УДОСКОНАЛЕННЯ ПІДХОДУ ЩОДО УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ДСНС УКРАЇНИ З УРАХУВАННЯМ ТЕОРІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кальченко Є.О., Снігуров А.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: yehor.kalchenko@nure.ua ,
arkadii.snihurov@nure.ua

Abstract

The study proposes an approach to improve the process of handling cyber incidents for the information and communication system of the State Emergency Service of Ukraine, taking into account the best practices presented in the ISO/IEC 27000 standard families. It is proposed to interrelate the processes of risk assessment and incident handling, taking into account the specifics of this information and communication system. The study proposes to improve the risk assessment mechanism using the CRAMM approach, which improves the process of categorization of critical assets, and also improves the process of determining vulnerability levels using the metrics of the Common Vulnerability Scoring System CVSS version 4.0.

Потенційні загрози інформаційної безпеки інформаційно-комунікаційній системі Державної служби України з надзвичайних ситуацій (далі – ІКС ДСНС) мають різноплановий характер, а саме:

– складні технічні кібератаки, спрямовані на порушення конфіденційності, цілісності та доступності інформації, інформаційних процесів в ІКС ДСНС (атаки з використанням шкідливих програм, DDOS – атаки, несанкціонований доступ та інші з експлуатацією наявних уразливостей та багатоетапним проникненням);

– атаки з використанням методів соціальної інженерії, маніпулятивному впливу на персонал, який експлуатує ІКС ДСНС;

– складні технічні атаки з використанням побічних електромагнітних випромінювань та наводок електронно-обчислювальної техніки ІКС ДСНС, перехоплення інформації, яка передається по каналам зв'язку ІКС ДСНС, використання акустичних каналів витоку мовної інформації посадових осіб та персоналу ІКС ДСНС та інші;

– технічні збої апаратної складової та програмного забезпечення ІКС ДСНС;

– наявність людського фактору, який може проявитися внаслідок недостатнього рівня безпекової обізнаності, непоінформованості персоналу ІКС ДСНС щодо необхідності виконання вимог нормативних документів, технічної документації при експлуатації системи.

На даний момент існує ряд міжнародних стандартів, які регламентуються вимоги та практичні підходи до побудови системи управління інформаційною безпекою (СУІБ) організацій та установ, складних інформаційних систем, до яких відносяться такі, як сімейство стандартів ISO/IEC 27000 (зокрема, 27001:2022 [1], 27005:2022 [2], 27035-1:2023 [3]) та інші.

Так стандарт ISO/IEC27001:2022 впроваджує вимоги до СУІБ, при яких пропонується комплексний підхід до забезпечення інформаційної безпеки у вигляді сукупності взаємопов'язаних процесів, стандарт ISO/IEC27005:2022 запроваджує механізм реалізації менеджменту ризиків інформаційної безпеки, стандарт ISO/IEC27035-1:2023 запроваджує стандартизований процес реагування на інциденти інформаційної безпеки.

Згідно з підходом, представленим цими стандартами, при плануванні, впровадженні, функціонуванні та моніторингу СУІБ здійснюється визначення інформаційних активів, обладнання та процесів, які є критичними для організації, визначаються рівні критичності цих активів, проводиться оцінювання ризиків інформаційної безпеки (далі ризики) для цих активів, визначаються на підставі даного оцінювання механізми обробки ризиків. Під час функціонування СУІБ здійснюється моніторинг ефективності її функціонування шляхом впровадження кількох процесів, одним з яких є обробка інцидентів інформаційної безпеки.

Процеси управління ризиками та інцидентами інформаційної безпеки є взаємодоповнюючими процесами. Під час першого процесу на підставі аналізу потенційних загроз, вразливостей інформаційної системи організації, формується перелік усіх ризиків для кожного з визначених критичних активів. Результати оцінювання ризиків є фактично прогнозом потенційних результатів реалізації загроз, на підставі яких обираються захисні засоби та заходи. Пріоритизація ризиків дозволяє провести їх класифікацію по ступеню небезпечності для функціонування інформаційної системи організації та визначити, на які ризики необхідно звернути особливу увагу з точки зору задіяння усіх видів ресурсів, матеріальних, людських та часових для зниження ризиків. Під час процесу обробки інцидентів оцінюється якість цього прогнозу та ефективність обраних захисних заходів з використанням певних метрик та критеріїв. Якщо якість функціонування СУІБ визначена неефективною, здійснюється переоцінювання ризиків з визначенням додаткових захисних засобів та заходів. Пріоритизація ризиків дозволяє підійти до найважливішого завдання – пріоритизації інцидентів інформаційної безпеки для ефективного та своєчасного реагування на них. Це дозволяє впровадити системний підхід до організації процесу управління інцидентами ІКС ДСНС.

На даний час у світі для оцінки ризику інформаційної безпеки існує значна кількість різних методик. До них можна віднести CRAMM (Великобританія), MARION (Франція), CRISAM (Австрія, Німеччина), COBRA (Великобританія), vsRisk (Великобританія), Risk Matrix (США), Mehati (Франція), MAGERIT (Іспанія), RiskWatch (США), MSAT (США), FRAP (США), OCTAVE (США) та інші. В дослідженні для оцінювання ризиками ІКС ДСНС взята за основу методика CRAMM, яка належить та підтримується Службою безпеки від імені Уряду Великобританії. Ця методика розроблена, в тому числі, для проведення аналізу ризиків інформаційних систем і мереж.

Методика CRAMM адаптована для специфіки організацій та установ Великобританії, особливо щодо формалізації рівнів критичних активів. В дослідженні проводиться удосконалення механізму оцінювання ризиків з використанням підходу CRAMM для специфіки ІКС ДСНС. Крім удосконалення процесу категоруваня критичних активів ІКС ДСНС також пропонується удосконалення процесу визначення рівнів вразливостей ІКС ДСНС з використанням метрик загальної системи оцінки вразливостей CVSS версії 4.0.

Такий підхід дозволить системно підійти до питання організації процесу управління інцидентами інформаційної безпеки ІКС ДСНС на підставі глибокого аналізу потенційних загроз, вразливостей, критичності активів даної системи, провести пріоритизацію потенційних інцидентів з метою своєчасного реагування на них.

Література

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/82875.html.
2. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/standard/80585.html.
3. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. URL: https://www.iso.org/standard/78973.html.
4. CRAMM (CCTA Risk Analysis and Management Method). URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.