Основні моделі управління інформаційною безпекою

Володимир Задворний
аспірант кафедри менеджменту,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
email: zadvornyivs@krok.edu.ua
Марта Копитко
керівник, д.е.н., професор,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,

Вплив інформаційних технологій на бізнес-процеси широко визнаний, і їхня роль у появі нових бізнес-моделей добре відома. Щоб використовувати переваги бізнес-процесів, що підтримуються IT, необхідно керувати безпекою базових інформаційних систем. Різні моделі передового досвіду та стандарти інформаційної безпеки є рішеннями для зниження та усунення широкого спектру ризиків.

Ризик менеджери часто стикаються з багатьма однаковими перешкодами, навіть якщо вони керують проектами різного розміру або в різних галузях. Базування практик безпеки на добре відомих, а іноді й регульованих урядом моделях інформаційної безпеки дозволяє вдосконалити процесів забезпечення інформаційної безпеки.

Однією з головних проблем в управлінні інформаційною безпекою є неповна інформація про ризики, з якими стикаються інформаційні системи, а також доступні засоби контролю для їх усунення. Таким чином, моделі планування, контрольні списки та рекомендації були і залишаються популярними. Оскільки кожна організація визначає загрози своїм інформаційним системам і визначає відповідні контрзаходи, з'являється набір найкращих практик і методів. У спробі стандартизувати зусилля в галузі інформаційної безпеки були розроблені рамки передової практики та стандарти [1].

Можна виділили декілька основних найпопулярніших у світі моделей інформаційної безпеки, яких дотримуються організації в усьому світі, щоб досягти рівня зрілості своїх програм захисту [2]:

NIST - Це агентство Міністерства торгівлі Сполучених Штатів, завданням якого є сприяння інноваціям і промисловій конкурентоспроможності шляхом розвитку науки, стандартів і технологій вимірювань. NIST розробляє та випускає стандарти, рекомендації та найкращі практики в різних сферах, включаючи кібербезпеку, інформаційні технології та фізичні науки.

ISO 27000 - це серія міжнародних стандартів, які забезпечують основу для систем управління інформаційною безпекою (ISMS). Стандарти розроблені Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC).

ISO/IEC 27001:2013 - це основний стандарт, який визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті загальних бізнес-ризиків

організації. Він визначає критерії оцінки ефективності системи управління інформаційною безпекою організації.

CIS Critical Security Controls (CIS Controls) - це набір найкращих практик і вказівок, розроблених Центром безпеки в Інтернеті (CIS), щоб допомогти організаціям посилити свою позицію кібербезпеки. CIS Controls - це пріоритетний набір дій, призначених для пом'якшення найпоширеніших кіберзагроз і підвищення загальної безпеки організації.

PCI-DSS - Норми стандарту безпеки даних (DSS) індустрії платіжних карток (PCI) зосереджені на захисті платіжної інформації споживачів, яка зберігається під час операцій обробки карток. Існує 12 вимог для того, щоб організація була визнана сумісною з PCI DSS, і цього вимагають усі компанії, які обробляють або передають інформацію про власників карток у рамках свого бізнесу.

GDPR - Загальний регламент захисту даних Європейського Союзу зосереджується на вимогах організацій у ЄС щодо захисту даних споживачів. Модель інформаційної безпеки також включає захист інформації, що передається від організації, які розташовані в ЄС.

В Україні також діють національні нормативні акти що регламентують вимоги та правила щодо забезпечення інформаційної безпеки на території держави. До основних таких документів відносяться: Закон України "Про інформацію", Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", Закон України "Про захист персональних даних", а також нормативні документи в галузі технічного захисту інформації та державні стандарти України.

Перевагами застосування Міжнародних стандартів є забезпечення безперервності, мінімізація ризиків, забезпечення комплексного та централізованого контролю рівня захисту інформації, забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів, інформаційно-комунікаційних систем та мереж, зниження витрат на інформаційну безпеку [3].

Вибір моделі та стандартів забезпечення інформаційної безпеки залежить від різних факторів, основними з яких є юрисдикція у якій здійснює свою діяльність організація, галузь та галузеві регулятори які займаються регулюванням діяльності тієї чи іншої галузі, ринкові умови у яких діють ті чи інші організації.

Ключові слова: управління; інформаційна безпека.

Список використаних джерел

1. Danijel Milicevic, Matthias Goeken Application of Models in Information Security Management. Conference: Proceedings of the Fifth IEEE International Conference on Research Challenges in Information Science, RCIS 2011, Gosier, Guadeloupe, France, 19-21 May, 2011 https://www.researchgate.net/publication/221430579_Application_of_models_in_information_security_management.

2. Kaitlyn Graham Top 3 Most Common Cybersecurity Models Explained. URL: https://www.bitsight.com/blog/cybersecurity-model-types (дата доступу 20.11.2023 р.).

3. Дикий О.В. Стандарти інформаційної безпеки: компаративне дослідження. Право та державне управління. 2019, № 2 (35). том 1 С. 80-87.