УДК 004.056.5:004.056.55

Методи та засоби побудови комплексної системи захисту інформації типового об’єкта інформаційної діяльності

Дмитро Задворний[0009-0005-5163-1472]
Валерій Козачок[0000-0003-0072-2567]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. У статті розглянуто методи та засоби побудови комплексної системи захисту інформації (КСЗІ) для типового об’єкта інформаційної діяльності (ОІД). Запропоновано модель КСЗІ, що враховує сучасні кіберзагрози, вимоги національного законодавства та міжнародних стандартів. Розроблено рекомендації щодо технічних, програмних, криптографічних, організаційних заходів захисту, а також проведено оцінку ефективності впроваджених рішень.
Ключові слова: інформаційна безпека, комплексна система захисту інформації, об’єкт інформаційної діяльності, модель загроз, модель порушника.

Methods and Means of Building a Comprehensive Information Security System for a Typical Information Activity Object

Dmytro Zadvornyi[0009-0005-5163-1472]
Valeriy Kozachok[0000-0003-0072-2567]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. This paper examines the methods and means of building a comprehensive information security system for a typical information activity object (IAO). A CISS model is proposed that takes into account modern cyber threats, as well as the requirements of national legislation and international standards. Recommendations have been developed regarding technical, software, cryptographic, and organizational protection measures, and the effectiveness of the implemented solutions has been evaluated.
Keywords: information security, comprehensive information security system, information activity object, threat model, intruder model.

Вступ

В умовах глобальної інформатизації ключовим активом стає інформація, від якої залежить стабільність і конкурентоспроможність організацій в усіх сферах діяльності – від бізнесу та управління до освіти й медицини. Водночас зростає кількість і складність кіберзагроз, що підвищує потребу в ефективних системах захисту інформації [1].

Актуальність теми зумовлена збільшенням кіберінцидентів, необхідністю відповідності міжнародним стандартам ISO/IEC 27001, GDPR та впровадженням національної нормативно-правової бази у сфері інформаційної безпеки. Додатковим чинником є людський фактор, який залишається одним із головних джерел ризику [2].

Новизна роботи полягає у створенні моделі побудови КСЗІ для типового підприємства з урахуванням принципу багаторівневого захисту (defense in depth). Модель інтегрує технічні, криптографічні й організаційні заходи, а також сучасні технології DLP, PAM, SOC/SIEM, SOAR, DevSecOps, що забезпечує відповідність як національним, так і міжнародним стандартам [3].

Метою є розробка моделі побудови КСЗІ для типового ОІД з урахуванням сучасних кіберзагроз, нормативних вимог і міжнародних стандартів.

Об’єкт дослідження є процес забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах ОІД.

Предметом дослідження є методи, засоби та організаційні механізми побудови КСЗІ.

Часткові завдання:

1. Дослідити нормативно-правову базу у сфері захисту інформації.
2. Вивчити методологію створення КСЗІ та визначити їх вимоги до захисту ОІД.
3. Розробити модель побудови КСЗІ для типового підприємства.
4. Провести аналіз інформаційних потоків, загроз і вразливостей, сформувати профіль захищеності.
5. Сформувати комплекс технічних, програмних, криптографічних, організаційних заходів захисту та оцінити доцільність запропонованих рішень.

Методи та моделі

У роботі застосовано системний, ризик-орієнтований і сценарний підходи відповідно до міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-53 та принципів Secure Controls Framework (SCF). Порівняно з роботою «Технологія побудови та оптимізації комплексної системи захисту інформації типового об’єкту інформаційної діяльності», де КСЗІ розглядалася переважно в теоретичному аспекті з використанням базових моделей аналізу загроз, у цьому дослідженні запропоновано практичну реалізацію багаторівневої архітектури захисту, що об’єднує організаційний, технічний і криптографічний рівні. Запроваджено інтеграцію сучасних інструментів кіберзахисту – SIEM/SOAR, DLP, PAM, систем резервного копіювання та багатофакторної автентифікації [4]. Порівняно з роботою «Технологія забезпечення безпеки систем розробка актуальної системи КСЗІ на базі нормативних документів системи технічного захисту інформації», яка акцентує увагу на нормативно-правових аспектах кібербезпеки та концепції SCF як теоретичної моделі контролів, ця робота доповнює нормативну основу практичною імплементацією SCF у процес побудови корпоративної КСЗІ. Це дозволило узгодити політики, процедури та технічні засоби безпеки в єдиній системі управління ризиками [5–7]. Особливістю запропонованої моделі є використання сценарного аналізу загроз і поведінкових шаблонів порушників, що дає змогу формувати динамічний профіль ризиків та оцінювати ефективність заходів за показниками MTTD, MTTR і кількістю критичних інцидентів.

Отже, дана робота поєднує теоретичні підходи, представлені у дослідженнях Кременецького Владислава Володимировича та Чумаченка Сергія Сергійовича, із практичною моделлю побудови КСЗІ, яка орієнтована на сучасні тенденції кіберзахисту, автоматизоване реагування та безперервне вдосконалення систем безпеки.

Результати

Результатом стала розроблена модель створення КСЗІ для умовного підприємства «ЕнергоТрансЛогістика», що дало змогу сформувати цілісне бачення стану інформаційної безпеки та визначити основні напрями її вдосконалення.

Проведений аналіз засвідчив, що початковий рівень захисту організації характеризувався лише частковим використанням технічних засобів, недостатнім впровадженням організаційних заходів і відсутністю стратегічного підходу до управління ризиками. Це створювало потенційні загрози для забезпечення конфіденційності, цілісності та доступності інформаційних активів.

У процесі дослідження було здійснено детальне обстеження інформаційно-телекомунікаційної системи, проведено ідентифікацію інформаційних потоків, а також побудовано моделі загроз і порушників.

Результати показали, що найбільшу небезпеку становлять внутрішні дії персоналу, фішингові кампанії, зловживання з боку підрядників, експлуатація мережевих вразливостей і використання застарілих криптографічних протоколів.

Рівень захищеності об’єкта оцінено як середній: частина технічних рішень (NGFW, антивірусні системи, резервне копіювання) функціонує ефективно, проте критичні напрями – такі як: DLP, PAM, SOAR, централізоване управління доступом, BCP та IRP – залишаються недостатньо розвиненими. Це підтверджено побудованими матрицями загроз, порушників і зрілості. Запропоновані заходи з удосконалення КСЗІ включають розробку комплексної політики інформаційної безпеки, впровадження DLP і PAM-систем, уніфікацію засобів криптографічного захисту, розширення можливостей SIEM і SOC до цілодобового режиму роботи (24×7), автоматизацію реагування за допомогою SOAR, підвищення рівня обізнаності персоналу, а також формалізацію планів IRP та BCP. Оцінка ефективності цих рішень показала, що їх реалізація дасть змогу скоротити кількість критичних інцидентів на 60–70 %, зменшити фінансові втрати на 30–40 % і досягти відповідності вимогам міжнародного стандарту ISO/IEC 27001.

Реалізація запропонованої моделі дозволяє підприємству «ЕнергоТрансЛогістика» перейти від фрагментарного та реактивного управління безпекою до системного й проактивного, що забезпечує кіберстійкість, безперервність бізнес-процесів і довіру клієнтів та партнерів [8, 9].

Обговорення

Ефективність побудованої КСЗІ визначається рівнем зниження ризиків, підвищенням стійкості бізнес-процесів і відповідністю нормативним вимогам. Для підприємства «ЕнергоТрансЛогістика» ключовими критеріями стали: відповідність стандартам ДССЗЗІ, ISO/IEC 27001 та GDPR; зменшення кількості критичних інцидентів; скорочення часу виявлення (MTTD) і реагування (MTTR) на події; підвищення рівня зрілості організаційних процесів. До впровадження заходів інформаційна безпека мала фрагментарний характер: відсутність DLP і PAM, слабкий контроль доступів, застарілі криптографічні протоколи, неформалізовані процедури реагування. Після реалізації дорожньої карти організація перейшла до системного управління безпекою – впроваджено комплексну політику ІБ, класифікацію даних [9], автоматизовані рішення DLP, PAM, SIEM/SOC 24×7, SOAR для типових інцидентів [10], а також криптографічний захист на базі TLS 1.3 та AES-256 [11, 12]. Порівняльна оцінка показала істотне покращення за всіма напрямами: скорочення внутрішніх витоків на 60 %, зменшення часу реагування на інциденти у 3–4 рази, зниження кількості критичних загроз на 70 %, а фінансових втрат – приблизно на 30–40 %. Підвищення рівня автоматизації процесів та формалізація політик забезпечили контроль над діями адміністраторів, зменшили вплив людського фактора та посилили відповідальність персоналу. Загалом ефективність запропонованих рішень можна оцінити як високий рівень зрілості. Проведені дії підтвердили доцільність і результативність комплексного підходу до побудови КСЗІ [8].

Висновки

Таким чином, було детально розглянуто теоретичні, методологічні та практичні аспекти створення КСЗІ для типового ОІД. Поставлена мета – розробка моделі КСЗІ з урахуванням сучасних кіберзагроз, нормативних вимог і міжнародних стандартів – досягнута шляхом виконання визначених завдань.

Практичне значення полягає у можливості використання розробленої моделі як методологічної основи для впровадження систем захисту на підприємствах різного масштабу.

Джерела

1. Мінекономрозвитку України. (2023). ДСТУ ISO/IEC 24745:2023. Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації (ISO/IEC 24745:2022, IDT). Київ: Мінекономрозвитку України. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104381

2. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO. https://www.iso.org/standard/27001

3. Верховна Рада України. (1996). Конституція України: Офіційний текст від 28.06.1996 № 254к/96-ВР із змінами та доповненнями. Київ: Відомості Верховної Ради України. https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

4. Кременецький, В. В. (2020). Технологія побудови та оптимізації комплексної системи захисту інформації типового об’єкту інформаційної діяльності. Київ: Університет Грінченка, Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка. https://studbase.kubg.edu.ua/article/5267

5. Чумаченко, С. С. (2022). Технологія забезпечення безпеки систем: розробка актуальної системи КСЗІ на базі нормативних документів системи технічного захисту інформації. Київ: Університет Грінченка, Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка. https://studbase.kubg.edu.ua/article/7631

6. Kriuchkova, L., Skladannyi, P., & Vorokhob, M. (2023). Pre-project solutions for building an authorization system based on the zero trust concept. Cybersecurity: Education, Science, Technique, 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

7. Складанний, П., Машкіна, І., Рзаєва, С., & Костюк, Ю. (2025). Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології, 2(87), 59–76. https://doi.org/10.31673/2412-4338.2025.027860

8. International Organization for Standardization. (2022). ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on information security risk management. Geneva: ISO. https://www.iso.org/standard/80585.html

9. Мінекономрозвитку України. (2023). ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT). Київ: Мінекономрозвитку України. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104399

10. Scarfone, K. A., & Mell, P. M. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-94

11. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of Applied Cryptography. CRC Press. https://doi.org/10.1201/9780429466335

12. National Institute of Standards and Technology. (2023). Post-quantum cryptography standardization project. Gaithersburg: NIST. https://csrc.nist.gov/pqc-standardization