КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.135143
УДК 004.056

Літвінчук Ірина Сергіївна
Науко вий співробітник
Військова частина А1906, Київ, Україна
ORCID: 0000-0002-0854-5393
Litvinchuk.irina94@gmail.com

Коршун Наталія Володимирівна
Доктор технічний наук, доцент, професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-2908-970X
N.korshun@kubg.edu.ua

Ворохоб Максим Віталійович
Аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5160-7134
M.vorokhob@kubg.edu.ua

СПОСІБ ОЦІНЮВАННЯ ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Анотація. Стаття присвячена розробці способу оцінювання ефективності рівня захисту на об'єкті інформаційної діяльності при використанні інтегрованої системи безпеки. Такі системи передбачають спільне використання ресурсів підсистем пожежної та охоронної сигналізації, відеоспостереження, систем контролю управління доступом та інших. Застосування інтеграції забезпечує низку переваг, серед яких: швидка і точна реакція на події, що відбуваються, полегшення роботи оператора за рахунок автоматизації процесів управління, контроль і прийняття рішень по забезпеченню безпеки, зменшення ймовірності помилкових дій оператора, зменшення витрат на обладнання. Серед вимог до інтегрованих систем безпеки - зниження ролі людини в процесі забезпечення безпеки за рахунок підвищення інтелектуальності систем, зниження рівня помилкових спрацьовувань за рахунок більш тісного використання підсистем та відкритість. Реалізація цих вимог дозволить збільшити ефективність систем безпеки, знизити людський фактор та зробить побудову інтегрованих систем більш прозорою. Запропонований спосіб оцінювання інтегрованої системи безпеки узагальнює стан захищеності на об'єкті інформаційної діяльності, вказує на слабкі сторони існуючої інтегрованої системи безпеки, які потребують поліпшення. Він може застосовуватися також при виборі відповідної інтегрованої системи безпеки. Оцінка рівня захищеності враховує такі критерії, як комплексність, функціональність, розмір, швидкодія, відмовостійкість, масштабованість, взаємодія із зовнішніми системами, можливість розширення.

Ключові слова: загроза; інтегрована система безпеки; ефективність; рівень захисту; оцінювання.

1. ВСТУП

Постановка проблеми. Комплексний захист інформації досягається проведенням відповідних правових, організаційних та інженерно-технічних заходів. Останні два, як правило, асоціюються з технічним захистом інформації, під яким розуміють діяльність, спрямовану на запобігання порушенню цілісності, блокуванню та витоку інформації технічними каналами [1].

Передумовою появи загроз інформаційній безпеці є як об'єктивні (недосконаліть засобів захисту), так і суб'єктивні фактори (промислове шпигунство, несумлінні співробітники тощо). Джерелами загроз можуть виступати: людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище [2]. В роботі [3] зазначено, що входами системи захисту інформації є такі явища, як: вплив зловмисників у процесі фізичного проникнення до місцезнаходження джерел конфіденційної інформації з метою її викрадення, внесення змін або знищення; різноманітні фізичні поля, електромагнітні сигнали, які створюються технічними засобами зловмисників і впливають на засоби обробки й збереження інформації; стихійні лиха, що призводять до знищення або перекручування інформації; фізичні поля та електричні сигнали з інформацією, які передаються функціональними каналами зв'язку; побічні електромагнітні наведення й акустичні поля, а також електричні сигнали, що виникають у процесі діяльності об'єктивного захисту та несуть у собі конфіденційну інформацію. В роботі [4] до випадкових загроз відносять, зокрема, випадки руйнації, втрати або зміни даних, конфіденційної інформації або ресурсів під час природних катаклізмів, які не підвладні людині (пожежі, землетруси, повені, магнітні бурі, падіння метеоритів та радіоактивні випромінювання).

«Класичний» набір систем безпеки на об'єкті інформаційної діяльності (ОІД) – це система контролю управління доступом (СКУД), пожежна та охоронна сигналізація, відеоспостереження, периметрова охорона, пожежогасіння та інше. Кожна з цих систем автономна та працює, виходячи зі своїх вузьконаправлених функціональних можливостей. Більш складні умови захисту потребують розробки складніших охоронних комплексів. Актуальними питаннями є співвідношення між собою системи технічного захисту та системи технічної охорони (СТО) об'єкту, у тому числі які державні органи мають координувати, організовувати та контролювати СТО, які загрози необхідно обов'язково враховувати при складанні окремої моделі загроз в рамках побудови СТО та комплексної системи захисту інформації або комплексу технічного захисту інформації тощо [1]. На тлі розвитку ринку виникла необхідність інтеграції різних систем безпеки в одну єдину монолітну систему, яка може вирішувати весь спектр поставлених завдань – це інтегрована система безпеки .

Інтегрована система безпеки (ІСБ) передбачає спільне використання ресурсів підсистем (пожежної та охоронної сигналізації, відеоспостереження, систем контролю управління доступом та іншого), в результаті чого система як ціле набуває нових якісних властивостей, на відміну від автономної роботи підсистем.

Не дивлячись на те, що ринок пропонує широкий асортимент моносистем безпеки, які працюють окремо від інших складових технічної охорони, жодна з них не здатна повністю захистити інтереси ОІД, що охороняється. Тому більш ефективними у захисті безпеки є ІСБ, які складаються не тільки з підсистем, а й з власних каналів зв'язку, баз даних, алгоритмів роботи та програмного забезпечення.

Оскільки сучасність вимагає більш удосконалених та ефективних засобів захисту на ОІД, а такий рівень забезпечує ІСБ, то важливо правильно оцінити та підійти до вибору ІСБ з усіх представлених на ринку. Тому можна вважати, що питання, присвячене оцінюванню ІСБ для забезпечення найвищого рівня захисту на ОІД, є досить важливим.

Аналіз останніх досліджень і публікацій. Крім забезпечення безпеки, ІСБ повинні забезпечувати вирішення задач протидії широкому спектру загроз, що носять різний характер та надходять від різноманітних порушників [5]. Питання інтеграції та

інтегрованих систем безпеки розглянуто в [6]. У цій роботі здійснено огляд традиційного та інтегрованого підходу до побудови системи безпеки, детально описано недоліки та переваги обох підходів, визначено важливість застосування саме інтегрованих систем безпеки та їх значний вплив на забезпечення безпеки, підкреслюючи важливість перспективи їх розвитку.

У порівнянні з простою сукупністю окремих систем і засобів захисту, застосування інтеграції забезпечує наступні переваги:

- більш швидку і точну реакцію на події, що відбуваються;
- суттєве зменшення потоку інформації, одержуваної оператором;
- полегшення роботи оператора за рахунок автоматизації процесів управління, контролю і прийняття рішень по забезпеченню безпеки;
- суттєве зменшення ймовірності помилкових дій оператора (як наслідок двох попередніх пунктів);
- можливість аналізу і вироблення різноманітних керуючих впливів на основі єдиного інформаційного поля;
- простоту і можливість отримання максимуму різноманітної інформації;
- можливість створення і впровадження складних алгоритмів функціонування окремих елементів системи;
- зменшення витрат на обладнання через багатофункціональне використання окремих систем і більш повне їх завантаження.

До недоліків інтегрованих систем можна віднести підвищені вимоги до надійності керуючої підсистеми (при її наявності).

Основні напрями розвитку інтегрованих систем безпеки визначаються наступними вимогами:

- зниження ролі людини в процесі забезпечення безпеки за рахунок підвищення інтелектуальності систем;
- зниження рівня помилкових спрацьовувань за рахунок більш тісного використання підсистем;
- вимога відкритості. Розробники ІСБ повинні забезпечити замовнику за допомогою відкритих протоколів можливості підключення систем і устаткування інших виробників і гнучкого налаштування ІСБ під свої потреби.

Реалізація зазначених вимог, з одного боку, дозволить збільшити ефективність систем безпеки, знизити людський фактор, з іншого - зробить побудову інтегрованих систем більш прозорою [6].

Мета статті. Метою статті є розробка способу оцінювання ефективності рівня захисту на об’єкті інформаційної діяльності при використанні інтегрованої системи безпеки.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Забезпечення надійного захисту ОІД завжди було та буде актуальним, оскільки від створених умов захисту активів (на кожному ОІД визначаються свої) залежить цілісність та працездатність ОІД.

Без надійного захисту ОІД важко контролювати зростаючу кількість загроз, у тому числі комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, пожежі або інші стихійні явища. Людські ресурси, як і матеріальні, є якісними та кількісними, мають

собівартість, тому важливо знайти правильний підхід до оцінки рівня захищеності на ОІД з використанням ІСБ.

Для систематичного аналізу ІСБ та ефективності її роботи на ОІД (якщо ІСБ вже встановлена та функціонує на ОІД), а також для розуміння необхідності удосконалення її складових/систем та вибору для встановлення нової ІСБ пропонується розробка способу оцінки ефективності ІСБ у цілому. На даний час не існує єдиного підходу до оцінки результативності по забезпеченню безпеки на ОІД за рахунок ІСБ, щоб давало б повну картину дієвості ІСБ. У зв'язку з цим пропонується ввести спосіб оцінювання ефективності рівня захисту на ОІД за рахунок використання ІСБ. Спосіб оцінювання ІСБ узагальнює стан захищеності на ОІД та вказує на слабкі сторони існуючої ІСБ, які потребують поліпшення, та допоможе при виборі відповідної ІСБ.

Вищезгаданий спосіб був розроблений на основі аналізу функціональних можливостей складових ІСБ та аналізу реагування (співвідношення частоти помилкових спрацьовувань) ІСБ на інциденти безпеки.

Перший етап - оцінка рівня захищеності на ОІД за наповненістю та певними характеристиками складових ІСБ, що дає можливість оцінити ІСБ в цілому. Оцінка рівня захищеності складається з восьми критеріїв: комплексність, функціональність, розмір, швидкодія, відмовостійкість, масштабованість, взаємодія із зовнішніми системами, можливість розширення. Всі ці критерії є нічим іншим, як часто повторюваними характеристиками при описі будь-якої з існуючих, як складових, так і ІСБ в цілому. Їх оцінено в таблиці 1.

Таблиця 1.

Оцінка ІСБ

Комплексність (*середньозахищений ОІД має включати не менше 4 систем безпеки*)		
Оцінка	Опис	
1	Об'єднує менше трьох систем	Система пожежогасіння, система відеоспостереження.
2	Об'єднує від 3 до 5 систем	Система пожежогасіння, система відеоспостереження, СКУД, система охоронної сигналізації.
3	Об'єднує більше 5 систем	Система пожежогасіння, система відеоспостереження, СКУД, система охоронної сигналізації та інші.
Функціональність (*набір основних функціональних характеристик ІСБ за обміном інформацією і управлінням складовими ІСБ*)		
Оцінка	Опис	
1	Малофункціональна ІСБ	Передача інформації між системами відбувається тільки при виникненні тривоги в якій-небудь одній системі. Відсутня можливість управління всіма системами одночасно з одного робочого місця. Бази даних систем не синхронізовано.
2	Середньофункціональна ІСБ	Передача інформації між системами відбувається тільки при виникненні тривоги в якій-небудь одній системі. Є можливість управління всіма системами одночасно з одного або декількох робочих місць. Бази даних окремих систем не синхронізовано.
3	Високофункціональна ІСБ	Передача інформації між системами відбувається не тільки при виникненні тривоги в одній з систем,

		але і при виконанні системою своїх штатних функцій. Є можливість управління всіма системами одночасно з одного або декількох робочих місць, що мають загальну програмну оболонку з широким набором функцій. Бази даних систем синхронізовані.
Розмір (*розмір ІСБ залежить від розміру складових, що входять в кожну з систем безпеки*)		
Оцінка	Опис	
1	Мала	Складається з систем, в кожній з яких до 50 точок (адресних елементів/адресних датчиків/зчитувачів/відеоканалів).
2	Середня	Складається з систем, в кожній з яких від 50 до 500 точок.
3	Велика	Складається з систем, в кожній з яких більше 500 точок.
Швидкодія (*визначення проміжку часу між подією в одній системі безпеки і відповідною реакцією в іншій/інших системах безпеки, що входять в ІСБ*)		
Оцінка	Опис	
1	Низька	Час реакції перевищує 2 секунди.
2	Середня	Час реакції знаходиться в межах від 1 до 2 секунд.
3	Висока	Час реакції між системами становить менше 1 секунди.
Відмовостійкість/живучість		
Оцінка	Опис	
1	Низька	ІСБ має один нерезервований сервер управління або нерезервований процесорний модуль. Лінії зв'язку не резервовані. Збій в роботі сервера, процесора або обрив лінії зв'язку одразу призводять до порушення обміну інформації в ІСБ і «розсипання» її на окремі системи безпеки.
2	Середня	ІСБ має резервний сервер або процесор, що працюють в «гарячому» режимі. Лінії зв'язку резервовані. У такій ІСБ одноразовий збій в роботі сервера або обрив лінії зв'язку не призводять до порушення роботи систем ІСБ.
3	Висока	ІСБ має резервний сервер або процесор, що працюють в «гарячому» режимі. Лінії зв'язку резервовані. Інтеграція між системами виконана не тільки на програмному, а й на апаратному рівні.
Масштабованість (*збільшення розміру систем, з яких складається ІСБ в процесі експлуатації*)		
Оцінка	Опис	
1	Фіксована	ІСБ не може збільшувати свій розмір.
2	Масштабована	ІСБ може значно збільшувати існуючий розмір за рахунок додавання закінчених модулів або нових окремих систем.
Взаємодія із зовнішніми системами		
Оцінка	Опис	

1	Відкрита	ІСБ забезпечує можливість обміну інформацією на програмному рівні із зовнішніми системами інших виробників.
2	Закрита	ІСБ не забезпечує можливості обміну інформацією на програмному рівні з зовнішніми системами інших виробників.
Можливість розширення		
Оцінка	Опис	
1	Розширювана	ІСБ дозволяє додавати в існуючий склад ІСБ системи нових виробників.
2	Нерозширювана	ІСБ включає до свого складу тільки жорсткий перелік обладнання певних виробників. Додати устаткування інших виробників неможливо.

Низький рівень захищеності – менше 8 балів.

Середній рівень захищеності – від 9 до 15 балів.

Високий рівень захищеності – від 16 до 21 балів.

Висновок по першому етапу: у разі отримання результатів, які визначають ІСБ як «з низьким рівнем захищеності», принципи побудови повинні бути переглянуті на предмет підвищення рівня безпеки або переходу на нову та більш сучасну ІСБ. Що стосується «середнього рівня захищеності» - можливе доопрацювання по тих пунктах, у яких оцінка була на найнижчому рівні. ІСБ на «високому рівні захищеності» потребує лише контролю за справністю складових та на майбутнє – відслідковування більш сучасних складових, щоб залишатись на тому ж рівні.

Другий етап – співвідношення величини виникнення помилкових спрацьовувань та втручання людини в процес виявлення інцидентів безпеки.

Необхідно провести аналіз місячної активності по виникненню інцидентів безпеки. Якщо зі 100 відсотків інцидентів більше, ніж 60 відсотків, були з помилковим спрацюванням, з втручанням людини в процес або взагалі без спрацьовування на інцидент, що виник, то можна вважати таку ІСБ недієвою і рекомендується скористатися першим кроком для коректування ІСБ або обрання нової більш дієвої.

Таким чином, використавши спосіб оцінки рівня захисту інформації на ОІД за рахунок використання ІСБ через визначення величини помилкових спрацьовувань та інших складових, можна скласти чітке уявлення щодо рівня ефективності ІСБ.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

ІСБ – це достатньо організована система по забезпеченню безпеки на будь-якому рівні. Вона самостійно може приймати рішення щодо питань забезпечення безпеки при можливості настання інциденту, не потребуючи значного втручання людських ресурсів в роботу. Найбільшою перевагою такої системи є підключення, завдяки прозорим протоколам розробників, систем і устаткування різних виробників і, звичайно ж, гнучкого налаштування ІСБ, яке буде повністю відповідати потребам певного ОІД. Запропонований спосіб оцінювання ефективності ІСБ дозволяє визначити відповідність системи вимогам об’єкта. В подальшому планується його деталізація з урахуванням у тому числі показників надійності та фінансових показників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] О.В. Манжай, В.П. Коваль, Ю.М. Онищенко, «Проблемні питання захисту інформації на об'єктах інформаційної діяльності», *Системи обробки інформації*, № 7 (81). С. 69-73, 2009.

[2] Р.М. Хмелевський, «Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності», *Сучасний захист інформації*, №4. С. 65-70, 2016.

[3] А. Нашинець-Наумова, «Організація системи захисту інформації суб'єктів господарювання», *Підприємництво, господарство і право*, №2. С. 110-116, 2016.

[4] Ю. Хохлачова, «Політика інформаційної безпеки об'єкта», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, №2(24). С. 23-29, 2012.

[5] В.А. Ворона, В.А. Тихонов «Комплексные (интегрированные) системы обеспечения безопасности». – М.: Горячая линия – Телеком, 2013. - 160 с.

[6] С.П. Журавлев, «Интеграция как новый подход к построению систем безопасности», *Журнал научных публикаций аспирантов и докторантов,* 2008. [Електронний ресурс] Режим доступу: http://www.jurnal.org/articles/2008/inf25.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Iryna S. Litvinchuk
Researcher
Military base A1906, Kyiv, Ukraine
ORCID: 0000-0002-0854-5393
Litvinchuk.irina94@gmail.com

Nataliia V. Korshun
Doctor of Technical Sciences, associate professor, Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-4055-1494
N.korshun@kubg.edu.ua

Maksym V. Vorokhob
Phd student
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0001-5160-7134
M.vorokhob@kubg.edu.ua

METHOD OF EVALUATION OF INTEGRATED SECURITY SYSTEMS AT THE OBJECT OF INFORMATION ACTIVITY

Abstract. The article is devoted to the development of a method for evaluating the effectiveness of the level of protection at the object of information activities when using an integrated security system. Such systems provide for the sharing of resources of subsystems of fire and security alarm, video surveillance, access control systems and others. The application of integration provides a number of benefits, including: quick and accurate reaction to events, facilitating the work of the operator by automating management processes, control and decision-making on security, reducing the probability of erroneous actions of the operator, reducing equipment costs. Among the requirements for integrated security systems are reducing the role of man in the security process by increasing the systems intelligence, reducing the level of false positives due to closer use of subsystems and openness. Implementation of these requirements will increase the efficiency of security systems, reduce the human factor and will make the construction of integrated systems more transparent. The proposed method of assessing the integrated security system summarizes the state of security at the object of information activities, points to the weaknesses of the existing integrated security system, those that need of improvement. It can also be used when selecting the appropriate integrated security system. The assessment of the level of protection takes into account such criteria as complexity, functionality, size, speed, fault tolerance, scalability, interaction with external systems, the possibility of expansion.

Keywords: threat; integrated security system; efficiency; level of protection; evaluation.

REFERENCES

[1] O.V. Manzhai and V.P. Koval and Yu.M. Onishchenko, “Problematic issues of information protection at the objects of information activity”, *Information processing systems*, № 7 (81). Pp. 69-73, 2009.

[2] R.M. Khmelevsky, "Research of information security threat assessment of information objects", *Modern information protection*, №4. Pp. 65-70, 2016.

[3] A. Nashynets-Naumova, "Organization of the information protection system of business entities", *Entrepreneurship, Economy and Law*, №2. Pp. 110-116, 2016.

[4] Yu. Khokhlachova, "Information security policy of the object", *Legal, regulatory and metrological support of the information protection system in Ukraine*, №2 (24). Pp. 23-29, 2012.

[5] V.A. Vorona and V.A. Tikhonov «Complex (integrated) security systems». – M.: Горячая линия – Телеком, 2013. - 160 с.

[6] S.P. Zhuravlev, «Integration as a new approach to building security systems», *Journal of scientific publications of graduate and doctoral students,* 2008. [Electronic resource]. Available: http://www.jurnal.org/articles/2008/inf25.html [20.10.2020].