INFORMATION SECURITY RISK MANAGEMENT

DOI 10.20535/2411-1031.2022.10.2.270437
УДК 004[056.53::413.4]

ВАСИЛЬ ЦУРКАН,
ОЛЕКСАНДР ШАПОВАЛ

АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ РИЗИКУ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Досліджено впровадження систем управління інформаційною безпекою в організації. Виокремлено комп'ютерні мережі як важливі інформаційні активи. Забезпечення непорушності їхніх властивостей досягнуто обиранням відповідних заходів і засобів. Для цього оцінюється ризик безпеки комп'ютерної мережі та, як наслідок, приймається рішення про необхідність його оброблення. Проаналізовано останні дослідження і публікації, за результатами яких встановлено їхню орієнтованість на узагальнене оцінювання ризиків інформаційної безпеки та кібербезпеки. Ними здебільшого залишаються поза увагою особливості збереження властивостей активів, наприклад, комп'ютерних мереж. З огляду на це, розглянуто типовий приклад представлення їхньої структури та виявлено характерні зони та особливості забезпечення безпеки в межах кожної з них. На прикладах продемонстровано наслідки реалізування загроз, зокрема, порушення властивостей конфіденційності, цілісності та доступності. Це дозволило виокремити потенційні області прояву ризику безпеки комп'ютерної мережі відповідно до рівнів моделі взаємодії відкритих систем. Проаналізовано методи оцінювання його величини та встановлено особливості використання кожного з них. Для цього визначаються рівні комунікування і експлуатування, контролювання доступу та активів. Кожен з них розглядається щодо поєднання суб'єктивних і об'єктивних ваг в умовах невизначеності. Крім того, враховується корельованість вузлів відповідно до середовища їхнього експлуатування. Вірогідні напрямки реалізування загроз через уразливості комп'ютерної мережі відображаються графом атак. До того ж долається проблема відсутності інформації про них завдяки врахуванню нечіткості і невизначеності. Додатково виокремлюються аспекти оцінювання ризику безпеки комп'ютерної мережі. Однак, шляхом аналізування відомих методів оцінювання встановлено їхню зосередженість перш за все на виконанні часткових завдань. Насамперед це стосується ідентифікування і визначення оцінок у межах аналізування ризиків. Залишено поза увагою зіставлення результатів оцінювання з прийнятним рівнем. Цим обмежується прийняття і обґрунтування рішення про необхідність оброблення ризику. До того ж урахування властивостей інформації і рівнів моделі взаємодії відкритих систем при її передаванні і забезпеченні безпеки в комп'ютерній мережі.

Ключові слова: інформаційний актив, комп'ютерна мережа, безпека комп'ютерної мережі, ризик безпеки комп'ютерної мережі, оцінювання ризику.

Постановка проблеми. Впровадження систем управління інформаційною безпекою в організаціях зводиться до обирання відповідних заходів зі встановленого набору [1], [2]. При цьому враховується залежність оброблення інформації від застосовності інформаційно-комунікаційних технологій. Вони виокремлюються як один з основних елементів створення, оброблення, зберігання, передавання і знищення інформації [3]. Пов'язані з нею комп'ютерні системи та мережі є важливими інформаційними активами для організацій. Тому успішність упровадження систем управління інформаційною безпекою визначається убудованістю відповідних засобів [4]. Такі засоби обираються протягом оброблення ризиків інформаційної безпеки, зокрема, щодо порушення властивостей інформації у комп'ютерних мережах. Цьому процесу передує оцінювання їхньої величини та як, наслідок, приймання рішення про необхідність оброблення [1], [2], [4].

Отже, аналізування методів оцінювання ризиків безпеки комп'ютерних мереж є актуальним завданням.

Аналіз останніх досліджень і публікацій. Дослідженню методів оцінювання ризиків інформаційної безпеки приділено увагу, наприклад, в [5] - [16]. Теоретичні і практичні аспекти вирішення даного завдання описано в [5]. Проаналізовано понятійний апарат, моделі, методи, нормативні документи та засоби оцінювання ризиків інформаційної безпеки. Запропоновано використання перевизначення еталонів параметрів для розроблення методів модифікування порядку лінгвістичної змінної. Практично продемонстровано оцінювання ризиків безпеки ресурсів інформаційних систем в реальному часі за CVSS (англ. Common Vulnerability Scoring System; укр. загальна система оцінювання уразливостей) метриками. При цьому виокремлено випадки без залучення фахівців з урахуванням як умов, так і шкал представлення отриманих результатів. Способи представлення оцінок ризиків інформаційної безпеки розглянуто в [6], [7]. Насамперед проаналізовано особливості використання дерева, троянди (зірки), спіралі, карти та коридору ризиків. Завдяки цьому встановлено переваги та недоліки кожного з виокремлених способів і, як наслідок, серед них обрано карти ризиків [6]. Встановлено особливості їхнього використання на практиці. Насамперед орієнтованість на визначення прийнятності окремого або групи ризиків інформаційної безпеки в лінгвістичних шкалах. Для цього використано величини ймовірності реалізування загрози та втрат. Водночас показано обмеженість практичного застосування карт ризиків через складність зіставлення отриманих оцінок. Його подолання досягнуто поєднанням лінгвістичних і порядкових шкал оцінювання [7]. Традиційні методи та метричний підхід до оцінювання ризиків поєднано в [8]. Отримані результати перш за все стосуються запобігання перехопленню маршрутів у системі глобальної маршрутизації мережі Інтернет. Цьому передувало класифікування загроз їхній безпеці. З огляду на це, використано комбінований підхід до моделей STRIDE і DREAD. На його основі формально описано двовимірну модель кількісного оцінювання ризику безпеці глобальної маршрутизації. Ризики безпеки промислових систем керування досліджено в [9]. Зосереджено увагу на необхідності їхнього врахування на всіх етапах життєвого циклу. Показано, що ідентифікування, аналізування, зіставлення і, загалом, кількісне оцінювання ризиків життєво важливе для прийняття рішень щодо інвестування у забезпечення безпеки промислових систем керування. Крім того, встановлюється відсутність адекватних (динамічних) методів орієнтованих на врахування особливостей даних систем. Для запобігання цьому пропонуються альтернативні напрями дослідження методів кількісного оцінювання ризиків інформаційної безпеки та кібербезпеки зокрема. Ітерпретаційну модель оцінювання граничних ризиків інформаційної безпеки розроблено в [10]. Її використання дозволяє формулювати вимоги як до комплексних систем захисту інформації, так і систем управління інформаційною безпекою. Величину граничного ризику запропоновано визначати через середньоквадратичне відхилення недоотриманого організацією прибутку протягом встановленого проміжку часу. Теоретичну ієрархію оцінювання ризиків інформаційної безпеки описано в [11]. Для цього виокремлено відповідні моделі, методи та стандарти. Завдяки побудові такої ієрархії запропоновано узагальнену модель оцінювання ризиків інформаційної безпеки. Тоді як стандарти на групи настанов щодо даного процесу, управління ним і принципів його упровадження. На основі даного групування узагальнено методи оцінювання ризиків інформаційної безпеки. Типові настанови щодо впровадження даного процесу проаналізовано в [12]. Сформовано критерії обирання методів оцінювання ризиків інформаційної безпеки та кібербезпеки – від науково-методичного обґрунтування до наявності каталогів загроз, порушників. На основі сформованих критеріїв розглянуто їхню загальну характеристику та виконано порівняльний аналіз. Серед виокремлених методів оцінювання ризиків інформаційної безпеки окрему увагу приділено NIST 800-30, CRAMM, OCTAVE, COBIT, MAGERIT, MEHARI. Використання штучного інтелекту для підтримання даного процесу запропоновано в [13]. Проаналізовано підходи до оцінювання ризиків інформаційної безпеки на основі дослідження систематичного картографування. При цьому враховано тенденції до зростання кількості результатів з 2010 року. Як наслідок, встановлено застосовність для оцінювання ризиків насамперед здійснення вторгнень і впровадження шкідливого програмного забезпечення. Метод дерева атак для визначення характеристик безпеки

інформаційної системи об'єкта критичної інфраструктури використано в [14]. Продемонстровано прямопропорційне збільшення імовірності успіху потенційної атаки до мотивації зловмисника та обернено пропорційне до зусиль її організування. Тому вартість активів, імовірність виникнення та ймовірність успіху атаки є параметрами оцінювання ризиків безпеки інформаційної системи. Взаємодії і взаємозалежності між кібер і фізичними компонентами кібер-фізичних систем досліджено в [15]. Описано проблему використання методів оцінювання ризиків, якими би враховувалися зазначені взаємодії і взаємозалежності. Дане обмеження вдалося подолати розробленням методу на основі залежностей. Ним можливе встановлення вірогідних шляхів реалізування загроз в кібер-фізичних системах з погляду зловмисника.

Отже, за результатами аналізування останніх досліджень і публікацій показано орієнтованість методів на оцінювання ризиків інформаційної безпеки та/або кібербезпеки загалом. При цьому здебільшого поза увагою залишається врахування особливостей збереження властивостей інформаційних активів, зокрема, комп'ютерних мереж.

Метою статті є встановлення особливостей використання відомих методів оцінювання ризику безпеки комп'ютерних мереж.

Виклад основного матеріалу дослідження. Здебільшого організації мають змішану структуру комп'ютерної мережі. Як її приклад розглянуто представлення на рис. 1 [4]. Відповідно до такого представлення, основою внутрішніх комунікацій є мережа інтранет. Крім того обов'язково виокремлюється бездротовий сегмент, який підключений до основної комп'ютерної мережі через систему забезпечення безпеки. При цьому окрема увага приділяється інфраструктурі відкритих ключів. Для голосового спілкування передбачається упровадження IP телефонії. Вона може з'єднуватися зі звичайною (аналоговою) телефонною мережею загального користування або з мережею стільникового зв'язку через GSM-шлюз. Екстранет використовується за потреби надання доступу до внутрішньої мережі зовнішнім зацікавленим сторонам (зокрема, партнерам) і для віддаленої роботи працівників організації.

Сегмент комп'ютерної мережі з доступом до нього з боку зовнішньої мережі виділяється в окрему частину – демілітаризовано зону (англ. Demilitarized Zone, DMZ). В цій частині знаходяться сервери та організовується доступ для віддалених робочих місць з підключенням до внутрішніх серверів за допомогою технологій віртуальних приватних мереж (англ. Virtual Private Network, VPN). Цей сегмент має безпосереднє підключення до мережі Інтернет і через нього проходить весь зовнішній трафік. У ньому розташовуються основні системи забезпечення безпеки. Зазвичай саме ця частина структури комп'ютерної мережі знаходиться в окремому приміщенні – серверній кімнаті. Крім того, у багатьох організаціях є віддалені майданчики (філії, склади, виробництво), які за допомогою технологій віртуальних приватних мереж повинні отримувати доступ до серверної інфраструктури, а також в обов'язковому порядку повинні мати власні системи забезпечення безпеки комп'ютерної мережі.

До того ж сучасні технології дають можливість використовувати велику кількість корисних сервісів, але водночас призводять до появи ризиків. Більшість протоколів при їх розробленні розраховувалися перш за все на швидкість та стабільність встановлення з'єднань. Забезпечення безпеки при цьому залишалося поза увагою, оскільки були відсутні відповідні загрози порушення властивостей інформації. Це важливо насамперед тому, що маючи досить глибокі знання принципів їхньої роботи можливе втручання (реалізування загроз) у комп'ютерні мережі. Несанкціоноване втручання орієнтоване на порушення властивостей конфіденційності, цілісності та доступності інформації. Такі втручання спостерігаються достатньо часто. Їхня ступінь може бути досить великою, що призводить до зупинки великої кількості сервісів, особливо це небезпечно для виробництва та критичної інфраструктури.

Проєктування безпечних середовищ комп'ютерних мереж це завжди прагнення до балансуванням між ризиками безпеки та вигодою у поєданні зі зручністю. Тому для розроблення таких мереж доцільно формулювати вимоги до них шляхом врахування особливостей середовища їхнього використання і, як наслідок, оцінювання ризиків як при створенні, так і експлуатуванні.

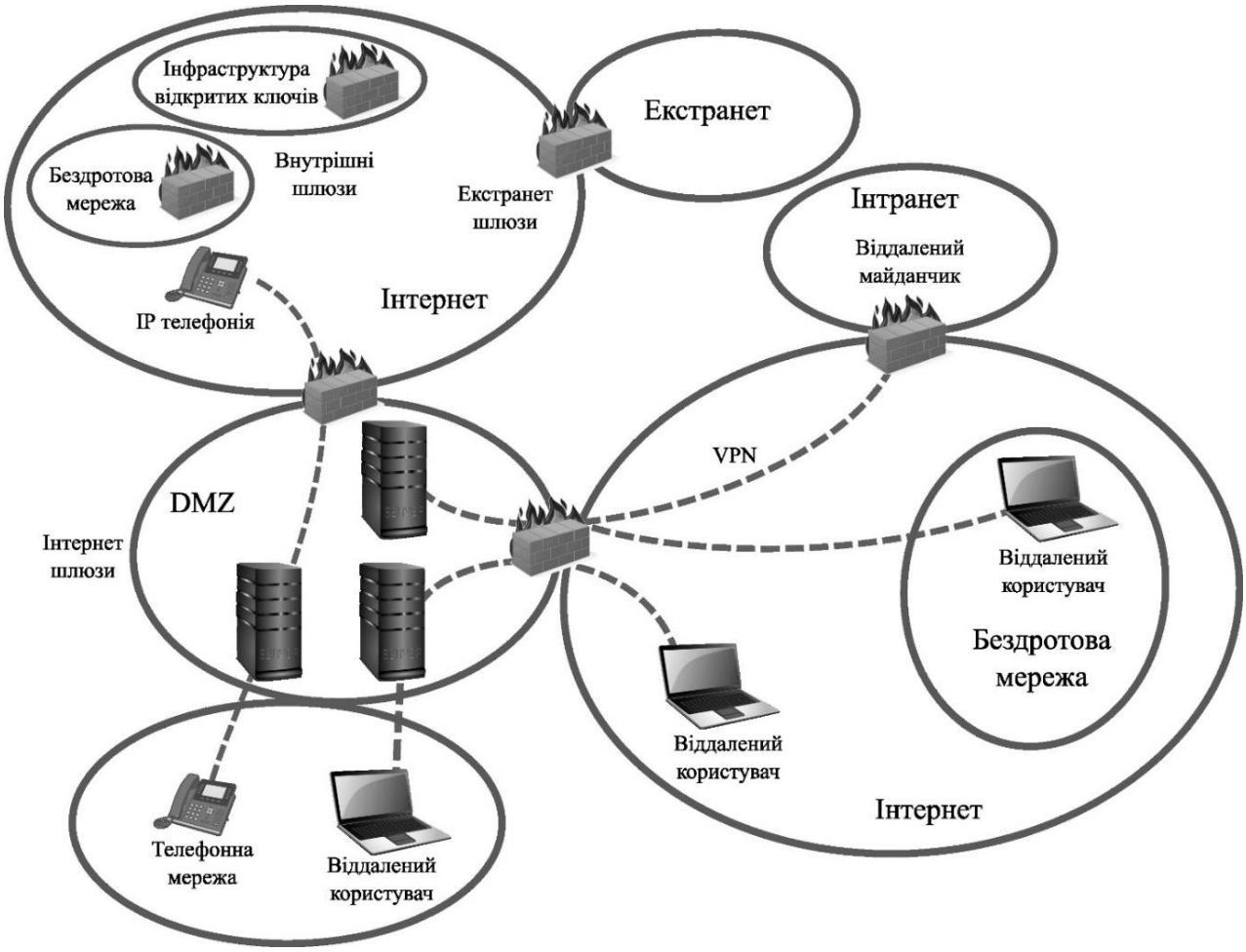

Рисунок 1 – Приклад середовища комп'ютерної мережі організації [4]

Відповідно до рис. 1, для оцінювання ризику рекомендується врахувати, наприклад [4], різновиди архітектур, з'єднань, сервісів та програмних застосунків. На основі отриманої інформації можливе ідентифікування, аналізування, зіставлення ризиків і, як наслідок, обирання заходів і засобів забезпечення збереженості властивостей інформації в комп'ютерній мережі [1], [3]. Серед отриманих обсягів доцільно визначити, яка інформація є найбільш важливою для організації. Саме її безпеку необхідно забезпечити перш за все, зокрема, непорушність конфіденційності, цілісності та доступності за будь-яких як внутрішніх, так і зовнішніх впливів. Для цього до того ж потрібно аналізувати сервіси та програмні застосунки, які мають доступ до неї. Перевіряти наявність у них відомих уразливостей, а також протоколи сервісів на всіх рівнях моделі взаємодії відкритих систем з урахуванням усі етапів з'єднань. Наприклад [4], безпосередньо передавання інформації може бути захищене шифруванням, але на етапі встановлення з'єднання часто використовується незахищені запит-відповідь системи доменних імен (англ. Domain Name System, DNS). При цьому можливе фальсифікування відповіді і, відповідно, неможливість встановлювати з'єднання, тобто порушується властивість доступності важливої інформації.

З погляду забезпечення безпеки з'єднань їх можливо розділити на три різновиди [4]: внутрішні з'єднання (у межах периметру комп'ютерної мережі організації, зазвичай не шифровані), зовнішні з'єднання з використанням технологій захисту трафіку (наприклад VPN), зовнішні з'єднання без використання технологій забезпечення безпеки (з'єднання з віддаленими сервісами, наприклад [4], електронна пошта, вебсерфінг, месенджери). Будь-яке зовнішнє з'єднання обумовлюється необхідністю проведення авторизації користувачів як для самого з'єднання, так і для окремих сервісів виходу за межі внутрішнього периметру

комп'ютерної мережі. Доцільно окремо розглянути з'єднання зі зовнішніх комп'ютерних мереж. Характерною їх особливість є наявність додаткового захисту трафіку. Такі з'єднання здебільшого використовуються працівниками для віддаленого доступу до визначеної частини комп'ютерної мережі та до обмеженого обсягу внутрішніх сервісів.

З урахуванням того, що нині запорукою успішності діяльності будь-якої організації є проєктування і впровадження комп'ютерних мереж доцільно окрему увагу приділяти безпечності встановлення і внутрішніх, і зовнішніх з'єднань. Зосередження такої уваги пов'язане з ризиковістю як з'єднань, так і користувачів з ініціативи яких вони встановлюються. Прикладами ризиків безпеки комп'ютерної мережі можуть бути [4]: несанкціонований доступ до конфіденційної інформації, несанкціоноване передавання інформації, упровадження шкідливого програмного забезпечення, відмовлення в обслуговуванні. Внаслідок їхніх проявів можливі втрачання для діяльності організації [4]:

- цілісності інформації і програмного забезпечення в комп'ютерній мережі;
- конфіденційності інформації і програмного забезпечення в комп'ютерній мережі;
- доступності інформації та послуг як для внутрішніх, так і зовнішніх з'єднань;
- журналів з'єднань і сесій у комп'ютерній мережі, насамперед звернень до баз даних;
- автентичності користувачів, адміністраторів і, внаслідок цього, достовірності інформації, що ними передається;
- контролю санкціонованого доступу до інформації в комп'ютерній мережі;
- контролю використання мережевих та апаратних ресурсів організації (процесорних ресурсів, мережевих ресурсів, накопичувачів інформації).

На рис. 2 представлена схема потенційних областей ризиків безпеки комп'ютерної мережі [4]. Так, з першого по третій рівні моделі взаємодії відкритих систем, вони стосуються порушення конфіденційності, цілісності, доступності та достовірності інформації. Їхнє оброблення досягається здебільшого технічними засобами. Тоді як на вищих – не технічними зокрема. З огляду на це, проаналізовано методи оцінювання їхньої величини [16] - [23].

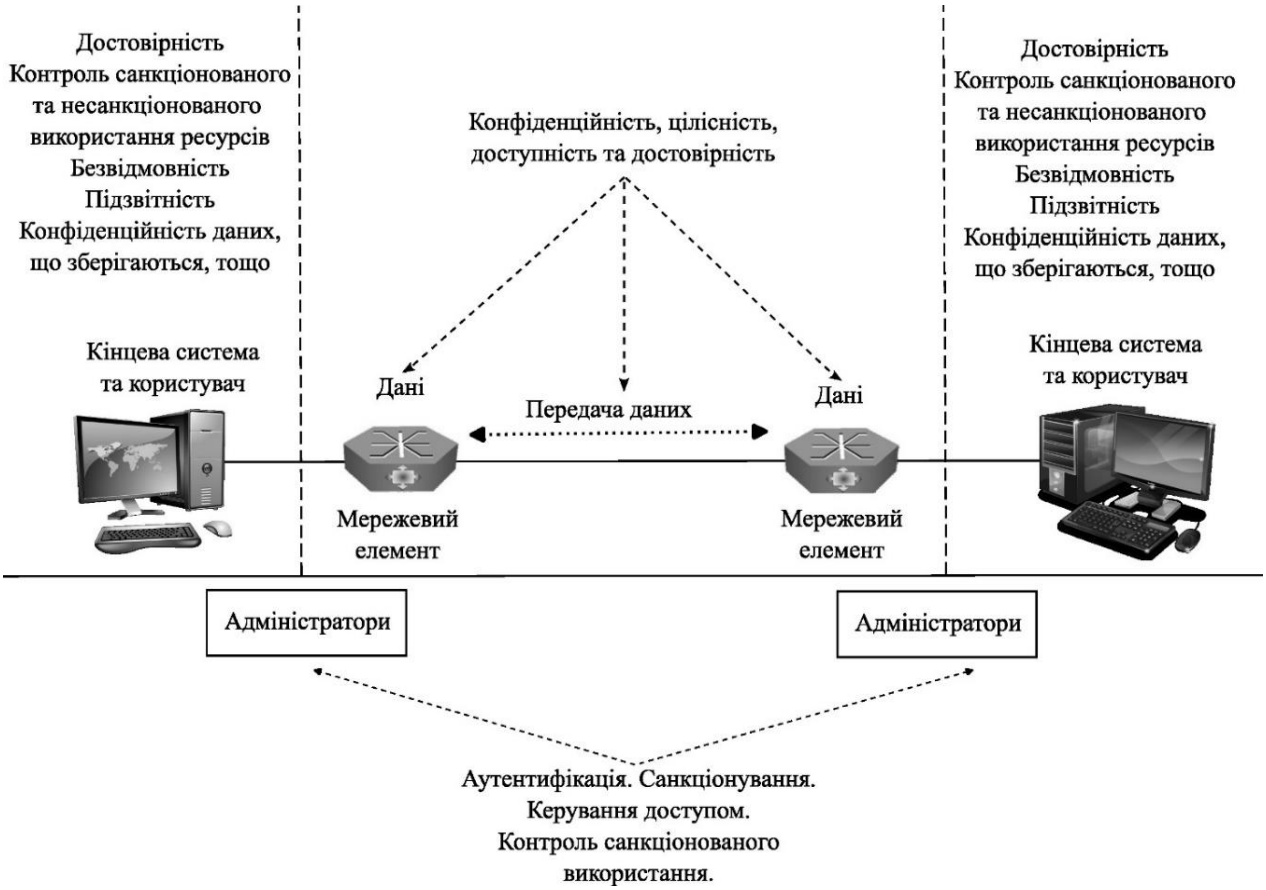

Рисунок 3 – Приклад представлення областей ризику безпеки комп'ютерної мережі [4]

Новий підхід до оцінювання ризику безпеки комп'ютерної мережі запропоновано в [16]. За основу його розроблення взято поєднання суб'єктивних і об'єктивних ваг в умовах невизначеності. Запропонований метод реалізується за шість етапів, відповідно до яких передумовою оцінювання ризику безпеки комп'ютерної мережі на першому етапі є створення моделі її ієрархічної структури. Вона представляється на таких рівнях: комунікування та експлуатування, контролювання доступу, активів. Це обумовлено важливістю врахування кожного з них при збережені властивостей інформації у комп'ютерній мережі. Отримана ієрархічна модель оцінювання ризику використовується експертами на другому етапі для встановлення його значень шляхом декомпозиціювання рівнів "Комунікування та експлуатування", "Контролювання доступу", "Активів". Оцінки отримуються за таким розподілом: дуже низький, низький, середній низький, середній, середній високий, високий, дуже високий. На третьому та четвертому етапах визначаються суб'єктивні та об'єктивні ваги, поєднання яких дозволяє отримати їхню комплексну величину. В межах п'ятого етапу шляхом використання правила комбінування середньозважених отримуються функції маси, на основі яких оцінюється ризик безпеки комп'ютерної мережі.

Корелювання вузлів взято за основу розроблення методу оцінювання ризику безпеки комп'ютерної мережі в [17]. Насамперед це пов'язано з недостатністю уваги до даного аспекту серед типових підходів до розв'язання такого завдання. Величина ризику безпеки вузла в комп'ютерній мережі визначається її середовищем. До того ж на його значення впливає ризик пов'язаних вузлів. З огляду на це їхня величина представляється двома складниками – прямим і непрямим ризиками. Цим обумовлюється доцільність урахування корельованості між вузлами комп'ютерної мережі, зокрема, їхній вплив (залежність) один на одного. Для врахування частки прямого/непрямого впливу на величини ризику використовується функція ваг. На її обирання впливає середовище функціонування комп'ютерної мережі. Це дозволяє отримати об'єктивні дані щодо фактичної ситуації забезпечення збереженості властивостей інформації. Тому ризик безпеки комп'ютерної мережі оцінюється з урахуванням як значення ризику кожного вузла, та і рівня його впливовості.

Міркування Байеса для оцінювання ризику безпеки комп'ютерної мережі використано в [18]. Основними результатами є модель графу атак і E-LOOP алгоритм оцінювання уразливостей. Граф атак реалізується для визначення вірогідних напрямів атак комп'ютерної мережі з огляду на експлуатування її уразливостей. Завдяки цьому можливе встановлення намірів зловмисника за допомогою обчислення імовірності Байеса. Запобігання появі циклів на графах атак досягається використанням запропонованого E-LOOP алгоритму. Для цього введено метрику складності атаки та запропоновано метод її визначення. Доступність уразливості описується на рівнях доступу, складності та автентифікації, значення кожного з яких зведені у відповідній таблиці. Водночас перехід між вузлами графу атак можливий за умови зайнятості батьківського вузла. З ним пов'язується експлуатування уразливості комп'ютерної мережі. Врахування запропонованих показників складності атаки, змінення стану вузла дозволяють знаходити відповідну апостеріорну ймовірність.

Ефективне оцінювання ризику безпеки комп'ютерної мереж реалізовано в [19]. Для цього запропоновано врахувати нечіткість якісного оцінювання та невизначеність, що спричинена відсутністю інформації. Це досягнуто використанням методу багато атрибутного оцінювання кількома особами на основі лінгвістичних змінних Грея. Його використання передбачає визначення елементів безпеки комп'ютерної мережі. Крім того, оцінюють за окремими елементами та, як наслідок, їх ранжують і зіставляють з погляду збереженості властивостей інформації. Однак, виконання даного завдання обмежується різноманітністю суджень експертів. Подолати дане обмеження можливо застосуванням лінгвістичних змінних Грея. Це дозволить уніфікувати аналізування і порівняння результатів оцінювання ризику безпеки комп'ютерної мережі багатьма експертами. Ефективність запропонованого методу визначається розгляданням як індикаторів факторів ризику, а саме: активів, уразливостей, загроз, ризиків.

Метод оцінювання ризику безпеки Ad Hoc мережі досліджено в [20]. За його основу взято твердження про відкритість таких бездротових мереж. Такою особливістю визначаються особливості здійснення атак. Насамперед це проявляється шляхом дотримання зловмисником протоколу зв'язку. Використання такої можливості призводить до викрадення ним інформації або знищення бездротової мережі загалом. Тому виокремлюються ризики на рівнях вузла, зв'язку та мережі. Серед їхніх основних елементів розглянуто активи, вразливості, загрози. Вони визначаються на етапі ідентифікування ризику безпеки бездротової мережі. До того ж враховується наявність уразливостей упроваджених заходів і засобів збереженості властивостей інформації. Імовірність/вірогідність появи подій забезпечення безпеки, зокрема, реалізування загрози через уразливість встановлюється з урахуванням її актуальності. Настання таких подій може призвести до втрат активів, розмір яких залежить від цінності інформації. Отримані значення (імовірності/вірогідності, втрат) використовуються для визначення оцінок ризику. Нею відображаються узагальнені збитки внаслідок пошкодження або втрати активів бездротової мережі.

Використання теорії нечітких множин для оцінювання ризику безпеки комп'ютерної мережі запропоновано в [21]. Для цього аналізуються правила на основі накопичених даних про реалізування загроз. Отримані результати поєднуються з поточними даними та, як наслідок, визначається оцінка ризику безпеки хоста. Нею враховується відкриті сервіси, загроза відкритого сервісу, вразливість хоста для відкриття сервісу, відкриті вразливості хоста, атаки зловмисника через вразливості сервісу, втрати внаслідок атаки зловмисника хоста через уразливості сервісу. Тому оцінка ризику безпеки хоста визначається частотою його атак, ступенем вразливості та ступенем втрат унаслідок реалізування загрози через уразливість. Їхнє застосування узагальнюється для оцінювання збереженості інформації в комп'ютерній мережі загалом. Насамперед встановлюється її структура та кількість хостів. Це важливо при знаходженні функції індексу ризику безпеки хоста та ваги його важливості в структурі комп'ютерної мережі.

Вдосконалення процесу аналітичної ієрархії використано для дослідження методу оцінювання ризику безпеки комп'ютерної мережі в [22]. Перш за все проаналізовано їх різновиди, зокрема, визначення якісних, кількісних, якісно-кількісних оцінок. Ризик безпеки комп'ютерної мережі представлено в трьох аспектах. По-перше, врахування важливості інформаційних активів. По-друге, реалізування загроз через їхні уразливості. Внаслідок цього можливе порушення властивостей інформації і, яка наслідок, нанесення втрат організації. По-третє, урахування уразливостей інформаційних активів, через які можуть реалізовуватися загрози. За даними аспектами встановлюється важливість факторів впливу на безпеку комп'ютерної мережі удосконаленим методом аналітичної ієрархії. Таке удосконалення обумовлене складністю безпосереднього оцінювання ризику. Тому вводиться нечіткий оператор, використання якого відображається на одному з п'яти рівнів з відповідною функцією належності для кожного з них.

Характеристики корпоративного середовища враховано при оцінюванні ризику безпеки комп'ютерної мережі в [23]. Насамперед запропоновано встановлення серйозності вразливості з огляду на економічні втрати організації. Для цього запропоновано набір відповідних показників та забезпечено їхнє інтегрування зі загальною системою оцінювання уразливостей і, як наслідок, вимогами забезпечення безпеки організації. З огляду на це розроблено динамічний метод оцінювання ризику шляхом використання моделі графа байєсівської атаки та комбінування змін середовища комп'ютерної мережі. Використання зазначеної моделі зводиться до встановлення множини атрибутів атаки. Серед них виокремлюються докази реалізувань загроз, що вже відбулися. Вони використовуються для визначення як апріорної, так і апостеріорної імовірностей атакування хоста комп'ютерної мережі за умови володіння доказами впливу на інший її хост. Цим враховуються тенденції виникнення і оброблення ризиків.

Отримані результати аналізування методів оцінювання ризику безпеки комп'ютерної мережі зведемо в табл. 1 [16] - [23]. Для цього використано підхід до їхнього представлення на основі завдань, зокрема, ідентифікування, аналізування (визначення імовірності/ вірогідності, наслідків реалізування загрози; оцінок ризику) і зіставлення [24].

Таблиця 1 – Аналіз застосовності методів оцінювання ризику безпеки комп'ютерної мережі

Метод	Оцінювання ризику безпеки комп'ютерної мережі				
	Ідентифікування ризику	Аналізування ризику			Зіставлення ризику
		Наслідки реалізування загрози	Імовірність/ вірогідність реалізування загрози	Оцінка ризику	
[16]	±	–	–	+	–
[17]	±	–	–	+	–
[18]	±	–	±	+	–
[19]	±	–	–	+	–
[20]	+	+	+	+	–
[21]	±	+	±	+	–
[22]	±	–	–	+	–
[23]	±	±	+	+	–

Висновки. Отже, комп'ютерні мережі є важливими інформаційними активами. Забезпечення їхньої безпеки розглядається як запорука успішності діяльності будь-якої організації. Для цього необхідно впроваджувати відповідні заходи та засоби, обирання яких здійснюється за результатами оцінювання ризику безпеки комп'ютерних мереж. Останні дослідження і публікації за даною тематикою здебільшого орієнтовані на інформаційні активи без урахуванням особливостей збереження їхніх властивостей. Тоді як аналізуванням відомих методів оцінювання ризику безпеки комп'ютерних мереж показано зосередженість на виконанні часткових завдань. Насамперед це стосується ідентифікування і визначення оцінок у межах аналізування ризиків. Водночас встановлено залишення поза увагою виконання окремого завдання щодо їхнього зіставлення з прийнятним рівнем. Цим обмежується прийняття і обґрунтування рішення про необхідність оброблення ризику в комп'ютерній мережі. До того ж урахування властивостей інформації і рівнів моделі взаємодії відкритих систем при її передаванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] International Organization for Standardization. (2013, Dec. 04). *ISO/IEC 27001, Information technology. Security techniques. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Aug 21, 2022.

[2] International Organization for Standardization. (2022, Febr. 15). ISO/IEC 27002, *Information security, cybersecurity and privacy protection. Information security controls*. [Online]. Available: https://www.iso.org/standard/75652.html. Accessed on: Aug 21, 2022.

[3] International Organization for Standardization. (2018, Febr. 07). ISO/IEC 27000, *Information technology. Security techniques. Information security management systems. Overview and vocabulary*. [Online]. Available: https://www.iso.org/standard/75652.html. Accessed on: Aug 21, 2022.

[4] International Organization for Standardization. (2015, Aug. 10; reviewed 2021, Apr. 19). ISO/IEC 27033-1, *Information technology. Security techniques. Network security. Part 1: Overview and concepts*. [Online]. Available: https://www.iso.org/standard/63461.html. Accessed on: Aug 21, 2022.

[5] О.Г. Корченко, С.В. Казмірчук, та Б.Б. Ахметов, *Прикладні системи оцінювання ризиків інформаційної безпеки*: монографія. Київ, Україна: ЦП "Компринт", 2017. [Online]. Available: https://er.nau.edu.ua/handle/NAU/40482. Accessed on: Aug 21, 2022.

[6] В. Мохор, О. Бакалинський, та В. Цуркан, "Аналіз способів представлення оцінок ризиків інформаційної безпеки", *Information Technology and Security*, vol. 6, iss. 1 (10), pp. 75-84, 2018, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.1.153189.

[7] В. Мохор, О. Бакалинський, та В. Цуркан, "Представлення оцінок ризиків інформаційної безпеки картою ризиків", *Information Technology and Security*, vol. 6, iss. 2 (11), pp. 94-104, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.2.153494.

[8] В.Ю. Зубок, "Поєднання традиційних методів і метричного підходу до оцінки ризиків від кібератак на глобальну маршрутизацію", *Реєстрація, зберігання і обробка даних*, т. 21, № 2, с. 41-48, 2019, doi: https://doi.org/10.35681/1560-9189.2019.21.2.180256.

[9] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, "Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges", *Journal of Internet Services and Information Security*, vol. 9, no. 3, pp. 1-22, 2019, doi: http://dx.doi.org/10.22667/JISIS.2019.08.31.052.

[10] В. Безштанько, та Я. Зінченко, "Інтерпретаційна модель оцінювання граничних ризиків інформаційної безпеки", *Information Technology and Security*, vol. 8, iss. 2 (15), pp. 224-231, 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.2.222610.

[11] Z. Ying, Q. Li, S. Meng, Z. Ni, Z. Sun, "A Survey of Information Intelligent System Security Risk Assessment Models, Standards and Methods", in *Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications*. X. Zhang, G. Liu, M. Qiu, W. Xiang, and T. Huang, vol. 322, Eds. Cham: Springer, 2020, pp. 603-611, doi: https://doi.org/10.1007/978-3-030-48513-9_48.

[12] О.В. Потій, Ю.І. Горбенко, О.А. Замула, та К.В. Ісірова, "Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних системах", *Радіотехніка*, вип. 206, с. 5-24, 2021, doi: https://doi.org/10.30837/rt.2021.3.206.01.

[13] G. Erdogan, E. Garcia-Ceja, Å. Hugo, P.H. Nguyen, and S. Sen, "A Systematic Mapping Study on Approaches for Al-Supported Security Risk Assessment", in *Proc. IEEE 45th Annual Computers, Software, and Applications Conference*, Madrid, 2021, pp. 755-760, doi: https://doi.org/10.1109/COMPSAC51774.2021.00107.

[14] І.Д. Горбенко, О.А. Замула, and Ю.С. Осипенко, "Концепція оцінки ризиків кібербезпеки інформаційної системи об'єкта критичної інфраструктури", *Радіотехніка*, вип. 209, с. 118-129, 2022, doi: https://doi.org/10.30837/rt.2022.2.209.12.

[15] A. Akbarzadeh, and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems", *International Journal of Information Security*, 2022. [Online], doi: https://doi.org/10.1007/s10207-022-00608-4. Accessed on: Aug. 28, 2022.

[16] Y. Duan, Y. Cai, Z. Wang, and X. Deng, "A Novel Network Security Risk Assessment Approach by Combining Subjective and Objective Weights under Uncertainty", *Applied Sciences*, vol. 8, iss. 3, pp. 1-20, 2018, doi: https://doi.org/10.3390/app8030428.

[17] Z. Wang, Y. Lu, and J. Li, "Network Security Risk Assessment Based on Node Correlation", *Journal of Physics: Conference Series*, vol. 1069, pp. 1-4, 2018, doi: https://doi.org/10.1088/1742-6596/1069/1/012073.

[18] X. Li, M. Li, and H. Wang, "Research on Network Security Risk Assessment Method Based on Bayesian Reasoning", in *Proc. IEEE 9th International Conference on Electronics Information and Emergency Communication*, Beijing, 2019, pp. 1-7, doi: https://doi.org/10.1109/ICEIEC.2019.8784470.

[19] J. Chen, Z. Zhou, Y. Tang, Y. He, and S. Zhao, "Research on Network Security Risk Assessment Model Based on Grey Language Variables", *IOP Conference Series: Materials Science and Engineering*, vol. 677, iss. 4, pp. 1-7, 2019, doi: https://doi.org/10.1088/1757-899X/677/4/042074.

[20] X. Lei, T. Ma, Z. Niu, C. Ma, and H. Shan, "Research on Ad Hoc Network Security Risk Assessment Method", in *Proc. IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference*, Melbourne, 2020, pp. 2272-2279, doi: https://doi.org/10.1109/ITNEC48623.2020.9085110.

[21] B. Yi, Y. P. Cao, and Y. Song, "Network security risk assessment model based on fuzzy theory", *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 4, pp. 3921-3928, 2020, doi: https://doi.org/10.3233/JIFS-179617.

[22] G. Wang, "Research on Network Security Risk Assessment Method Based on Improved Analytic Hierarchy Process", *International Journal of Network Security*, vol. 23, no. 3, pp. 515-521, 2021, doi: https://doi.org/10.6633/IJNS.202105_23(3).17.

[23] Y. Yang, Z. Yang, Q. Yang, G. Ji, and S. Xue, "Network Security Risk Assessment Based on Enterprise Environment Characteristics", *International Journal of Network Security*, vol. 24, no. 1, pp. 156-165, 2022, doi: https://doi.org/10.6633/IJNS.202201_24(1).18.

[24] International Electrotechnical Commission. (2019, June 17). *IEC 31010, Risk management. Risk assessment techniques*. [Online]. Available: https://www.iso.org/standard/72140.html. Accessed on: Aug 21, 2022.

Стаття надійшла до редакції 28.08.2022.

REFERENCE

[1] International Organization for Standardization. (2013, Dec. 04). *ISO/IEC 27001, Information technology. Security techniques. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Aug 21, 2022.

[2] International Organization for Standardization. (2022, Febr. 15). ISO/IEC 27002, *Information security, cybersecurity and privacy protection. Information security controls*. [Online]. Available: https://www.iso.org/standard/75652.html. Accessed on: Aug 21, 2022.

[3] International Organization for Standardization. (2018, Febr. 07). ISO/IEC 27000, *Information technology. Security techniques. Information security management systems. Overview and vocabulary*. [Online]. Available: https://www.iso.org/standard/75652.html. Accessed on: Aug 21, 2022.

[4] International Organization for Standardization. (2015, Aug. 10; reviewed 2021, Apr. 19). ISO/IEC 27033-1, *Information technology. Security techniques. Network security. Part 1: Overview and concepts*. [Online]. Available: https://www.iso.org/standard/63461.html. Accessed on: Aug 21, 2022.

[5] O. Г. Korchenko, S. V. Kazmirchuk, and B. B. Akhmetov, *Applied information security risk assessment systems: monograph*. Kyiv, Ukraine: Tsentr Polihrafiyi "KOMPRYNT", 2017. [Online]. Available: https://er.nau.edu.ua/handle/NAU/40482. Accessed on: Aug 21, 2022.

[6] V. Mokhor, O. Bakalynskyi, and V. Tsurkan, "Analysis of information security risk assessment representation methods", *Information Technology and Security*, vol. 6, iss. 1 (10), pp. 75-84, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.1.153189.

[7] V. Mokhor, O. Bakalynskyi, and V. Tsurkan, "Risk assessment presentation of information security by the risks map", *Information Technology and Security*, vol. 6, iss. 2 (11), pp. 94-104, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.2.153494.

[8] V.Yu. Zubok, "A combination of traditional methods and a metric approach to assessing the risks from cyber attacks to global routing", *Data Recording, Storage & Processing*, vol. 21, no. 2, pp. 41-48, 2019, doi: https://doi.org/10.35681/1560-9189.2019.21.2.180256.

[9] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, "Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges", *Journal of Internet Services and Information Security*, vol. 9, no. 3, pp. 1-22, 2019, doi: http://dx.doi.org/10.22667/JISIS.2019.08.31.052.

[10] V. Bezshtanko, and Ya. Zinchenko, "Interpretation model of assessments boundary information security risks", *Information Technology and Security*, vol. 8, iss. 2 (15), pp. 224-231, 2020, doi: https://doi.org/10.20535/2411-1031.2020.8.2.222610.

[11] Z. Ying, Q. Li, S. Meng, Z. Ni, Z. Sun, "A Survey of Information Intelligent System Security Risk Assessment Models, Standards and Methods", in *Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications*. X. Zhang, G. Liu, M. Qiu, W. Xiang, and T. Huang, vol. 322, Eds. Cham: Springer, 2020, pp. 603-611, doi: https://doi.org/10.1007/978-3-030-48513-9_48.

[12] O. Potii, Y. Gorbenko, O. Zamula, and K. Isirova, "Analysis of methods for assessing and managing cyber risks and information security", *Radiotekhnika*, no. 206, pp. 5-24, 2021, doi: https://doi.org/10.30837/rt.2021.3.206.01.

[13] G. Erdogan, E. Garcia-Ceja, Å. Hugo, P.H. Nguyen, and S. Sen, "A Systematic Mapping Study on Approaches for Al-Supported Security Risk Assessment", in *Proc. IEEE 45th Annual Computers, Software, and Applications Conference*, Madrid, 2021, pp. 755-760, doi: https://doi.org/10.1109/COMPSAC51774.2021.00107.

[14] I. Gorbenko, O. Zamula, and Yu. Osipenko, "The concept of assessing the risks of cybersecurity of the information system of the critical infrastructure object", *Radiotekhnika*, no. 209, pp. 118-129, 2022, doi: https://doi.org/10.30837/rt.2022.2.209.12.

[15] A. Akbarzadeh, and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems", *International Journal of Information Security*, 2022. [Online], doi: https://doi.org/10.1007/s10207-022-00608-4. Accessed on: Aug. 28, 2022.

[16] Y. Duan, Y. Cai, Z. Wang, and X. Deng, "A Novel Network Security Risk Assessment Approach by Combining Subjective and Objective Weights under Uncertainty", *Applied Sciences*, vol. 8, iss. 3, pp. 1-20, 2018, doi: https://doi.org/10.3390/app8030428.

[17] Z. Wang, Y. Lu, and J. Li, "Network Security Risk Assessment Based on Node Correlation", *Journal of Physics: Conference Series*, vol. 1069, pp. 1-4, 2018, doi: https://doi.org/10.1088/1742-6596/1069/1/012073.

[18] X. Li, M. Li, and H. Wang, "Research on Network Security Risk Assessment Method Based on Bayesian Reasoning", in *Proc. IEEE 9th International Conference on Electronics Information and Emergency Communication*, Beijing, 2019, pp. 1-7, doi: https://doi.org/10.1109/ICEIEC.2019.8784470.

[19] J. Chen, Z. Zhou, Y. Tang, Y. He, and S. Zhao, "Research on Network Security Risk Assessment Model Based on Grey Language Variables", *IOP Conference Series: Materials Science and Engineering*, vol. 677, iss. 4, pp. 1-7, 2019, doi: https://doi.org/10.1088/1757-899X/677/4/042074.

[20] X. Lei, T. Ma, Z. Niu, C. Ma, and H. Shan, "Research on Ad Hoc Network Security Risk Assessment Method", in *Proc. IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference*, Melbourne, 2020, pp. 2272-2279, doi: https://doi.org/10.1109/ITNEC48623.2020.9085110.

[21] B. Yi, Y. P. Cao, and Y. Song, "Network security risk assessment model based on fuzzy theory", *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 4, pp. 3921-3928, 2020, doi: https://doi.org/10.3233/JIFS-179617.

[22] G. Wang, "Research on Network Security Risk Assessment Method Based on Improved Analytic Hierarchy Process", *International Journal of Network Security*, vol. 23, no. 3, pp. 515-521, 2021, doi: https://doi.org/10.6633/IJNS.202105_23(3).17.

[23] Y. Yang, Z. Yang, Q. Yang, G. Ji, and S. Xue, "Network Security Risk Assessment Based on Enterprise Environment Characteristics", *International Journal of Network Security*, vol. 24, no. 1, pp. 156-165, 2022, doi: https://doi.org/10.6633/IJNS.202201_24(1).18.

[24] International Electrotechnical Commission. (2019, June 17). *IEC 31010, Risk management. Risk assessment techniques*. [Online]. Available: https://www.iso.org/standard/72140.html. Accessed on: Aug 21, 2022.

VASYL TSURKAN,
OLEKSANDR SHAPOVAL

ANALYSIS OF COMPUTER NETWORK SECURITY RISK ASSESSMENT METHODS

The implementation of information security management systems in the organization has been studied. Computer networks have been identified as essential information assets. Ensuring the integrity of their properties has been achieved by selecting appropriate measures and tools. For this purpose, the security risk of the computer network is assessed, and a decision is made on the need for processing. The latest research and publications have been analyzed, focusing on the generalized evaluation of information and cyber security risks. They often overlook the peculiarities of preserving the properties of assets, such as computer networks. Therefore, a typical example of their structure representation has been considered, characteristic zones and security features within each have been identified. The consequences of realizing threats, such as confidentiality, integrity, and availability properties, have been demonstrated through examples. This has allowed identifying potential areas of computer network security risk manifestation by model levels of the open systems interaction. The methods for evaluating the magnitude of the risk have been analyzed, and the peculiarities of using each of them have been established. This involves determining communication and exploitation levels, access, asset control and considering the combination of subjective and objective factors in conditions of uncertainty. In addition, the correlation of nodes with their operating environment is considered. The possible directions of threat realization through network vulnerabilities are displayed in an attack graph. The problem of needing more information about them is overcome by considering fuzziness and uncertainty.Furthermore, it has been highlighted aspects of assessing the security risk of the computer. However, by analyzing existing risk assessment methods, it has been found that they mainly focus on performing partial tasks, particularly identifying and estimating risks. Comparing the assessment results with an acceptable level needs to be addressed, limiting the decision-making and justification of the need for risk management. Moreover, it has been considered the properties of information and levels of interaction model of open systems in its transmission and securing in the computer network.

Keywords: information assets, computer network, computer network security, computer network security risk, risk assessment.

Цуркан Василь Васильович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і 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, v.v.tsurkan@gmail.com.

Шаповал Олександр Миколайович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-4960-2235, shapoval72@gmail.com.

Tsurkan Vasyl, candidate of technical sciences, associate professor, 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.

Shapoval Oleksandr, postgraduate student, Institute of special communication and information protection National technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.