INFORMATION SECURITY RISK MANAGEMENT

DOI: 10.20535/2411-1031.2018.6.1.153189
УДК 004.056.53

ВОЛОДИМИР МОХОР,
ОЛЕКСАНДР БАКАЛИНСЬКИЙ,
ВАСИЛЬ ЦУРКАН

АНАЛІЗ СПОСОБІВ ПРЕДСТАВЛЕННЯ ОЦІНОК РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянуто способи представлення оцінок ризиків інформаційної безпеки. Серед них виокремлено дерево ризиків, троянду (зірку) та спіраль ризиків, карту ризиків і коридор прийнятності ризиків. Класичний метод побудови дерева використано для представлення на його основі оцінок ризиків. Його елементами відображено окремі або групи ризиків. Їх використання орієнтоване на структуризацію і класифікацію ризиків. За основу побудови троянди (зірки) і спіралі взято використання кругових діаграм. Ними відображено послідовність розгляду ризиків інформаційної безпеки. Завдяки цьому здійснюється їх ранжування при порівняльному аналізуванні. Трояндою (зіркою) відображається тільки один з параметрів ризику інформаційної безпеки серед обраної сукупності з можливістю накладання відображень одне на одне з різними параметрами. Тому використання такого способу представлення зводиться до побудови сімейство троянд (зірок) оцінок ризиків інформаційної безпеки. Водночас встановлено найбільшу розповсюдженість використання карти ризиків інформаційної безпеки серед відомих способів їх представлення. Картою ризиків відображаються оцінки з огляду на ймовірність реалізації загрози та величина втрат. Завдяки універсальності такого способу представлення можливе об'єднання, порівняння, накладання та інтегрування карт ризиків інформаційної безпеки. Тому серед них виокремлюються загальні та прикладні карти ризиків. Характерною особливістю карт ризиків загального виду є наявність або відсутність шкали оцінювання. За наявності шкали величина ризику оцінюється якісно або кількісно. Тоді як за її відсутності оцінювання зводиться до виокремлення областей оцінок ризиків інформаційної безпеки. Для кожної з виокремлених областей встановлюються інтервальні значення імовірності реалізації загрози та величини ризику. Коридор прийнятності ризиків інформаційної безпеки встановлюється індивідуально кожній організації з максимально вірогідними оцінками. Цими оцінками визначаються зони прийнятності ризиків інформаційної безпеки. Таким чином, аналізування способів представлення оцінок ризиків інформаційної безпеки деревом, розою (зіркою), спіраллю, картою і коридором прийнятності дозволило встановити їх переваги та недоліки. Крім цього обрати напрям подальших досліджень представлення оцінок ризиків інформаційної безпеки картою ризиків.

Ключові слова: ризик інформаційної безпеки, оцінка ризику інформаційної безпеки, дерево ризиків, троянда (зірка) ризиків, спіраль ризиків, карта ризиків, коридор прийнятності ризиків.

Постановка проблеми. Наочне представлення ризиків інформаційної безпеки здійснюється з урахуванням параметрів їх оцінювання. Для цього використовуються різноманітні способи, наприклад [1] - [7]: дерево ризиків; троянда (зірка) і спіраль ризиків; карта ризиків; коридор прийнятного рівня ризиків (коридор толерантності ризиків). Їх використання дозволяє наочно в графічному виді представляти результати оцінювання ризиків інформаційної безпеки та, як наслідок, приймати рішення про необхідність їх обробляння.

Аналіз останніх досліджень і публікацій. Способам представлення оцінок ризиків інформаційної безпеки приділено уваги в [4] - [7]. Зокрема, розглянуто окремі аспекти їх представлення. Наприклад [5] - [7], деревом ризиків; використання кругових діаграм; карт ризиків з дискретними шкалами оцінок параметрів ризику. Водночас досліджується використання коридору прийнятності ризиків інформаційної безпеки. Однак, при цьому не враховується, по-перше, специфіка сфери інформаційної безпеки; по-друге, особливості вибору способу представлення оцінок ризику інформаційної безпеки. На практиці це призводить до складнощів вибору відповідно способу представлення і, як наслідок, обробляння ризиків інформаційної безпеки.

Метою статті є аналізування способів представлення оцінок ризику інформаційної безпеки.

Виклад основного матеріалу досліджень.

Дерево ризиків [5], [6]. При використанні даного способу застосовується класичний метод побудови дерева. Елементами дерева є окремі ризики або групи ризиків, а параметрами дерева – кількісні оцінки ризиків. Крім цього, дерево ризиків використовується при їх класифікації за рівнем керування (нормативно-стратегічні, стратегічні, тактичні, оперативні). Таким чином, дерева ризиків поділяються на дерева структуризації ризиків і дерева класифікації ризиків. Приклад дерева структуризації ризиків показано на рис. 1. Оскільки оцінювання ризиків інформаційної безпеки здійснюється за двома параметрами P і H (P може визначатися через P_1 – імовірність реалізації загрози або реалізації ризику, P_2 – імовірність зміни фінансових результатів діяльності організації, H – втрати в результаті реалізації ризику), елементами розглянутого дерева є саме ці величини. Доцільно зазначити, що на рис. 1 відображено лише фрагмент дерева для одного виду ризиків умовної організації. У реальних умовах дерево структуризації ризиків конкретної організації більш розгалужене і складее. Це обумовлено тим, що воно включає на 0-му рівні всі групи ризиків інформаційної безпеки (з метою класифікації таких груп доцільно розглядати розділи Додаток А [2], хоча можуть використовуватися і інші підходи до класифікації, наприклад, стосовно властивостей інформації).

Приклад побудови дерева класифікації ризиків за рівнем керування для організації представлений на рис. 2. Для прикладу, дерево включає дві групи стратегічних ризиків інформаційної безпеки (вони відповідають розділам А8 і А17 Додатку А [2]). Приклад дерева класифікації ризиків містить три види ризиків: стратегічні, тактичні й оперативні, що відповідає класичній моделі керування організацією/підприємством. За необхідності представлені дерева ризиків можуть бути поєднані.

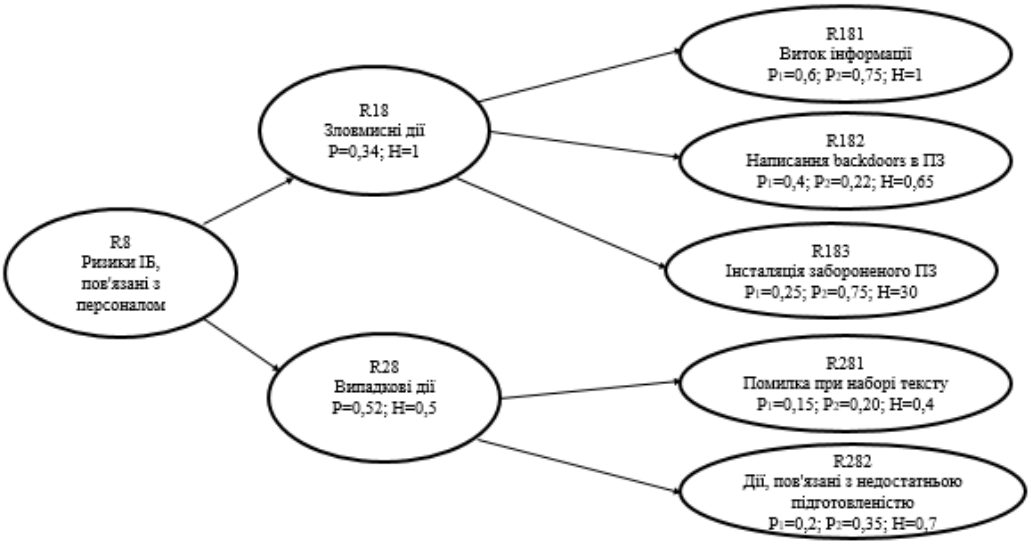


Рисунок1 – Фрагмент дерева структуризації ризиків

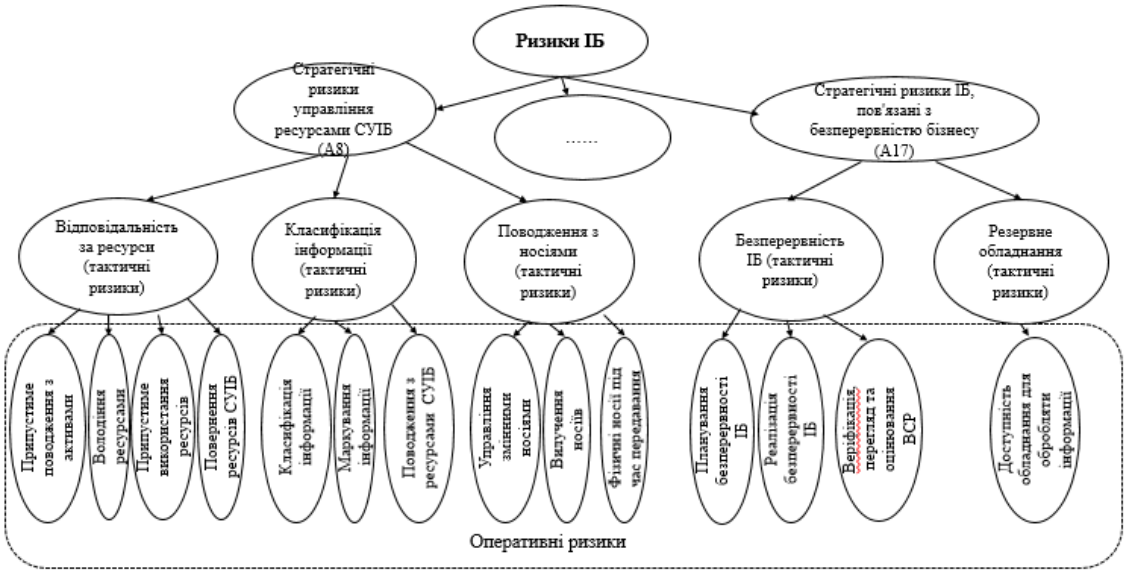


Рисунок 2 – Дерево класифікації ризиків організації за рівнем керування

Троянда (зірка) і спіраль ризиків [5], [6]. За основу побудови троянди (зірки) та спіралі ризків взято кругові діаграми. Троянда (зірка) (див. рис. 3) дозволяє відображати ризики в послідовності їх розгляду. Це спонукає до проведення ранжування ризиків при їх зіставленні. По осях відкладаються значення відповідних параметрів ризику. Кожна троянда (зірка) відображає тільки один з параметрів для обраної сукупності. При цьому, за необхідності, троянди ризиків з різними параметрами можуть "накладатися" одна на одну, або на одній троянді по осях можуть відкладатися два або три параметра ризиків.

У спіралі (див. рис. 4) ризики вказуються послідовно від найменшого значення показника кількісної оцінки ризику до найбільшого. Візуально така діаграма, яка використовується з метою відображення результатів оцінки показників ризиків, сприймається легше, ніж троянда ризиків, при цьому і аналіз ризиків проводити простіше.

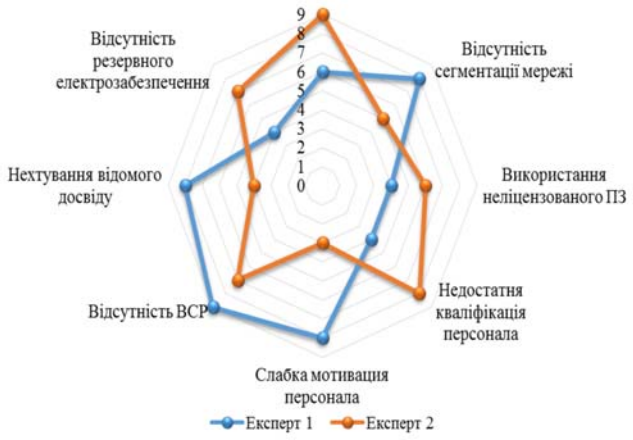


Рисунок 3 – Троянда аналізу груп ризиків за ймовірністю реалізації ризику

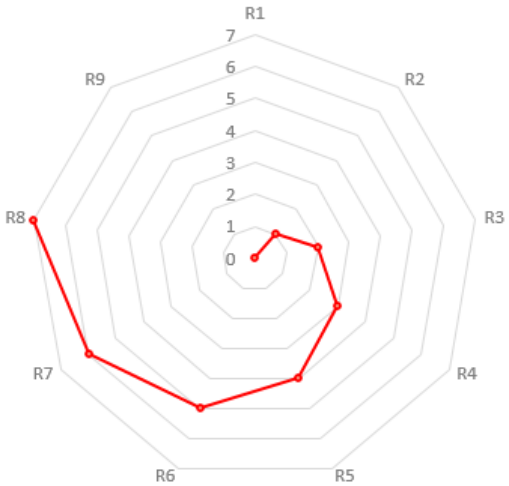


Рисунок4 – Спіраль аналізу груп ризиків за ймовірністю реалізації ризику

Доцільно зауважити, що немає необхідності одночасно використовувати обидва інструменти (і троянду, і спіраль ризиків), оскільки вони відображають однакові результати. В умовах керування ризиками інформаційної безпек реальної організації рекомендується будувати сімейство троянд або спіралей ризиків. Кожна троянда або спіраль ризиків може розроблятися: а) для всієї організації в цілому стосовно класифікаційних груп ризиків інформаційної безпеки (ризики, пов'язані з персоналом, з працездатністю інформаційних

технологій, з постачальниками); б) для окремих процесів, структурних підрозділів організації стосовно груп ризиків; в) для окремих груп ризиків з виділенням окремих ризиків, що входять в групу; г) на основі одного чи декількох критеріїв ризику, що використовуються для його оцінювання. Поєднання двох і більше діаграм дозволяє візуально проводити порівняльний аналіз ризиків за параметрами оцінки та величиною ризиків, за видами ризиків в межах групи, за групами ризиків в межах організації. Троянда і спіраль ризиків, як кругові діаграми, дозволяють наочно визначати "резерв" кожного окремого ризику і/або групи ризиків інформаційної безпеки з точки зору досягнення мінімального/максимального значення відповідного параметра. Крім цього, побудова та порівняння діаграм до визначення керівного впливу на ризики і після його здійснення дозволяє наочно спостерігати за результатами керування ризиками і проводити відповідний аналіз [6].

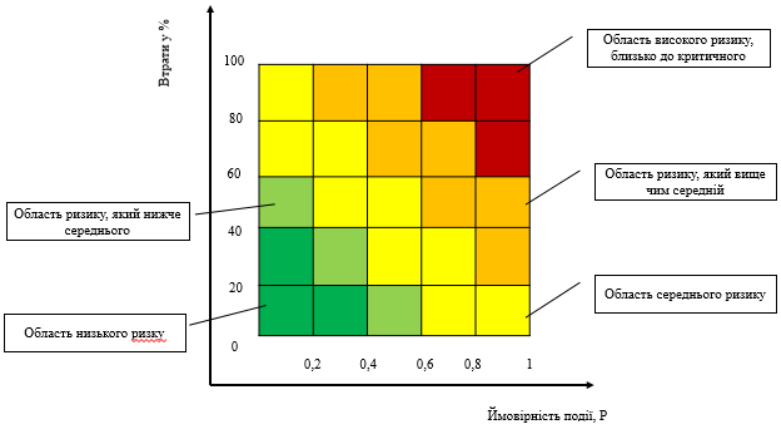
Карта ризиків [5]. Цей спосіб дозволяє системно наочно подати ризики відповідно до їх кількісної оцінки. Тому традиційно карта ризиків є координатною площиною, осями якої є показники оцінки ризиків. У більшості випадків – це параметри ймовірності і величини ймовірних втрат. Осями координат в картах ризиків є шкали, що розробляються і використовуються ризик-менеджерами для оцінювання ризиків. Карти ризиків зручно використовувати для їх моніторингу, коли за результатами його проведення ризики "наносяться" на координатну площину, і перегляд карт в динаміці дозволяє візуально системно уявити тенденції зміни ризиків. Карти ризиків можуть складатися для всієї організації в цілому, для окремих процесів, напрямків, структурних підрозділів організації, для окремих груп ризиків. Застосування універсальної (однотипної) форми карти для груп ризиків, підрозділів і всієї організації дозволяє об'єднувати, порівнювати, накладати, інтегрувати карти ризиків. Це забезпечує отримання нової інформації про ризики інформаційної безпеки організації, необхідної для проведення аналізу і прийняття рішень про керування ризиками. Доцільно зазначити, що умовно можна виділити такі різновиди карт ризиків [6]:

1) карти ризиків загального вигляду. Представляються як форми карт, які в подальшому можуть використовуватися для конкретної організації. Характерною особливістю даних карт є те, що це карти без нанесення на них ризиків відповідно за їхньою кількісною оцінкою. На даних картах також можуть бути відсутні шкали, які використовуються для оцінки конкретного виду ризику або його рівня (подібні шкали використовуються у вигляді координатних осей). Лише використовується традиційне розбиття осей. Варіанти найбільш традиційних форм карт ризиків організації представлені на рис. 5. Особливість карти ризиків, зображеної на рис. 5, а полягає в тому, що вона може використовуватися для будь-якого виду і/або групи ризиків і не містить шкал оцінки ризику.

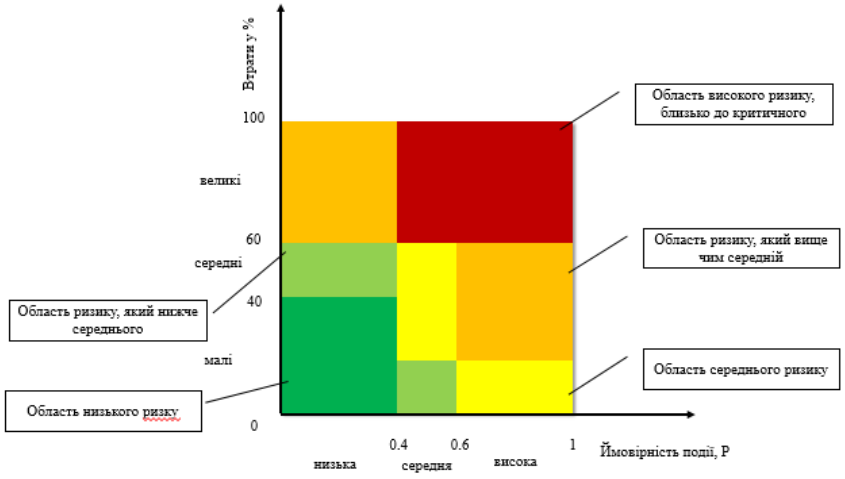
Це дозволяє використовувати дану карту для будь-яких ризиків, а відсутність шкал компенсується зазначеними областями рівнів ризику. Такими як області низького, нижче середнього, середнього, вище середнього і високого ризику, близького до критичного. Для кожної із зазначених областей встановлено інтервальні значення обраних показників оцінки ризиків.

Карта, представлена на рис. 5, б орієнтована на конкретний вид ризику і містить шкали для визначення якісних і кількісних оцінок ризиків, розташовані по координатним осях: по горизонтальній осі – шкала для оцінки ризику за параметром "Імовірність", а по вертикальній осі – шкала для оцінки ризику за параметром "Величина ймовірних втрат". На рис. 6 представлено ще один варіант карти ризиків загального вигляду [6], яка аналогічна карті на рис. 5, а. Однак, відрізняється наявністю трьох осей, що відповідають трьом параметрам ризиків (P_1, P_2 і H).

Такий варіант карти дозволяє оцінювати параметри ризиків в залежності від шкал і зон ризиків, що використовуються. По-друге, представлена на рис. 6 карта є більш гнучким і зручним інструментом аналізування ризиків. Оскільки вона дозволяє будувати сімейство карт при фіксованій імовірності P_1 (на рис. 6, як приклад, взято $P_1 = 0,4$).



а)



б)

Рисунок 5 – Варіанти найбільш традиційних форм карт ризиків загального вигляду:
а) карта ризиків без шкали якісної оцінювання ризиків;
б) карта ризиків зі шкалою якісного та кількісного оцінювання ризиків

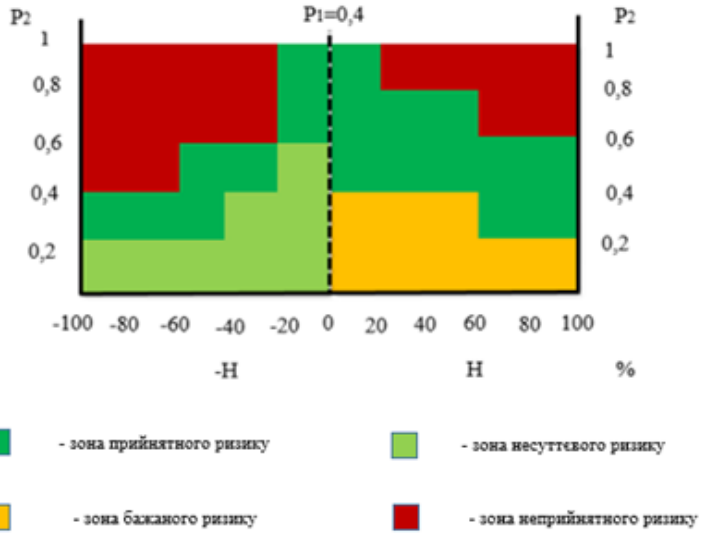


Рисунок 6 – Варіант побудови карти ризиків загального вигляду із зазначенням категорії ризику

При цьому є можливість отримання перетину тривимірної карти при фіксованому параметрі P_1, що змінюється у діапазоні від 0 до 1 (зазвичай з деяким кроком). Аналогічні сімейства карт можуть розроблятися для фіксованих параметрів P_2 і H. Необхідно зазначити, що дані карти корисні, перш за все, в теоретичному аспекті. В умовах реального керування ризиками застосовуються прикладні карти, що містять інформацію про параметри ризиків відповідно до їх кількісної оцінки;

2) прикладні карти ризиків. Приклад найбільш поширеної карти даного виду представлено на рис. 7. Як видно з рис. 7, як основа використовується форма карти загального вигляду з нанесенням на неї параметрів ризику інформаційної безпеки організації за їх кількісною оцінкою.

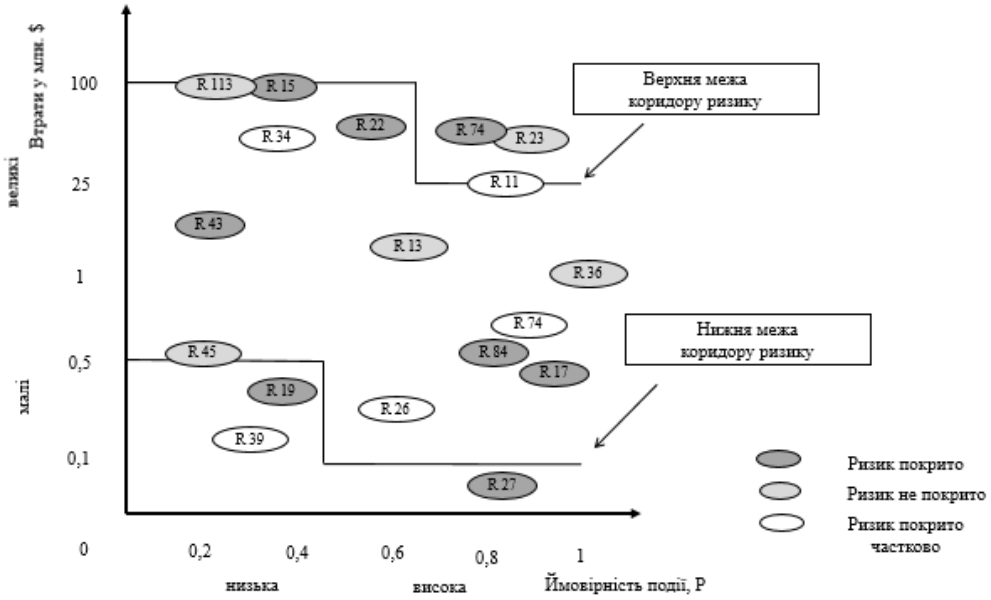


Рисунок 7 – Варіант побудови карти ризиків з урахуванням результатів керування ризиками

Часто в прикладних картах вказуються виявлені ризики інформаційної безпеки організації. Крім цього може зазначатся ступінь покриття кожного ризику: покритий, частково покритий, непокритий. У загальному випадку під покритим ризиком розуміється ризик, щодо якого здійснено керівний вплив. У результаті такого впливу ризик або його наслідки “нейтралізовано”. У вузькому, але більш точному професійному сенсі, під покритим ризиком розуміється оброблений ризик. Якщо на карті ризиків (див. рис. 7) не враховувати забарвння, то отримаємо прикладну карту ризиків організації з нанесенням виявлених ризиків відповідно до оцінки їх параметрів.

Коридор прийнятного рівня ризиків (коридор толерантності ризиків) [6]. Зазначені коридори встановлюються для кожної конкретної організації/підприємства, відповідно до прийнятої стратегії керування ризиками. Це мінімально і максимально можливі значення ризику, що визначають зони його прийнятності. Коридори толерантності встановлюються вищим керівництвом організації/підприємства спільно з прийняттям стратегії керування ризиками та враховуються при прийнятті керівних рішень і в керуванні ризиками. Коридори прийнятного рівня ризику можуть змінюватися не рідше ніж один раз на рік (ризики інформаційної безпеки, згідно [2], повинні переглядатися не рідше одного разу на рік), а за необхідності й частіше. Основне призначення коридорів – встановлення прийнятних для організації/підприємства нижньої і верхньої меж рівня ризику. Як правило, коридори толерантності ризиків “наносяться» на карти ризиків, що допомагає ризик-менеджерам і менеджерам обґрунтовано приймати узгоджені рішення. Приклади варіантів коридорів прийнятного рівня ризику вказані напівжирними лініями на рис. 7 і 8. На рис. 9. приведена карта ризиків для використання при проведенні аналізу ризиків, що включає зони ризиків, коридор прийнятного ризику і відображає результати керування ризиками.

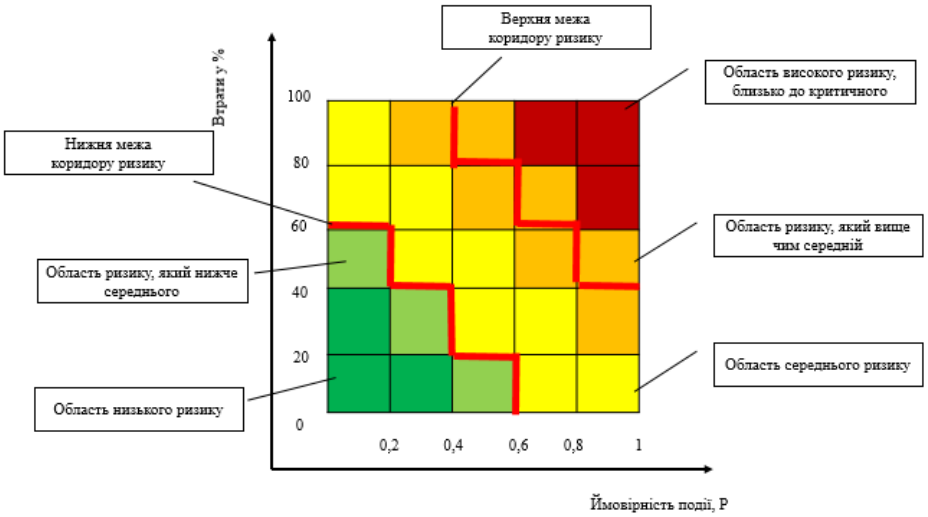


Рисунок 8 – Карта ризику загального вигляду з встановленим коридором зони прийнятного ризику

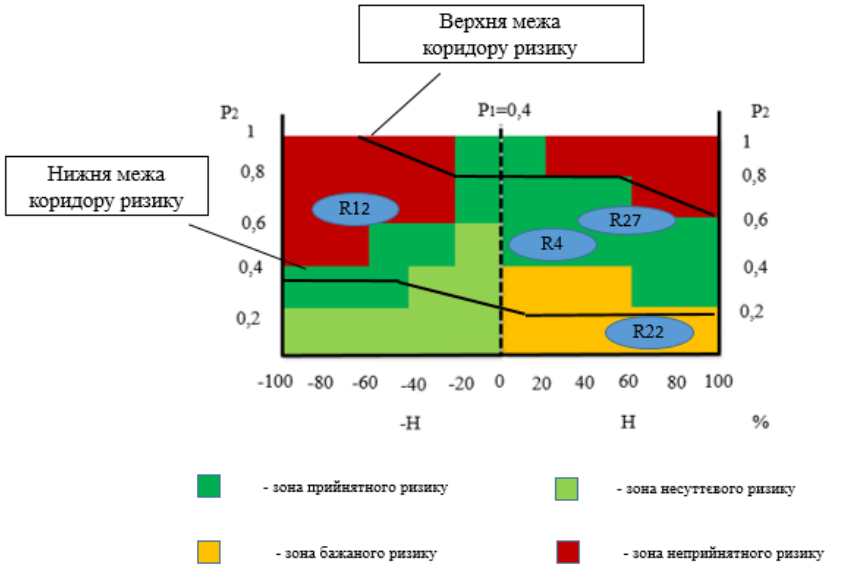


Рисунок 9 – Карта ризику з коридором прийнятності та відображеними ризиками

Висновки. Існує цілий ряд способів задавання вимог до ризиків інформаційної безпеки, що викладено в ряді стандартів з ризик-менеджменту. Серед цих способів – троянда і спіраль ризиків, древо ризиків, карта ризиків і коридори прийнятного рівня ризиків (коридор толерантності ризиків). Найбільш прийнятним на сьогодні є метод використання карт ризиків. Він має ряд переваг, зокрема:

– системне наочне уявлення ризиків відповідно до їх кількісної оцінки;

– зручність використання при моніторингу ризиків, коли за результатами його проведення ризики ”наносяться» на координатну площину, і перегляд карт в динаміці дозволяє візуально системно уявити тенденції зміни ризиків;

– можливість складати карти ризиків для всієї організації в цілому, для окремих бізнес-процесів, бізнес-напрямків, структурних підрозділів підприємства, для окремих груп ризиків;

– застосування універсальної (однотипної) форми карти для груп ризиків, підрозділів і всього підприємства дозволяє об’єднувати, порівнювати, накладати, інтегрувати карти ризиків, що забезпечує отримання нової інформації про ризики, що необхідна для проведення аналізу і прийняття рішень про керування ризиками.

Не дивлячись на досить велику кількість переваг, карти ризиків мають і ряд недоліків, які можуть істотно впливати на процес прийняття рішення, привносячи досить серйозну частку суб'єктивізму при виборі заходів обробляння інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html.

[2] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54533.html.

[3] International Organization for Standardization. (2011, June 10). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/standard/56742.html.

[4] International Organization for Standardization. (2018, Febr. 15). *ISO 31000. Risk management. Guidelines*. [Online]. Available: https://www.iso.org/standard/65694.html.

[5] International Organization for Standardization. (2009, Nov. 27). *IEC 31010. Risk management. Risk assessment techniques.* [Online]. Available: https://www.iso.org/standard/51073.html.

[6] А. Г. Бадалова, и А. В. Пантелеев, Управление рисками деятельности предприятия. Москва, Российская Федерация: Вузовская кника, 2016.

Стаття надійшла до редакції 25 березня 2018 року.

REFERENCE

[1] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html.

[2] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54533.html.

[3] International Organization for Standardization. (2011, June 10). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/standard/56742.html.

[4] International Organization for Standardization. (2018, Febr. 15). *ISO 31000. Risk management. Guidelines*. [Online]. Available: https://www.iso.org/standard/65694.html.

[5] International Organization for Standardization. (2009, Nov. 27). *IEC 31010. Risk management. Risk assessment techniques.* [Online]. Available: https://www.iso.org/standard/51073.html.

[6] A. G. Badalova, and A. V. Panteleev, *Risk management of the enterprise*. Moskow, Russia: Vuzovskaia knika, 2016.

ВЛАДИМИР МОХОР,
АЛЕКСАНДР БАКАЛИНСКИЙ,
ВАСИЛИЙ ЦУРКАН

АНАЛИЗ СПОСОБОВ ПРЕДСТАВЛЕНИЯ ОЦЕНОК РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрены способы представления оценок рисков информационной безопасноти. Среди них выделены дерево рисков, розу (звезду) и спираль рисков, карту рисков и коридор приемлемости рисков. Класический метод построения дерева ориентирован на его использование для представления оценок риска деревом. Его елементами отображены отдельные или группа рисков. Их использование ориентировано на структуризацию и

классификацию рисков. За основу построения рози (звезды) и спирали взято использование круговых диаграм. Этими диаграмами отображены последовательности рассмотрения рисков информационной безопасности. Благодаря этому осуществляется их ранжирование при сравнительному анализе. Розою (звездою) отображается только один параметр риска информационной безопасности среди выбраной совокупности с возможностью наложения отображений одно на другое с разными параметрами. Поэтому использование такого способа представления сводится к построению семейства роз (звезд) оценок рисков информационной безопасности. В тоже время установлено наибольшую распространенность использования карты рисков информационной безопасности среди известных способов их представления. Картою рисков отображаются оценки исходя из вероятности реализации угрозы и величины потерь. Благодаря универсальности такого способа представления возможно объединение, сравнение, наложение и интегрирование карт рисков информационной безопасности. Поэтому среди них выделеяются общие и прикладные карты рисков. Характерною особеностю карт рисков общего вида является наличие или отстутствие шкалы оценивания. При наличии шкалы, величина риска оценивается качественно или количественно. Тогда как в случае ее отсутствия оценка сводится к выделение областей оценок рисков информационной безопасности. наявності шкали величина ризику оцінюється якісно або кількісно. Для каждой из выделеных областей устанавливаются интервальные значения вероятности реализации угрозы и величины риска. Коридор приемлемости рисков информационной безопасности устанавливается индивидуально каждой организации с максимально возможными оценками. Этими оценками определяются зоны приемлемости рисков информационной безопасности. Таким образом, анализ способов представления оценок рисков информационной безопасности деревом, розою (звездою), спираллю, картою и коридором приемлемости позволил установить их преимущества и недостатки. Кроме этого выделить направление дальнейших исследований представления оценок рисков информационной безопасности картою рисков.

Ключевые слова: риск информационной безопасности, оценка риска информационной безопасности, дерево рисков, роза (звезда) рисков, спираль рисков, карта рисков, коридор приемлемости рисков.

VOLODYMYR MOKHOR,
OLEKSANDR BAKALYNSKYI,
VASYL TSURKAN

ANALYSIS OF INFORMATION SECURITY RISK ASSESSMENT REPRESENTATION METHODS

Methods of resenting information security risk assessments are considered. The method are divided into a tree of risks, a rose (star) and a helix of risks, a risk map and an acceptability risk corridor. The classic tree construction method is used to represent tree risk assessments. Its elements show individual risks or group of risks. The rose (star) and a spiral constructing a use as basis for the circular diagrams. These diagrams reflect the sequence of consideration of information security risks. Due to this, their ranking is carried out in a comparative analysis. Rose (star) displays only one of the parameters of the information security risk among the selected set with the ability to overlay maps with one with different parameters. Therefore, the use of such a presentation method is to build a family of roses (stars) of information security risk assessments. At the same time, the most widespread use of information security risk maps among known methods of their presentation is defined. The risk map represents estimates based on the probability of the threat realization and the amount of losses. Due to the versatility of such a way of representation, it is possible to combine, compare, overlay and integrate information security risk maps. Therefore, common and applied risk maps are segregate among them. A characteristic feature of risk maps of the general type is the presence or absence of a scale of evaluation. In the presence of a scale, the risk value is evaluated qualitatively or quantitatively. While in its absence, the assessment is reduced to the

selection of areas of information security risk assessment. For each of the identified areas, the interval values of the probability of the threat realization and the size of the risk are established. Corridor of acceptability of information security risks is set individually for each organization with the most probable estimations. These estimates determine the areas of acceptability of information security risks. Thus, process of analyzing of methods for presenting information security risk assessments by tree, rosy (star), spiral, map and corridor of acceptability allowed to define their advantages and disadvantages. In addition, it allowed to choose the direction of further researches to present information security risk assessments with a risk map.

Keywords: information security risk, information security risk assessment, tree of risks, rose (star), helix of risks, risk map, acceptability risk corridor.

Володимир Володимирович Мохор, член-кореспондент Національної академії наук України, доктор технічних наук, професор, директор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0001-5419-9332.

E-mail: v.mokhor@gmail.com.

Олександр Олегович Бакалинський, начальник відділу, Департамент формування та реалізації державної політики у сфері кіберзахисту Адміністрації Держспецзв'язку, Київ, Україна.

ORCID: 0000-0001-9712-2036.

E-mail: baov@meta.ua.

Василь Васильович Цуркан, кандидат технічних наук, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0003-1352-042X.

E-mail: v.v.tsurkan@gmail.com.

Владимир Владимирович Мохор, член-корреспондент Национальной академии наук Украины, доктор технических наук, профессор, директор, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Александр Олегович Бакалинський, начальник отдела, Департамент формирования и реализации государственной политики в сфере киберзащиты Администрации Госспецсвязи, Киев, Украина.

Василий Васильевич Цуркан, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Volodymyr Mokhor, corresponding member of the National Academy of Sciences of Ukraine, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

Oleksandr Bakalynskyi, head of department, Department of formation and implementation of state policy on cyber protection of Administration of state serves of special communication and information protection of Ukraine, Kyiv, Ukraine.

Vasyl Tsurkan, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.