DOI: 10.18372/2225-5036.26.14947

ОСОБЛИВОСТІ РОЗПОВСЮДЖЕННЯ РИЗИКО-ОРІЄНТОВАНОГО ПІДХОДУ ДО ОЦІНКИ ВРАЗЛИВОСТІ ОБ'ЄКТІВ КІБЕРЗАХИСТУ

Ігор Рубан[1], Вадим Тютюник[2], Володимир Заболотний[1], Ольга Тютюник[3]

[1]Харківський національний університет радіоелектроніки, Україна
[2]Національний університет цивільного захисту України, Україна
[3]Харківський національний економічний університет імені Семена Кузнеця, Україна

РУБАН Ігор Вікторович, Заслужений працівник освіти України, д.т.н., професор, академік Академії наук прикладної радіоелектроніки

Рік та місце народження: 1968 рік, Україна.
Освіта: Харківське вище військове командно-інженерне училище ракетних військ імені Маршала М.І. Крилова, 1990 рік.
Посада: перший проректор з 2019 року.
Наукові інтереси: кібернетична безпека, методи і засоби цифрової обробки зображень.
Публікації: більше 300 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи, матеріали та тези доповідей на конференціях.
E-mail: ihor.ruban@nure.ua.
Orcid ID: 0000-0002-4738-3286.

ТЮТЮНИК Вадим Володимирович, д.т.н., ст. наук. спів., академік Академії наук прикладної радіоелектроніки.

Рік та місце народження: 1972 рік, м. Запоріжжя, Україна.
Освіта: Харківський військовий університет, 1995 рік.
Посада: начальник кафедри управління та організації діяльності у сфері цивільного захисту з 2017 року.
Наукові інтереси: національна безпека, моніторинг надзвичайних ситуацій, цивільна та інформаційна безпека, автоматизовані системи безпеки.
Публікації: більше 200 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи, матеріали та тези доповідей на конференціях.
E-mail: tutunik_v@ukr.net.
Orcid ID: 0000-0001-5394-6367.

ЗАБОЛОТНИЙ Володимир Ілліч, к.т.н., доцент.

Рік та місце народження: 1948 рік, м. Чернігів, Україна.
Освіта: Військова інженерна академія ім. О.Ф. Можайського, 1972 рік.
Посада: професор кафедри безпеки інформаційних технологій з 2009 року.
Наукові інтереси: комплекси технічного захисту інформації.
Публікації: більше 50 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях та авторські свідоцтва.
E-mail: volodymyr.zabolotnyi@nure.ua.
Orcid ID: 0000-0003-3258-8489.

ТЮТЮНИК Ольга Олександрівна, к.т.н., доцент, член-кореспондент Академії наук прикладної радіоелектроніки.

Рік та місце народження: 1983 рік, м. Харків, Україна.
Освіта: Харківський національний економічний університет імені Семена Кузнеця, 2005 рік.
Посада: доцент кафедри інформатики та комп'ютерної техніки з 2019 року.
Наукові інтереси: системи управління безпекою, проблеми прийняття антикризових рішень.
Публікації: більше 100 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: tutunik.o@ukr.net.
Orcid ID: 0000-0002-3330-8920.

© Ruban I., Tiutiunyk V., Zabolotnyi V., Tiutiunyk O. Vulnerability Assessment of Cyber Defense Objects Based on a Risk-Oriented Approach // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 3, pp. 145-155.

Анотація. *Представлено результати розповсюдження ризико-орієнтованого підходу для оцінки ефективності функціонування системи інформаційної безпеки об'єкту кіберзахисту (ОКЗ) в умовах можливого розголошення та витоку інформації, її блокування та модифікаціції. Показано, що основою системи інформаційної безпеки ОКЗ є класичний контур управління, який забезпечує збір, обробку та аналіз інформації, а також моделювання розвитку інформаційної небезпеки на ОКЗ та розробку й реалізацію антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків. На базі отриманих результатів розроблено структурно-логічну схему процесу антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації наслідків загроз. Розроблена схема антикризового управління включає діагностику кризового стану ОКЗ, визначення цілей, завдань і суб'єкту антикризового управління, оцінювання часових обмежень та ресурсного потенціалу, а також розробку та упровадження антикризової програми щодо запобігання виникнення загроз для інформації.*

Ключові слова: *об'єкт кіберзахист, оцінка вразливості, ризико-орієнтований підхід, система інформаційної безпеки, антикризове управління***.**

Вступ

Територія України, як природно-техногенно-соціальна система з рознесеними у просторі і часі параметрами, у процесі життєдіяльності потребує забезпечення нормальних умов функціонування об'єктів критичної інфраструктури, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення.

Виведення з ладу або порушення функціонування цих об'єктів може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, а також заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [1–3].

До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які: 1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Ці об'єкти у процесі свого функціонування потребують забезпечення відповідного рівня їх кіберзахисту, шляхом комплексної реалізації організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації.

Об'єктами кіберзахисту в державі є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [4–6].

Актуальними при реалізації відповідної системи безпеки ОКЗ є наукові дослідження спрямовані на розвиток науково-технічних основ раннього виявлення загроз та попередження виникнення різного роду небезпек для ОКЗ, які свідчать про необхідність проведення оцінки вразливості ОКЗ та встановлення для цих об'єктів ризику виникнення різного роду загроз [7–12].

Аналіз існуючих досліджень

Для отримання порівняльної оцінки рівня небезпеки для ОКЗ в умовах прояву різної природи загроз слід використовувати наступні методи: статистичний, що базується на аналізі даних статистики виникнення загроз протягом кількох років для визначення показників небезпеки ОКЗ; імовірний, оснований на застосуванні математичних моделей, які пов'язують передумови до виникнення загроз із можливістю їх прояву; експертний, що базується на експертному оцінюванні у поєднанні з теорією нечітких множин.

Перевагою статистичного методу є об'єктивність. Імовірний та експертний методи дозволяють враховувати джерела потенційної небезпеки, які рідко проявляються у формі небезпеки, але наслідки від якої є катастрофічними для нормального функціонування ОКЗ.

Однак імовірнісний метод є надзвичайно громіздким і трудомістким, вимагає великого числа вихідних даних, що призводить до низької точності одержуваних результатів.

За відсутністю апробованих математичних моделей і досить достовірних та формалізованих вихідних даних для них, оцінку впливу на умови нормального функціонування ОКЗ великого числа потужних небезпек доцільно проводити експертним методом [13, 14]. Використаний у роботах [15–17] ризико-орієнтований підхід поряд з оцінкою рівня

загроз потребує визначення збитків від наслідків небезпек.

Він може бути застосованим, насамперед, для наукового обґрунтування прийнятного рівня безпеки функціонування ОКЗ та прийняття рішень щодо розміщення нових ОКЗ і розширення або зміни профілю діючих.

Метою цієї роботи є розробка системи критеріїв оцінювання ефективності функціонування системи інформаційної безпеки ОКЗ шляхом проведення наукових досліджень, спрямованих на розповсюдження ризико-орієнтованого підходу для оцінки вразливості ОКЗ.

Основна частина дослідження

Забезпечення належного рівня безпеки функціонування ОКЗ в умовах імовірнісного прояву великої кількості загроз небезпек для інформації, що циркулює у процесі функціонування ОКЗ, є перше черговою задачею ефективної системи інформаційної безпеки цього об'єкту, основу створення якої, як показано у роботах [2, 3], має складати класичний контур управління – рис. 1.

Перший рівень – це пристрої реєстрації факторів загроз для інформації, що циркулює у процесі функціонування ОКЗ. Вони призначені для контролю поодиноких або відразу декількох параметрів та рознесені у просторі по горизонталі й по вертикалі. При цьому, отримана засобами контролю первинна інформація про фактори загроз для інформації, що циркулює у процесі функціонування ОКЗ, по кабелях або радіоканалу транслюється до пристроїв другого рівня, призначених виконувати обробку отриманої інформації та представляти її у вигляді, необхідному для третього рівня. Обробка отриманої інформації може виконуватися як в одному місці, так і на декількох, залежно від конкретної підсистеми моніторингу системи безпеки ОКЗ та розмірів контрольованого підсистемою моніторингу зони інформаційної безпеки ОКЗ.

Оброблена інформація у відповідному вигляді потрапляє до третього рівня, де виконується аналіз отримуваної інформації та систематизація даних, на основі якої робиться висновок про стан небезпеки для інформації, що циркулює у процесі функціонування ОКЗ.

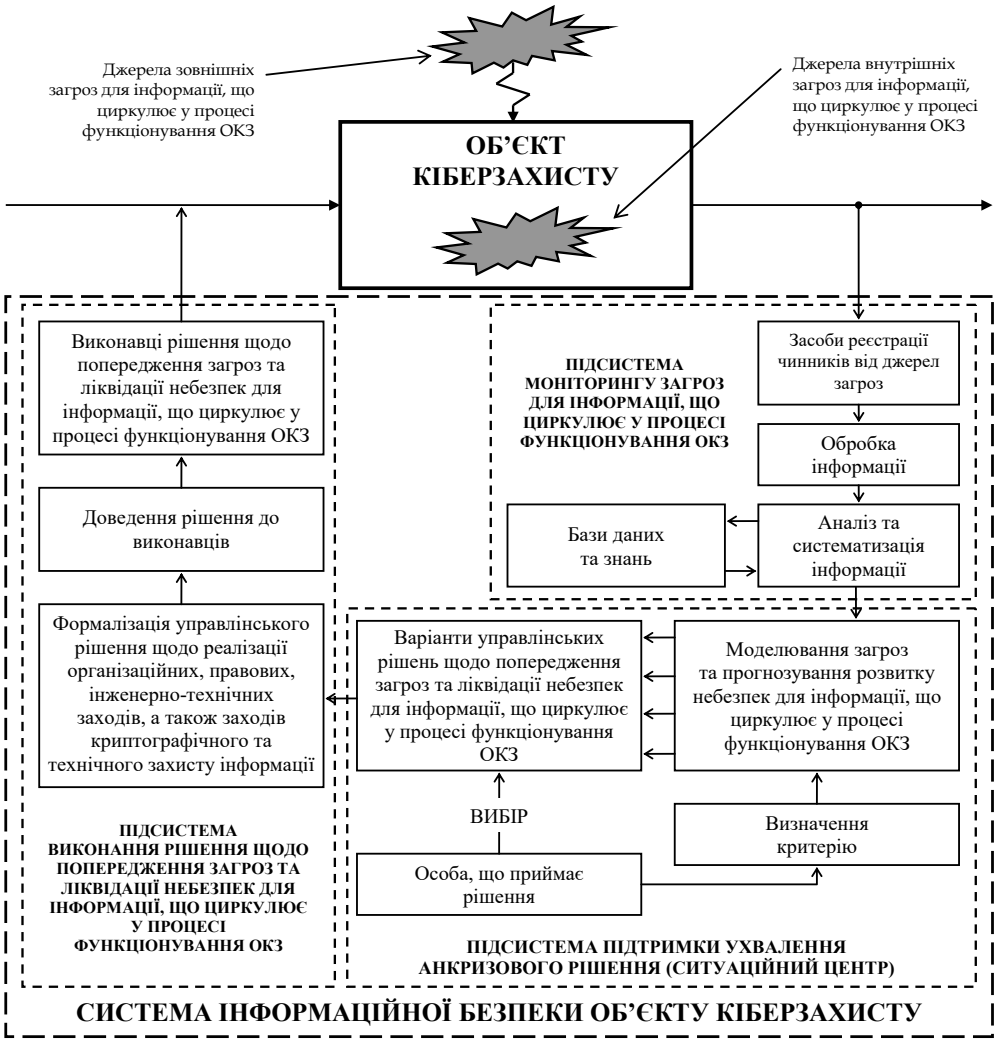

Рис. 1. НКК для дослідження рівня захищеності об'єкта КІ

Використання автоматизованих засобів обробки інформації дозволяє прискорити процеси на другому та третьому рівнях підсистеми моніторингу системи безпеки ОКЗ, а також створити електронні, доступні в

реальному масштабі часу, бази даних та знань. Розробка спеціального програмного забезпечення та навчання персоналу для цих цілей дозволяє на основі отриманої інформації виконувати моделювання загрози та здійснювати прогнозування її розвитку до рівня небезпеки для інформації, що циркулює у процесі нормального функціонування ОКЗ, при цьому графічно (у тому числі у вигляді електронних карт) відображати прогнозовану динаміку небезпечних для ОКЗ подій.

Інша інформаційна система, яка, як показано на рис. 1, є системою підтримки ухвалення антикризового рішення. Тут особа, що приймає рішення, визначає один або декілька критеріїв, відповідно до яких здійснюється прогностичне моделювання розвитку небезпек для інформації, що циркулює у процесі функціонування ОКЗ, та виробляються варіанти управлінських рішень, які обґрунтовані відповідними розрахунками. Отримавши набір варіантів управлінських антикризових рішень, особа, що приймає рішення, обирає один з них або задає ще додаткові критерії, відповідно до яких виконується моделювання та розробка управлінських рішень, направлених на недопущення розвитку небезпеки до рівня інформаційної катастрофи для ОКЗ, або, якщо катастрофи вже не уникнути, то виконується розробка управлінських рішень, спрямованих на мінімізацію наслідків від неї.

Затверджене вказаною вище особою антикризове рішення потрапляє до системи виконання рішення, де виконується його формалізація та доведення до виконавців, які, у свою чергу, впливають на джерела інформаційної небезпеки, які виникли на ОКЗ. Зміни стану ОКЗ та зміни стану інформаційної небезпеки на ньому викликатимуть зміни у величинах вимірюваних параметрів, що фіксуються пристроями контролю. Надалі ці зміни будуть відпрацьовані, а подальше моделювання покаже ефективність виконання управлінського антикризового рішення – контур управління рівнем інформаційної безпеки функціонування ОКЗ замкнувся.

З метою оцінки ефективності функціонування системи інформаційної безпеки об'єкту кіберзахисту та базуючись на основних постулатах ризико-орієнтованого підходу, показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, можливо представити як:

$$R_{ОКЗ}^{Інформац.} = \sum_{i=1}^{3} R_{ОКЗ_i}^{Інформац.}, \quad (1)$$

де $R_{ОКЗ_1}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується розголошенням інформації;

$R_{ОКЗ_2}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації;

$R_{ОКЗ_3}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування.

Під розголошенням інформації мається на увазі навмисні або випадкові дії співробітників, що призвели до ознайомлення з конфіденційною інформацією осіб, які не мають до неї доступу.

Цей вид інформаційної небезпеки реалізується через передачу, надання та пересилання повідомлень каналами їх поширення.

Під витоком інформації мається на увазі безконтрольне виведення конфіденційної інформації за межі організації або кола осіб, яким її було довірено.

Показник ризику для інформації, що обертається у процесі функціонування ОКЗ, який характеризується витоком інформації, включає наступні складові:

$$R_{ОКЗ_2}^{Інформац.} = \sum_{m=1}^{4} R_{ОКЗ_{2.m}}^{Інформац.}, \quad (2)$$

де $R_{ОКЗ_{2.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по технічним каналам;

$R_{ОКЗ_{2.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по каналам зв'язку;

$R_{ОКЗ_{2.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації;

$R_{ОКЗ_{2.4}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається.

Показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по технічним каналам, включає наступні складові:

$$R_{ОКЗ_{2.1}}^{Інформац.} = \sum_{n=1}^{4} R_{ОКЗ_{2.1.n}}^{Інформац.}, \quad (3)$$

де $R_{ОКЗ_{2.1.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу;

$R_{ОКЗ_{2.1.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу;

$R_{ОКЗ_{2.1.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по параметричному каналу (перехоплення інформації шляхом «високочастотного опромінення» технічних засобів прийому, обробки та зберігання інформації);

$R_{ОКЗ_{2.1.4}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по вібраційному каналу (аналіз відповідності між символом, що друкується, і його акустичним образом).

Показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу, включає наступні складові:

$$R_{ОКЗ_{2.1.1}}^{Інформац.} = \sum_{p=1}^{3} R_{ОКЗ_{2.1.1.p}}^{Інформац.}, \quad (4)$$

де $R_{ОКЗ_{2.1.1.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу за рахунок електромагнітного випромінювання елементів технічних засобів прийому, обробки та зберігання інформації;

$R_{ОКЗ_{2.1.1.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу за рахунок електромагнітні випромінювання на частотах роботи високочастотних генераторів засобів прийому, обробки та зберігання інформації;

$R_{ОКЗ_{2.1.1.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу за рахунок випромінювання на частотах самозбудження підсилювачів низької частоти.

Показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу, включає наступні складові:

$$R_{ОКЗ_{2.1.2}}^{Інформац.} = \sum_{w=1}^{4} R_{ОКЗ_{2.1.2.w}}^{Інформац.}, \quad (5)$$

де $R_{ОКЗ_{2.1.2.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок наведення електромагнітних випромінювань елементів технічних засобів прийому, обробки та зберігання інформації на сторонні провідники;

$R_{ОКЗ_{2.1.2.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок просочування інформаційних сигналів в лінії електроживлення;

$R_{ОКЗ_{2.1.2.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок просочування інформаційних сигналів у коло заземлення;

$R_{ОКЗ_{2.1.2.4}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу за рахунок знімання інформації з використанням закладних пристроїв.

Показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по каналам зв'язку, включає наступні складові:

$$R_{ОКЗ_{2.2}}^{Інформац.} = \sum_{q=1}^{4} R_{ОКЗ_{2.2.q}}^{Інформац.}, \quad (6)$$

де $R_{ОКЗ_{2.2.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електромагнітному каналу зв'язку, а саме електромагнітні випромінювання передавачів зв'язку, модульовані інформаційним сигналом (прослуховування радіотелефонів, стільникових телефонів, радіорелейних ліній зв'язку);

$R_{ОКЗ_{2.2.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по електричному каналу зв'язку, а саме підключення до ліній зв'язку;

$R_{ОКЗ_{2.2.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по індукційному каналу зв'язку, а саме ефект виникнення навколо високочастотного кабелю електромагнітного поля при проходженні інформаційних сигналів;

$R_{ОКЗ_{2.2.4}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації по паразитному каналу зв'язку, а саме паразитні ємнісні, індуктивні і резистивні зв'язку і наведення близько розташованих один від одного ліній передачі інформації.

Показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації, включає наступні складові:

$$R_{ОКЗ_{2.3}}^{Інформац.} = \sum_{d=1}^{5} R_{ОКЗ_{2.3.d}}^{Інформац.}, \quad (7)$$

де $R_{ОКЗ_{2.3.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по акустичному каналу, де середовищем поширення є повітря;

$R_{ОКЗ_{2.3.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по віброакустичному каналу, де середовищем поширення є огороджувальні будівельні конструкції; $R_{ОКЗ_{2.3.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по параметричному каналу (результат впливу акустичного поля на елементи схем, що призводить до модуляції високочастотного сигналу інформаційним);

$R_{ОКЗ_{2.3.4}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по акустоелектричному каналу (перетворення акустичних сигналів в електричні);

$R_{ОКЗ_{2.3.5}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком мовної інформації по оптико-електронному (лазерному) каналу (опромінення лазерним променем вібруючих поверхонь).

Показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається, включає наступні складові:

$$R_{ОКЗ_{2.4}}^{Інформац.} = \sum_{f=1}^{3} R_{ОКЗ_{2.4.f}}^{Інформац.}, \quad (8)$$

де $R_{ОКЗ_{2.4.1}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається шляхом спостереження за об'єктами (для спостереження днем застосовуються оптичні прилади і телевізійні камери; для спостереження вночі – прилади нічного бачення, тепловізори, телевізійні камери);

$R_{ОКЗ_{2.4.2}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається шляхом зйомки об'єктів (для зйомки об'єктів використовуються телевізійні і фотографічні засоби; для зйомки об'єктів в день з близької відстані застосовуються портативні камуфльовані фотоапарати і телекамери, суміщені з пристроями відеозапису);

$R_{ОКЗ_{2.4.3}}^{Інформац.}$ – показник ризику для інформації, що циркулює у процесі функціонування ОКЗ, який характеризується витоком інформації, що відображається шляхом зйомки документів (зйомка документів здійснюється з використанням портативних фотоапаратів).

Показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, включає наступні складові:

$$R_{ОКЗ_3}^{Інформац.} = \sum_{k=1}^{3} R_{ОКЗ_{3.k}}^{Інформац.}, \quad (9)$$

де $R_{ОКЗ_{3.1}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується втратою інформації;

$R_{ОКЗ_{3.2}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується зміною інформації;

$R_{ОКЗ_{3.3}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації.

Найбільш небезпечним з позицій інформаційної безпеки в даний час вважається несанкціонований доступ до комп'ютерної інформації.

Показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації, включає наступні складові:

$$R_{ОКЗ_{3.3}}^{Інформац.} = \sum_{g=1}^{9} R_{ОКЗ_{3.3.g}}^{Інформац.}, \quad (10)$$

де $R_{ОКЗ_{3.3.1}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом перегляду інформації (на екранах комп'ютерів, на друкуючих пристроях тощо);

$R_{ОКЗ_{3.3.2}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом копіювання програм і даних (копіювання з інформаційних носіїв і жорстких дисків при слабкому захисті комп'ютерів, при поганій організації зберігання копій і архівів, при читанні даних по лініям зв'язку в мережах, при отриманні інформації за рахунок встановлення спеціальних закладок тощо);

$R_{ОКЗ_{3.3.3}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни потоку повідомлень (в тому числі застосування закладок, що змінюють передану інформацію, при тому, що на екрані вона залишається без змін);

$R_{ОКЗ_{3.3.4}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни конфігурації комп'ютерних засобів (зміна прокладки кабелів, зміна комплектації комп'ютерів і периферійних пристроїв під час технічного обслуговування, завантаження сторонньої операційної системи для доступу до інформації, встановлення додаткового порту для зовнішнього пристрою тощо);

$R_{ОКЗ_{3.3.5}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом зміни розташування комп'ютерних засобів та/або режиму обслуговування та умов експлуатації. Це – установка додаткових пристроїв поблизу комп'ютерів (систем пожежної та охоронної сигналізації, телефонних мереж, систем електроживлення тощо), зміни розташування комп'ютерів для поліпшення доступу до інформації (візуального спостереження);

$R_{ОКЗ_{3.3.6}}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом несанкціонованої модифікації контрольних процедур (наприклад, при перевірці аутентичності електронного підпису, якщо він виконується програмними засобами);

$R_{ОКЗ3.3.7}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом підробки та/або додавання об'єктів, які не є легальними, але володіють основними властивостями легальних об'єктів (наприклад, додавання підроблених записів в файл). Особливо це небезпечно при використанні систем автоматизованого обліку різних об'єктів;

$R_{ОКЗ3.3.8}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом додавання фальшивих процесів та/або підміна справжніх процесів обробки даних фальшивими. Це відноситься як до роботи операційних систем, так і особливо до роботи пакетів прикладних програм;

$R_{ОКЗ3.3.9}^{Інформац.}$ – показник ризику для комп'ютерної інформації, що циркулює у процесі функціонування ОКЗ, який характеризується отриманням несанкціонованого доступу до інформації шляхом фізичного руйнування апаратних засобів або переривання функціонування комп'ютерних засобів різними способами з метою часткового або повного знищення інформації, що зберігається.

При цьому складові ризику для інформації, що циркулює у процесі функціонування ОКЗ, обчислюють за формулою:

$$R_{ОКЗi.j}^{Інформац.} = P_{ОКЗi.j}^{Інформац.} \cdot U_{ОКЗi.j}^{Інформац.}, \quad (11)$$

де $P_{ОКЗi.j}^{Інформац.}$ – оцінка ймовірності перевищення нормативного показника для j-го аспекту і-го процесу небезпеки для інформації, що циркулює у процесі функціонування ОКЗ;

$U_{ОКЗi.j}^{Інформац.}$ – оцінка збитку від перевищення нормативного показника впливи j-го аспекту і-го процесу небезпеки для інформації, що циркулює у процесі функціонування ОКЗ.

При одночасному впливі на інформацію, що циркулює у процесі функціонування ОКЗ, декількох процесів небезпеки, необхідно враховувати можливість прояву синергетичного ефекту [18–20].

У цьому випадку імовірність перевищення нормативного показника для двох спільних аспектів небезпеки для інформації, що обертається у процесі функціонування ОКЗ, можна розрахувати як:

$$P_{ОКЗ_{i.j}}^{Інформац.} = P_{ОКЗ_{i.1}}^{Інформац.} + P_{ОКЗ_{i.2}}^{Інформац.} - \\ -P_{ОКЗ_{i.1}}^{Інформац.} \cdot P_{ОКЗ_{i.2}}^{Інформац.}. \quad (12)$$

Оцінку збитку від перевищення нормативного показника обчислюють як суму збитку вид складових небезпеки для інформації, що циркулює у процесі функціонування ОКЗ.

Загальний очікуваний збиток $U_{ОКЗ}^{Інформац.}$ визначають за формулою:

$$U_{ОКЗ}^{Інформац.} = \sum_{i,j} U_{ОКЗi.j}^{Інформац.}, \quad (13)$$

де $U_{ОКЗ}^{Інформац.}$ – математичне очікування загального економічного збитку ОКЗ від процесів небезпеки для інформації, що циркулює у процесі функціонування ОКЗ;

$U_{ОКЗi.j}^{Інформац.}$ – математичне очікування збитку ОКЗ за ризиком j-го аспекту і-го процесу небезпеки для інформації, що циркулює у процесі функціонування ОКЗ.

Виходячи з представленого у вигляді виразів (1)–(13) матеріалу щодо розповсюдження ризико-орієнтованого підходу для оцінки вразливості ОКЗ та базуючись на основних постулатах теорії систем та

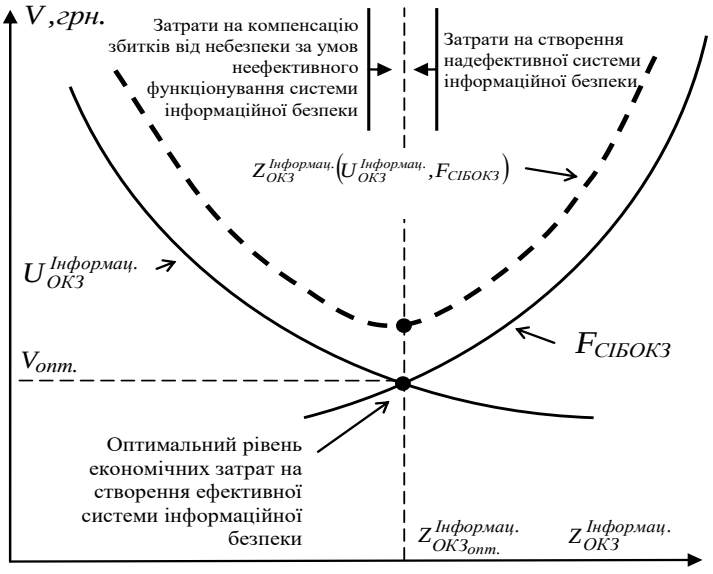

Рис. 2. Співвідношення між рівнем захищеності ($Z_{ОКЗ}^{Інформац.}$) та вартістю (V) захисту об'єкту кіберзахисту

синергетики [2, 18-22], рівень захищеності ОКЗ в умовах імовірнісного прояву різного роду аспектів процесу інформаційної небезпеки, а також економічної ефективності функціонування системи інформаційної безпеки об'єкту кіберзахисту – $F_{СІБОКЗ}$, можливо представити у вигляді даних рис. 2 та записати у вигляді рівняння:

$$Z_{ОКЗ}^{Інформац.} = \varphi\left(U_{ОКЗ}^{Інформац.}, F_{СІБОКЗ}\right). \qquad (14)$$

Вираз (14) представлено у вигляді загального функціоналу, вирішення якого можливо при проведенні аудиту щодо стану захищеності в умовах імовірнісного прояву різного роду аспектів процесу інформаційної небезпеки конкретного об'єкту кіберзахисту.

Процес антикризового управління в умовах ризику або загроз для інформації, що циркулює у процесі функціонування ОКЗ, ситуаційним центром (який, згідно даних рис. 1, є складовою системи інформаційної безпеки ОКЗ) реалізується згідно представленому на рис. 3 алгоритму.

Так, діагностика (на базі наведеного у вигляді виразів (1)–(13) ризико-орієнтованого підходу) кризового стану й загрози для інформації, що циркулює у процесі функціонування ОКЗ, може здійснюватися безпосередньо співробітниками служби безпеки ОКЗ чи зовнішніми незалежними експертами.

Результати діагностики допомагають установити ступінь небезпеки для інформації та для повсякденного функціонування ОКЗ, а отже — визначити цілі й завдання антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

Залежно від ступеню небезпеки такими завданнями можуть бути: виведення ОКЗ зі стану існування загроз для інформації; недопущення виникнення небезпеки для інформації; локалізація існуючих загроз для інформації, стабілізація процесу функціонування ОКЗ, запобігання повторенню кризи.

На етапі визначення суб'єкта антикризової діяльності щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків необхідно встановити суб'єкт, який бере на себе відповідальність за розроблення й реалізацію антикризових процедур, та його повноваження.

На етапі оцінювання часових обмежень процесу антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків визначається час, наявний у ОКЗ для вжиття запобіжних заходів.

Часові обмеження залежать від інтенсивності поширення загроз для інформації.

Розуміння цього сприяє недопущенню подальшого поглиблення кризи, оскільки подолання глибшої кризи пов'язане з більшими витратами й труднощами.

У разі реальної загрози для інформації, що циркулює у процесі функціонування ОКЗ, стає жорстким обмеженням, набуває центрального значення.

Це робить необхідним прогнозування розмірів соціальних, матеріальних та екологічних збитків у наслідок розголошенням та витоку інформації, а також виникнення небезпек для комп'ютерної інформації.

Наступним етапом є оцінювання (за базі наведеного на рис. 2 підходу щодо визначення оптимального рівня затрат на створення системи інформаційної безпеки за функціонально-вартісним критерієм від рівня економічного збитку в умовах виникнення небезпеки для інформації – точка перетину кривих $F_{СІБОКЗ}$ і $U_{ОКЗ}^{Інформац.}$) ресурсного потенціалу антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

Фахівці в галузі безпеки розглядають ОКЗ як систему ресурсів, що взаємодіють між собою та забезпечують досягнення певних результатів щодо досягнення необхідного рівня інформаційної безпеки. Основними видами ресурсів є технічні, технологічні, кадрові, просторові, ресурси організаційної структури системи управління, інформаційні, фінансові тощо.

Розроблення антикризової програми ОКЗ становить обґрунтовану сукупність заходів, що мають бути вжиті для досягнення визначених цілей та виконання завдань антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування об'єкту кіберзахисту, а також ліквідації або мінімізації їх наслідків. Зміст програми обумовлюється результатами проведеної діагностики, часовими й ресурсними обмеженнями антикризового процесу.

У її складі зазвичай виділяють окремі антикризові політики — сукупність дій, засобів та інструментів досягнення певних результатів. Після розроблення антикризової програми настає етап безпосереднього впровадження антикризової програми щодо реалізації організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, а також контролю за її виконанням.

Найважливішою управлінською функцією на цьому етапі є організація контролю за виконанням антикризової програми для своєчасної модернізації або корегування розробленої політики (процедур, заходів) у зв'язку з не прогнозованими збуреннями у внутрішньому й зовнішньому середовищах функціонування ОКЗ.

Система інформаційної безпеки ОКЗ має забезпечувати: по-перше, відстеження динаміки зовнішніх проявів джерел загроз для інформації, факторів розвитку небезпеки для інформації, інтегральних показників кризового стану; по-друге, оцінювання результатів вжитих антикризових заходів за їх характером, термінами, наслідками реалізації.

Відповідно до ступеня досягнення поставлених цілей щодо забезпечення відповідного рівня інформаційної безпеки ОКЗ можливі такі управлінські дії:

1) продовження реалізації розробленої антикризової програми при досягненні поставлених цілей і завдань, необхідної результативності вжитих заходів;

2) модернізація й корегування антикризової програми в разі недотримання її окремих параметрів (терміни реалізації, досягнутий ефект, необхідні ресурси тощо) або появи несподіваних збурень у зовнішньому середовищі ОКЗ;

3) кардинальний перегляд розробленої програми та внесення відповідних коректив.

Метою етапу розроблення й реалізації профілактичних заходів щодо запобігання повторного виникнення загроз для інформації, що обертається у процесі функціонування ОКЗ, є створення або модернізація основних елементів системи інформаційної безпеки ОКЗ.

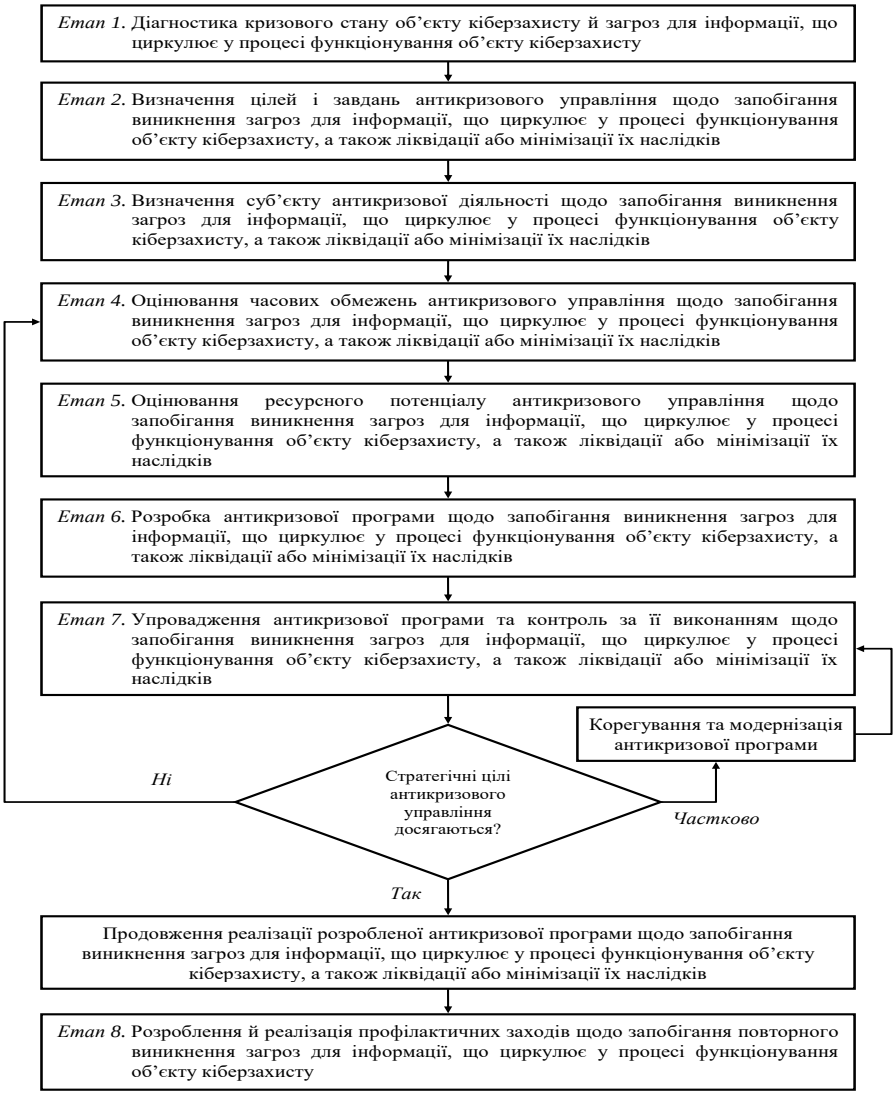

Рис. 3. Структурно-логічна схема процесу антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування об'єкту кіберзахисту, а також ліквідації або мінімізації їх наслідків

Для цього мають бути внесені відповідні зміни в основні функціональні стратегії та політики безпеки ОКЗ, які повинні враховувати передові технології, інструменти й засоби управління інформаційною безпекою, забезпечувати відповідний рівень безпеки функціонування ОКЗ.

Таким чином, запропоновані в роботі результати є основою для оцінювання ефективності функціонування системи інформаційної безпеки ОКЗ та антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

Висновки

1. Показано, що основою системи інформаційної безпеки ОКЗ є класичний контур управління, який забезпечує збір, обробку та аналіз інформації, а також моделювання розвитку інформаційної небезпеки на ОКЗ та розробку й реалізацію антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

2. Представлено результати розповсюдження ризико-орієнтованого підходу до оцінки ефективності функціонування системи інформаційної безпеки ОКЗ в умовах розголошення та витоку інформації, а також в умовах виникнення загроз для комп'ютерної інформації, та розроблено структурно-логічну схему процесу антикризового управління щодо запобігання виникнення загроз для інформації, що циркулює у процесі функціонування ОКЗ, а також ліквідації або мінімізації їх наслідків.

Література

[1] *Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII*. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#n355.

[2] Андронов В.А., Дівізінюк М.М., Калугін В.Д., Тютюник В.В. *Науково-конструкторські основи створення комплексної системи моніторингу надзвичайних ситуацій в Україні*: Монографія. Харків: Національний університет цивільного захисту України, 2016. - 319 с.

[3] Тютюник В.В., Калугін В.Д., Писклакова О.О. Основоположні принципи створення у Єдиній державній системі цивільного захисту інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків надзвичайних ситуацій. *Системи управління, навігації та зв'язку*. Полтава: Полтавський національний технічний університет імені Юрія Кондратюка, 2018, Вип. 4(50). - С. 168–177.

[4] *Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII* [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

[5] *Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»* [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016.

[6] Постанова кабінету міністрів України від 19.06.2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

[7] Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. За заг. ред. В.Б. Толубко. *Інформаційна та кібербезпека: соціотехнічний аспект*. Київ: Державний університет телекомунікацій, 2015. - 288 с.

[8] Козлова О.Ю., Кононович В.Г., Кононович І.В., Романюков М.Г., Тимошенко Л.М. Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки. *Інформатика та математичні методи в моделюванні*. 2017, Том 7, №3, С. 205–212.

[9] Конеев И.Р., Беляев А.В. *Информационная безопасность предприятия*. СПб.: БХВ-Петербург, 2003. - 752 с.

[10] Ярочкин В.И. *Система безопасности фирмы*. М.: Ось-89, 2003. - 352 с.

[11] Тютюник В.В., Шевченко Р.І. Принцип комплектування технічними засобами складової «інформаційна безпека» інтегральної системи безпеки за критерієм «ефективність–інтегральна ціна». *Системи озброєння і військова техніка*. Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2009, №2(18), С. 159–165.

[12] Заболотний В.І., Задорожна Є.В. Обгрунтування вибору заходів захисту характеристик продукції від конкурентної розвідки. *Прикладная радиоэлектроника*. Харків: Харківський національний університет радіоелетроніки, 2013, Том12, №2, С. 351–355.

[13] Гражданкин А.И., Белов П.Г. Экспертная система оценки техногенного риска опасных производственных объектов. *Безопасность труда в промышленности*. 2000, №11, С. 6–10.

[14] Райншке К., Ушаков И.А. *Оценка надежности систем с использованием графов*. Москва: Радио и связь, 1988. - 180 с.

[15] Журин С., Цветков Т. Учет и анализ рисков. *Безопасность, достоверность, информация*. 2004, №1(52), С. 40–43.

[16] Вишняков Я.Д., Радаев Н.Н. *Общая теория рисков*. Москва: Издательский центр «Академия», 2008. - 368 с.

[17] Брушлинский Н. Н. Снова о рисках и управлении безопасностью. *Проблемы безопасности и чрезвычайных ситуаций*. Москва: ВИНИТИ РАН, 2002, №4, С. 230–234.

[18] Хакен Г. *Синергетика*. Москва: Изд. «Мир», 1980. - 414 с.

[19] Курдюмов С.П., Малинецкий Г.Г. *Синергетика и системный синтез. Новое в синергетике: взгляд в третье тысячелетие*. Москва: Наука, 2002. - 180 с.

[20] Малинецкий Г.Г. *Математические основы синергетики: Хаос, структуры, вычислительный эксперимент*. Москва: Книжный дом «ЛИБРОКОМ», 2012. - 312 с.

[21] Рубальський П.С., Малигін М.М., Берека В.В. Концептуальний підхід до прогнозування вартості розробки систем захисту інформації на етапі формування тактико-технічного завдання. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2012, №2(46). - С. 90-95.

[22] Тютюник В.В., Писклакова О.О. Теорія систем та системний аналіз. Харків: Національний університет цивільного захисту України, 2020. - 104 с.

УДК [347.132.15:614.8](477)

Рубан И.В., Тютюник В.В., Заболотный В.И., Тютюник О.А. Оценка уязвимости объектов кибер-защиты на основе риск-ориентированного подхода

Аннотация. *Представлены результаты распространения риск-ориентированного подхода для оценки эффективности функционирования системы информационной безопасности объекта киберзащиты (ОКЗ) в условиях возможного разглашения и утечки информации, ее блокировки и модификации. Показано, что основой системы информационной безопасности ОКЗ является классический контур управления, обеспечивающий сбор, обработку и анализ информации, а также моделирование развития информационной опасности на ОКЗ, разработку и реализацию антикризисного управления относительно предупреждения возникновения угроз для информации, вращается в процессе функционирования ОКЗ, а также ликвидации или минимизации последствий. На базе полученных результатов разработана структурно-логическая схема процесса антикризисного управления по предотвращению возникновения угроз для информации, вращающейся в процессе функционирования ОКЗ, а также ликвидации или минимизации последствий угроз. Разработанная схема антикризисного управления включает диагностику кризисного состояния ОКЗ, определение целей, задач и субъекта антикризисного управления, оценивание временных ограничений и ресурсного по-*