів
Відділ кадрів	Персональні дані співробітників	К	Витік через викрадені носії та паперові справи
ІТ-відділ	Сервери, робочі станції, мережеве обладнання, відеоспостереження	Д, Ц	Фізичне знищення, аварійне вимкнення, підміна або модифікація обладнання
Фінансовий відділ	Дані про митні платежі, штрафи, звіти	Ц, К	Втрата незавершених транзакцій, розбіжність даних
Оперативний відділ	Результати оглядів, дані про порушення митних правил	К, Ц	Витік відомостей про перевірки, втрата відеодоказів
Відділ комунікацій	Внутрішня мережа, захищені канали з центральними органами, ключі та сертифікати	К, Ц, Д	Розрив каналів, компрометація ключів, стороннє підключення

Інший характер мають загрози для відділу кадрів та оперативного відділу, де на перший план виходить конфіденційність. Основна небезпека тут полягає не в знищенні даних, а в їх витоку: через відкритий периметр, розбиті сейфи та викрадені носії сторонні особи можуть отримати персональні дані чи відомості про перевірки. Натомість для архіву й фінансового відділу вирішальною є цілісність, адже підміна документів, втрата незавершених транзакцій і розбіжність даних призводять до недостовірних результатів митного оформлення.

Отже, фізичне втручання загрожує не лише доступності інформації, як може здатися на перший погляд. Поки периметр і фізичний рівень захисту не працюють, а до приміщень мають доступ сторонні особи, перелік загроз значно ширший, ніж у штатному режимі. Ремонт і увімкнення обладнання без перевірки можуть повернути доступність, але залишать відкритими загрози конфіденційності та цілісності. Тому після інциденту КСЗІ слід вважати скомпрометованою, доки не доведено протилежне.

Щоб визначити обсяг необхідних відновлювальних заходів, ушкодження КСЗІ запропоновано класифікувати за чотирма ступенями. Критерієм класифікації є не обсяг руйнувань будівлі, а рівень довіри до засобів захисту, що залишилися.

І ступінь – незначне ушкодження. Пошкоджено скління або частину периметра, сталося коротке знеструмлення, приміщення з технікою не відкривалися. Довіра до засобів захисту збережена, тому достатньо перевірити цілісність даних і журнали подій та відновити периметр.

ІІ ступінь – середнє ушкодження. Частково виведено з ладу фізичний рівень захисту або мережу, сервери цілі. Довіра до засобів захисту часткова: відкриті приміщення перевіряються, а уражені рівні відновлюються на місці з використанням резервного каналу зв’язку.

ІІІ ступінь – значне ушкодження. Пошкоджено серверну або вузол зв’язку, КСЗІ не функціонує, техніка певний час залишалася без нагляду. Довіри до засобів захисту немає до завершення

перевірки, тому робота переноситься в тимчасовий захищений сегмент, відновлюються всі рівні захисту, а ключі замінюються.

IV ступінь – повне ушкодження. Об'єкт знищено або він тривалий час недоступний. Усі засоби захисту вважаються скомпрометованими, тому КСЗІ будується заново на новому обладнанні, а всі сертифікати посту відкликаються.

Визначені ступені ушкодження надалі становлять сукупність вихідних даних для побудови алгоритму відновлення КСЗІ.

Таким чином, відновлення митного посту після фізичного втручання є насамперед відновленням його КСЗІ, оскільки законодавство дозволяє обробляти державні інформаційні ресурси лише в системах із КСЗІ [1], і ремонт обладнання сам по собі не дає підстав відновити обробку даних. Аналіз об'єктів КСЗІ показав, що фізичний вплив загрожує всім трьом властивостям інформації, тому запропонована класифікація ступенів ушкодження ґрунтується на рівні довіри до засобів захисту, а не на обсязі руйнувань будівлі.

Список використаних джерел

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 09.10.2026).

2. Про затвердження Положення про Єдину автоматизовану інформаційну систему Держмитслужби України : наказ. URL: https://zakon.rada.gov.ua/rada/show/va341342-10 (дата звернення: 09.10.2026).

3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 09.10.2026).

4. ISO 27001:2022 Annex A 5.29 – Information Security During Disruption. ISMS.online. URL: https://www.isms.online/iso-27001/annex-a-2022/5-29-information-security-during-disruption-2022/ (дата звернення: 09.10.2026).

5. ISO 27001:2022 Annex A 7.1 – Physical Security Perimeters. ISMS.online. URL: https://www.isms.online/iso-27001/annex-a-2022/7-1-physical-security-perimeters-2022/ (дата звернення: 09.10.2026).

6. Key Definitions Used in ISO 22301 and ISO 22313. PECB. URL: https://pecb.com/en/article/key-definitions-used-in-iso-22301-and-iso-22313 (дата звернення: 09.10.2026).

7. Swanson M. et al. Contingency Planning Guide for Federal Information Systems : NIST Special Publication 800-34 Rev. 1. Gaithersburg : NIST, 2010. URL: https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final (дата звернення: 09.10.2026).

8. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile : NIST Special Publication 800-61 Rev. 3. Gaithersburg : NIST, 2025. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (дата звернення: 09.10.2026).

9. WCO Guidelines on Disaster Management and Supply Chain Continuity. World Customs Organization. URL: https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/guidelines-on-disaster-management.aspx (дата звернення: 09.10.2026).

10. Про затвердження Порядку виконання невідкладних робіт щодо ліквідації наслідків збройної агресії Російської Федерації, пов'язаних із пошкодженням будівель та споруд : постанова Кабінету Міністрів України від 19.04.2022 № 473. URL: https://zakon.rada.gov.ua/laws/show/473-2022-%D0%BF (дата звернення: 09.10.2026).

11. Фіксація пошкодження майна установи внаслідок збройної агресії. Бюджетна бухгалтерія. 2023. № 38. URL: https://i.factor.ua/ukr/journals/bb/2023/october/issue-38/article-126595.html (дата звернення: 09.10.2026).