УДК 35.004 DOI: 10.31673/2412-4338.2022.012935

Гордієнко С.Б. *Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій, Національна академія СБ України*

АКТУАЛЬНІ ПИТАННЯ УПРАВЛІННЯ ІТ РИЗИКАМИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація: *На сьогодні актуальним питанням безпекової галузі є спрямування на стан інформаційної безпеки об'єктів критичної інфраструктури з ефективним застосуванням відповідних заходів щодо підтримання її в належному стані.*

В даній статті підкреслюється особлива актуальність даних питань з акцентом на найбільш значущі аспекти забезпечення інформаційної безпеки на об'єктах критичної інфраструктури шляхом управління ризиками та стратегії реагування на них. Розкривається сутність способів реагування на ризики та їх обробки.

Попереднє планування процесу управління ризиками, пов'язаними з інформаційною інфраструктурою і є ключовим аспектом процесу управління ризиками безпеки. Грамотно спланований процес передбачає відповідність значущості бізнес-процесу для об'єкту критичної інфраструктури тим затратам, які необхідні для управління ризиками, що впливають на цей бізнес-процес. Всі бізнес-процеси, для яких величина збитку більше деякої заздалегідь визначеної величини, оголошуються критичними.

Діяльність з планування управління ризиками найефективніше здійснює спеціальна робоча група, до складу якої входять топ-менеджер, керівники інших підрозділів та IT менеджер. Робоча група формує стратегії реагування на виявлені, оцінені і проранжовані ризики. Необхідно підкреслити, що аналізуючи ризики, потрібно брати до уваги не тільки роботу систем в штатному режимі, але і пікове навантаження на них.

При прийнятті рішень щодо реагування на відповідні ризики мають враховуватись витрати з урахуванням повної оцінки рівня ризиків характерних для функціонування об'єктів критичної інфраструктури.

Коли керівниками бізнес-підрозділів визначаються завдання по боротьбі з ризиками в їх підрозділах, найчастіше вони приймають будь-які ризики не розуміючи наслідків, так як їх реальні цілі пов'язані з виконанням основних службових завдань, які впливають на кінцевий результат діяльності. Варіанти обробки ризику повинні бути оцінені на основі зниження ступеню ризику і ступеню будь-яких створюваних додаткових вигод або можливостей.

Особлива увага звернута на стратегію прийняття ризиків, яка потребує значних професійних та інтелектуальних здібностей осіб, які приймають рішення. З урахуванням особливостей даного способу реагування необхідна розробка підходу адаптованого для конкретного об'єкту інформаційної діяльності з визначенням питання економічної доцільності застосування безпекових заходів стосовно прояву можливих інцидентів інформаційної безпеки.

Ключові слова: *об'єкти критичної інфраструктури,стратегія реагування, прийняття ризиків,інформаційна безпека.*

Gordienko S.B. *Educational and Scientific Institute of Information Security and Strategic Communications, National Academy of the Security of Ukraine*

TOPICAL ISSUES OF IT RISK MANAGEMENT AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Abstract: *Today, the urgent issue of the security industry is to address the state of information security of critical infrastructure objects with the effective application of appropriate measures to maintain it in*

proper condition.

This article emphasizes the particular relevance of these issues with an emphasis on the most significant aspects of ensuring information security at critical infrastructure facilities through risk management and strategies for responding to them. The essence of ways of responding to risks and their processing is revealed.

Preliminary planning of the risk management process related to the information infrastructure is a key aspect of the security risk management process. A well-planned process involves matching the significance of the business process for the critical infrastructure object with the costs necessary to manage the risks affecting this business process. All business processes for which the value of the loss is greater than some predetermined value are declared critical.

Risk management planning activities are most effectively carried out by a special working group consisting of the top manager, heads of other departments and the IT manager. The working group forms strategies for responding to identified, assessed and ranked risks. It should be emphasized that when analyzing risks, it is necessary to take into account not only the operation of systems in regular mode, but also the peak load on them.

When making decisions about responding to relevant risks, costs must be taken into account, taking into account the full assessment of the level of risks characteristic of the operation of critical infrastructure objects.

When managers of business units determine tasks to combat risks in their units, most often they accept any risks without understanding the consequences, since their real goals are related to the performance of the main official tasks that affect the final result of the activity. Risk treatment options should be evaluated based on the degree of risk reduction and the degree of any additional benefits or opportunities created.

Special attention is paid to the risk-taking strategy, which requires significant professional and intellectual abilities of decision-makers. Taking into account the peculiarities of this method of response, it is necessary to develop an approach adapted for a specific object of information activity with the determination of the question of the economic feasibility of applying security measures in relation to the manifestation of possible information security incidents.

Keywords: *critical infrastructure facilities, response strategy, risk acceptance, information security.*

Вступ. Темпи розвитку глобальної інформаційної інфраструктури на основі сучасних інформаційних технологій є підґрунтям того, що на сьогодні, як елементи національної критичної інфраструктури так і інші бізнес утворення з різними формами власності стають об’єктами деструктивних впливів злочинних та різноманітних терористичних угруповань.

В той же час коли можливості інфокомунікаційних технологій широко відомі та ефективно використовуються у забезпечення функціональних та безпекових процесів всередині критичної інфраструктури,значимість їх на сьогодні сприймається з недостатнім ступенем серйозності. Інтенсивно зростаючий обсяг та значимість інформаційних ресурсів, сучасні можливості електронних засобів по їх обробці роблять інформаційні системи дуже привабливими для деструктивних посягань.

Об’єкти інформаційної діяльності та їх інформаційні системи все частіше стикаються з різними загрозами безпеки такими як шпигунство, комп'ютерне шахрайство та ін. Такі джерела збитку, як комп'ютерні віруси, комп'ютерний злом і атаки типу відмови в обслуговуванні, стають поширенішими агресивнішими і все більш витонченішими.

Залежність від інформаційних систем і послуг означає, що елементи національної критичної інфраструктури та інші бізнес утворення, стають все більш уразливими по відношенню до загроз безпеки. Взаємодія мереж загального користування і приватних мереж, а також спільне використання інформаційних ресурсів ускладнює управління доступом до інформаційних ресурсів.

Актуальність даної статті обумовлена необхідністю виявлення факторів ризику щодо ефективної діяльності об’єктів критичної інфраструктури та їх інформаційної складової. Розробка системи контролю і управління інформаційними ризиками наразі є пріоритетним

завданням. Заходи по управлінню ризиками обійдуться значно дешевше, якщо будуть включені в специфікацію вимог на стадії проектування системи.

Посилена увага суспільства та фахівців з інформаційної безпеки до деструктивних проявів недружніх держав в інформаційній сфері стосовно України зумовлюють зацікавленість багатьох вчених та державних діячів у висвітленні даного питання на рівні адекватного розуміння проблеми в цілому. Такі фахівці як А. Астрахов, М. Луцкий, В. Домарєв, О. Юдін, В. Богуш, О. Хорошко та інші у свої дослідженнях та публікаціях звертають значну увагу на існуючу проблему та шляхи її вирішення.

В силу специфічності тематики на сьогодні існують неоднозначні підходи та розуміння питань стратегії реагування на ризики інформаційної безпеки і тому головною спрямованістю в цих питаннях є застосування безпекових заходів до конкретних об’єктів інформаційної діяльності що відносяться до критичної інфраструктури.

Мета статті - аналіз, систематизація та розгляд актуальних питань стратегії реагування на ризики інформаційної безпеки, а також розуміння ступеню економічної доцільності застосування тих чи інших безпекових заходів стосовно прояву можливих інцидентів інформаційної безпеки.

Виклад основного матеріалу. Розвиток національної критичної інфраструктури України, її інформаційної складової на сьогодні є основою обороноздатності країни, її економічного і соціального розвитку і тому належна взаємодія на між установами різної форми власності та державним ІТ сектором в сфері інформаційної безпеки є важливою.

З урахуванням специфічних особливостей, забезпечення інформаційної безпеки систем функціонування об’єктів критичної інфраструктури вимагає особливого підходу. Для того щоб виробити такий підхід, необхідно, перш за все, оцінити серйозність проблеми в цілому, потім, спираючись на накопичену статистику інцидентів, піддати ретельному аналізу специфічні для системи загрози і вразливості і на підставі цього аналізу визначити особливі вимоги до режиму забезпечення інформаційної безпеки критичної інфраструктури .

Ключовий аспектом процесу управління ризиками є планування процесу управління ризиками які пов'язані з ІТ інфраструктурою. Грамотно спланований процес передбачає відповідність значущості бізнес-процесу для об'єкту критичної інфраструктури тим затратам, які необхідні для управління ризиками, що впливають на цей бізнес-процес.[1]

Діяльність з планування управління ризиками найефективніше здійснює спеціальна робоча група до складу якої входять топ-менеджер, керівники інших підрозділів та ІТ менеджер. Якщо до процесу впровадження методології управління ІТ ризиками вирішено залучати консультантів в галузі управління ІТ, то їх участь вже на етапі планування також є обов'язковою. З консультантом з інформаційної безпеки слід радитися, по можливості негайно, в разі підозри на виявлення інциденту порушення інформаційної безпеки або вразливості безпеки для забезпечення кваліфікованої поради або виділення ресурсів.

Детальніше зупинимося на тому, який внесок вносить в роботу групи кожний її учасник:

• Питання формування стратегічних цілей процесу управління ризиками, бюджету цього процесу і координації зусиль різних підрозділів очевидним чином відносяться до компетенції топ менеджменту.

• У рамках нарад робочої групи, завдання керівників інших підрозділів надати інформацію про внутрішній устрій бізнес-процесів, необхідну для аналізу ризиків.

• ІТ менеджмент, приймаючи участі в нарадах робочої групи, бере на себе технічні питання, пов'язані з ІТ.

На етапі планування робоча група досягає ряд цілей:

• виявлення бізнес-процесів об’єктів критичної інфраструктури;

• затвердження карти ймовірностей і наслідків;

• розробка плану зборів робочої групи, метою яких є аналіз ризиків для всіх критичних бізнес-процесів.

Кожен з цих процесів важливий і особливо з точки зору співробітників які в ньому беруть участь. Тому, повністю закономірне запитання: яким же чином виділити більш критичні бізнес-процеси ніж інші?

Існує кілька типових підходів до вирішення цього завдання. Наприклад, можна провести оцінку величини збитку, понесеного для кожного з досліджуваних бізнес-процесів, в разі його зупинки на строк до одного дня. При цьому, розмір матеріальної шкоди розраховується в деяких умовних одиницях, які враховують як прямі втрати, так і як недоотриманий прибуток, збиток репутації.

Всі бізнес-процеси, для яких величина збитку більше деякої заздалегідь визначеної величини, оголошуються критичними.

Календарний план сесій аналізу для виділених критичних процесів є підставою для виділення бюджету для цього типу робіт.

Як правило, участь робочої групи в повному складі на етапі аналізу не доцільна тому до роботи в рамках кожних зборів, залучаються лише ті керівники інших підрозділів, які відповідають за групу бізнес-процесів, яка розглядається і співробітники IT-підрозділу.

Для запису інцидентів порушення інформаційної безпеки та інших пов'язаних з безпекою подій слід створювати журнали аудиту і зберігати їх протягом узгодженого періоду часу.

Аналіз бізнес-процесів і аудит ризиків - наступний крок на шляху впровадження методології управління IT ризиками. Цей процес логічно розділити на ряд послідовних етапів:

• формалізація бізнес-процесів;

• виявлення IT активів, задіяних при кожному кроці;

• виявлення вузьких місць і проблемних ділянок IT інфраструктури;

• формалізація і ранжування ризиків.

Найчастіше бізнес-процеси описані досить абстрактно, не достатньо для аналізу ризиків, тому першим кроком є їх формалізація. Для кожного етапу бізнес-процесу IT підрозділ визначає, які елементи IT інфраструктури в ньому задіяні й наскільки ймовірним є збій у їх роботі. [1]

Необхідно підкреслити, що аналізуючи ризики, потрібно брати до уваги не тільки роботу систем в штатному режимі, але і пікове навантаження на них. Наприклад, IT-система яка зазвичай функціонує без збоїв, може вийти з ладу під час передноворічного піку навантаження.

Перевірка інформаційної безпеки може бути виконана внутрішнім аудитом, незалежним менеджером або сторонньою організацією, що спеціалізується на таких перевірках, при чому фахівці які залучаються до перевірок, повинні володіти відповідними досвідом і навичками.

Наступний етап - формування робочою групою стратегії реагування на виявлені,оцінені і проранжовані ризики.

При прийнятті рішень щодо реагування на відповідні ризики мають враховуватись витрати з урахуванням повної оцінки рівня ризиків характерних для функціонування об’єктів критичної інфраструктури.

В результаті процесу реагування на ризик і його обробки завжди існує залишковий ризик, який підлягає відпрацюванню, після чого приймається рішення по завершенню процесу реагування на ризик.

Можливі чотири варіанти такої стратегії реагування:

Зменшення ризику. Для зменшення ризику застосовуються відповідні заходи та засоби захисту, якими володіють відповідні структури. Можливим результатом є зниження ризику до рівня прийнятного для компанії.

Передача ризику. В цьому випадку ризик переадресовується сторонній організації на обслуговування та подальше реагування на нього (страхування або аутсорсинг). Якщо загальний чи залишковий ризик дуже високий для компанії, вона може придбати страховку, щоб перенести ризик на страхову компанію.

Відмова від ризику. Відмова від бізнес-процесів організації, що є причиною ризику. Наприклад, відмова від електронних платежів. Якщо компанія вирішує припинити діяльність, яка викликає ризик, це називається *уникненням ризику*.

Прийняття ризику. Цей спосіб реагування на ризики є найбільш цікавим з точки зору його розуміння та ефективного застосування. Ризик у конкретному випадку вважається усвідомлено припустимим – організація сприймає ризик яким він є, розуміючи можливі негативні наслідки. Зазвичай це означає, що вартість контрзаходів значно перевершує фінансові втрати у випадку реалізації загрози або організація не може знайти відповідні заходи і засоби безпеки. [2]

Останній підхід полягає в усвідомленому прийнятті ризику компанією, яка розуміє його рівень, розміри потенційного збитку, і, тим не менш, вирішує жити з цим ризиком і не впроваджувати контрзаходи. Для компанії доцільно прийняти ризик, коли аналіз витрат/вигоди показує, що витрати на контрзаходи перевищують розміри потенційних втрат.

Ключовим питанням при прийнятті ризику є розуміння того, чому це є найкращим виходом з конкретної ситуації.

На жаль, у наш час багато відповідальних осіб в компаніях приймають ризики, не розуміючи повною мірою, що вони приймають.

Зазвичай це пов'язано з відносною новизною процесів управління ризиками в області безпеки, недостатнім рівнем освіти і досвідом роботи людей які приймають рішення.

Коли керівниками бізнес-підрозділів визначаються завдання по боротьбі з ризиками в їх підрозділах, найчастіше вони приймають будь-які ризики не розуміючи наслідків, так як їх реальні цілі пов'язані з виконанням основних службових завдань які впливають на кінцевий результат діяльності, а зовсім не з ризиками. Вони не хочуть бути пов’язаними для них незрозумілою і дратівливою безпекою.

Прийняття ризику має бути засноване на декількох чинниках. Зокрема, потрібно відповісти на наступні питання.

- *Потенційні втрати менше вартості контрзаходів?*
- *Чи зможе компанія жити з тим "болем", якого завдасть їй прийняття цього ризику?*
- *Прийняття ризику може призвести до зростання кількості інцидентів безпеки – чи готова компанія впоратися з цим?*

Людина або група, яка приймає ризик, повинні розуміти потенційні наслідки цього рішення.

Коли нові або змінені ризики у виробничій сфері оцінюються як неприйнятні, на виконання обробки ризику може знадобитися певний час. У таких випадках керівництво повинно розуміти, що такі ризики приймаються на період часу, який буде потрібно для виконання обробки ризику. Може бути доречно накласти обмеження на операції на цей період.

Варіанти обробки ризику повинні бути оцінені на основі зниження ступеню ризику і ступеню будь-яких створюваних додаткових вигод або можливостей, відповідно до розроблених раніше критеріїв.

Вибір найбільш відповідного варіанту включає зіставлення вартості реалізації кожного варіанту з вигодами, одержуваними від нього. Загалом, вартість менеджменту ризиків повинна бути співмірною одержуваних вигід. [3]

Рішення щодо реагування на ризики потребують ретельного розгляду та врахування всіх без виключення та приниження значущості ризиків безпеки. Головним результатом має бути зниження ризику до можливого мінімуму не зважаючи на визначені раніше критерії.

Як правило обробка та реагування на ризики відбувається на комбінованій основі з урахуванням економічної та безпекової доцільності.

Деякі варіанти обробки ризику можуть ефективно вирішувати питання більш ніж одного ризику (наприклад, навчання і підвищення розуміння безпеки).

У тих випадках, коли сукупна вартість реалізації всіх варіантів обробки ризику перевищує доступний бюджет, план обробки ризику повинен чітко ідентифікувати впорядкування за пріоритетами, в якому будуть реалізовуватися індивідуальні варіанти обробки ризику. Упорядкування за пріоритетами може бути встановлено з використанням різних методів, включаючи ранжирування ризику та аналіз витрат. [3]

В рамках сесій з розробки стратегії реагування, для кожного сценарію і кожної дії необхідно визначити відповідального, а також передбачити механізми контролю за його діями.

Висновки. Пріоритетним завданням при управлінні інформаційними ризиками на об’єктах критичної інфраструктури є розробка системи контролю і управління ними. Заходи по управлінню ризиками обійдуться значно дешевше, якщо будуть включені в специфікацію вимог на стадії проектування системи забезпечення безпеки об’єктів.

В статті здійснено аналіз підходів реагування на ризики інформаційної безпеки об’єктів критичної інфраструктури. Особливий підхід щодо забезпечення інформаційної безпеки систем функціонування об’єктів критичної інфраструктури вимагає належної взаємодії між установами різної форми власності та державним ІТ сектором в сфері інформаційної безпеки.

Грамотно спланований процес передбачає відповідність значущості бізнес-процесу тим затратам, які необхідні для управління ризиками, що впливають на цей процес. При прийнятті рішень щодо реагування на відповідні ризики повинні враховуватись витрати на супровід механізмів безпеки, політика керівництва, простота реалізації, думка експертів та ін.

Особлива увага приділяється такій стратегії реагування як *прийняття ризику.* Цей спосіб реагування на ризики є найбільш цікавим з точки зору його розуміння та ефективного застосування. Ризик у конкретному випадку вважається усвідомлено припустимим – організація сприймає ризик яким він є. Прийняття ризику вимагає відповіді на важливі питання життєдіяльності об’єкту критичної інфраструктури.

Варіанти стратегії реагування на ризики оцінюються на основі зниження ступеню ризику і ступеню будь-яких створюваних додаткових вигод або можливостей, з урахуванням розроблених раніше критеріїв. Вибір найбільш відповідного варіанту включає зіставлення вартості реалізації кожного варіанту з вигодами, одержуваними від нього.

Список літератури

1. Постанова КМ України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» від 19 червня 2019 р. № 518 Київ *{Із змінами, внесеними згідно з Постановою КМ № 991 від 02.09.2022}.*

2. Іформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа];.— К.: ДУТ, 2015.— 288 с.

3. Домарев, В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В. В. Домарєв, В. В. Домарєв. – Донецьк: Велстар, 2012, 2012 – 146 с.

4. Богуш В. М. Юдін О. К. Інформаційна безпека держави. Харків: Консум. 2004. С-508.

5. Гарасим Ю.Р. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем / Ю.Р. Гарасим, В.А. Ромака,М.М. Рибій // Вісник Національного університету “Львівська політехніка” “Автоматика, вимірювання та керування”. – 2013. – № 756. – С. 105-123.

6. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

8. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

9. ДСТУ ISO/IEC TR 19791:2015 Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем (ISO/IEC TR 19791:2010, IDT).

10. НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ, Департамент інформатизації, Постанова Правління Національного банку України від 28.10.2010 N 474 (v0474500-10) "Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України", «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України.

References

1. Resolution of the Cabinet of Ministers of Ukraine "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" dated June 19, 2019 No. 518 Kyiv {Amended according to Resolution of the Cabinet of Ministers No. 991 dated 09/02/2022}.

2. Information and cyber security: sociotechnical aspect: textbook / [V. L. Buryachok, V. B. Tolubko, V. O. Khoroshko, S. V. Tolyupa];. K.: DUT, 2015.— 288 p.

3. Domarev, V.V. Management of information security in banking institutions (Theory and practice of implementing standards of the ISO 27k series) / V.V. Domarev, V.V. Domarev. - Donetsk: Velstar, 2012, 2012 - 146 p.

4. Bogush V. M. Yudin O. K. Information security of the state. Kharkiv: Konsum. 2004. S-508.

5. Garasim Y.R. Analysis of the information security risk management process in the process of ensuring the survivability of systems / Yu.R. Garasym, V.A. Romaka, M.M. Rybiy // Bulletin of the Lviv Polytechnic National University "Automation, measurement and control". - 2013. - No. 756. - P. 105-123.

6. DSTU ISO/IEC 27001:2015 Information technologies. Protection methods. Information security management systems. Requirements (ISO/IEC 27001:2013; Cor 1:2014, IDT).

7. DSTU ISO/IEC 27002:2015 Information technologies. Protection methods. Code of practices regarding information security measures (ISO/IEC 27002:2013; Cor 1:2014, IDT).

8. DSTU ISO/IEC 27005:2015 Information technologies. Protection methods. Information security risk management (ISO/IEC 27005:2011, IDT).

9. DSTU ISO/IEC TR 19791:2015 Information technologies. Protection methods. Security assessment of operating systems (ISO/IEC TR 19791:2010, IDT).

10. NATIONAL BANK OF UKRAINE, Department of Informatization, Resolution of the Board of the National Bank of Ukraine dated 28.10.2010 N 474 (v0474500-10) "On entry into force of information security management standards in the banking system of Ukraine", "Methodological recommendations on the implementation of the information security management system and risk assessment methods in accordance with the standards of the National Bank of Ukraine.