Хорошко Володимир Олексійович, доктор технічних наук, професор, Національний авіаційний університет.
Khoroshko Vladimir, Professor, National Aviation University.

Хохлачева Юлия Евгеньевна, ассистент, Национальный авиационный университет.
E-mail: hohlachova@gmail.com
Хохлачова Юлія Євгенівна, асистент, Національний авіаційний університет.
Hohlacheva Julia, assistant, National Aviation University.

УДК 004.054

ОЦІНЮВАННЯ ЯКОСТІ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ МЕТОДОМ ЕКСПЕРТНИХ ОЦІНОК У КОМПЛЕКСНІЙ СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ

Наталія Пігур, Володимир Погребенник

Для побудови комплексної системи захисту інформації необхідно використовувати комплекс заходів із забезпечення безпеки на трьох рівнях: правовому, організаційному та технічному. На організаційному рівні, існує багато компонентів захисту, що призводить до того, що необхідно оцінити їх якість. Оцінювання якості організаційних заходів методом експертних оцінок є важливим, оскільки задаючи певний поріг (при якому можливе вилучення деяких заходів) можна зменшити їх кількість, що призведе до зменшення витрат, отже і до зменшення вартості системи. Оцінено якість організаційних заходів захисту, наведено приклади експертного оцінювання цих заходів в процесі створення системи, підготовки її до експлуатації та в процесі експлуатації системи.

Ключові слова: *комплексна система захисту інформації, організаційні заходи, безпека інформації, оцінка якості, метод експертних оцінок.*

Вступ. Надійне забезпечення безпеки інформації неможливе без реалізації комплексного підходу до вирішення такої задачі. Звідси і потреба, як у створенні комплексної системи захисту інформації, так і підготовці спеціалістів з даного профілю.

Оскільки комплексна система захисту інформації (КСЗІ) є складною системою, яка містить сукупність організаційних, інженерно-технічних заходів та програмно-апаратних засобів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу, розглянемо організаційні заходи, які є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються за необхідністю.

Організаційне забезпечення має такі компоненти: підбір співробітників та служби безпеки, облаштування службових приміщень, організація режимно-пропускної служби, організація зберігання документів, організація системи діловодства, експлуатація технічних засобів, створення зон, що охороняються [1].

Метою роботи є застосування методу експертних оцінок до організаційних заходів захисту у процесі створення КСЗІ, підготовки її до експлуатації та в процесі експлуатації.

Оцінювання якості та метод експертних оцінок. Оцінка якості – числова характеристика показника якості, яку можливо отримати шляхом досліджень або ж за допомогою розрахунків з використанням моделі показника якості.

Оцінювання якості – процедура прийняття рішення про якість об’єкту.

Процедура оцінювання якості КСЗІ реалізовується в два етапи на двох рівнях:

– кількісне оцінювання (вимірювання) якості, що реалізується в розімкненій схемі;

– якісне оцінювання (власне оцінювання) якості, що реалізується в замкненій схемі.

Схему дослідження об’єкту, в якій визначається оцінка показника якості (міра якості) називається розімкненою. У розімкнутій схемі якість об’єкту тільки вимірюється, а не оцінюється. Оцінювання якості можливе лише у замкнутій схемі, тобто коли до якості об’єкту висунуті вимоги. Саме вимоги «замикають» схему оцінювання.

Експертне оцінювання ефективності захисту – це вибір системи вимірів (вербальні і вербально-числові шкали), організація процедури експертного оцінювання (підбір експертів, складання анкет, процедура проведення, опрацювання результатів).

Методи експертних оцінок – це спосіб прогнозування та оцінювання майбутніх результатів дій на основі прогнозів фахівців. До складу експертів слід включати людей з різними типами мислення – образне і словесно-логічне, що сприяє ус-

пішному розв'язанню проблеми. Експертів підбирають за ознакою їх формального професійного статусу – посади, наукового ступеня, стажу роботи та ін. Такий підбір сприяє тому, що в число експертів потрапляють високопрофесійні спеціалісти з великим практичним досвідом у даній галузі.

Метод експертних оцінок – це фактично метод прогнозування, основоположним критерієм якого є досягнення згоди серед усіх членів експертної групи. Організаційно це виглядає так. Експерти, обізнані у взаємопов'язаних сферах діяльності, детально відповідають на питання анкети, пов'язаної з досліджуваною проблемою. Кожен з них фіксує свою думку про проблему, а потім повідомляє про відповідь своїм колегам. У випадку розбіжності його прогнозу з думкою інших, експерт зобов'язаний пояснити причину такої невідповідності. Далі процедура повторюється до тих пір, поки думки експертів не збіжаться. При цьому потрібно дотримуватися анонімності, що допомагає уникнути можливості групових роздумів над проблемною ситуацією [2].

Виділяють дві основні групи методів експертного опитування:

– особисті та заочні;

– індивідуальні та групові (колективні) [3].

Особисте опитування – процедура, в якій дослідник здійснює особистий контакт з експертом. Недоліком є великі затрати праці та часу, як зі сторони дослідника, так і зі сторони експертів.

Заочне опитування здійснюється надсиланням анкети експерту поштою. Перевагою є простота та дешевизна, однак надійність отриманих даних може бути нижчою, чим за особистого опитування, тому що деякі питання експерт може неправильно витлумачити, а на деякі взагалі не дати відповіді.

Порівняно простим методом індивідуального експертного опитування є спосіб типу "інтерв'ю". Свої судження експерт висловлює в розмові з людиною, яка здійснює опитування (прогнозистом), відповідаючи на поставлені перед ним питання. Результати інтерв'ю багато в чому залежать від спеціальної підготовки прогнозиста та від навиків вести вільну розмову, утримуючи ініціативу у своїх руках.

Основними перевагами індивідуальних методів експертних оцінок є простота організації обстеження, зрозумілість, врахування і використання набутих знань і досвіду кожного експерта. Обмеженням застосування цих методів виступає обмеженість знань, інформації експертів з суміжних сфер діяльності. Виходячи з цього, більшого поширення на практиці набули колективні експертні методи.

Застосування методу до організаційних засобів захисту. Якість КСЗІ визначається повнотою виконання вимог, які ставляться до КСЗІ. В основу оцінки якості КСЗІ покладені вихідні дані, котрі були отримані методом експертних оцінок.

Відомо, що до КСЗІ ставляться ряд вимог: функціональних, технічних, економічних, організаційних. Однією з головних вимог є організаційні. Наскільки важливі є організаційні заходи, говорить той факт, що жодна система не обходиться без персоналу, який її обслуговує, саме тому основною задачею було застосування методу експертних оцінок до організаційних заходів захисту.

До організаційних заходів щодо ЗІ в процесі створення системи слід віднести [4]:

– розроблення загального проекту системи та її структурних елементів (Зп);

– будівництво чи переобладнання приміщень (Бп);

– розроблення посадових інструкцій щодо забезпечення режиму секретності відповідно до чинного законодавства (Пі);

– виділення у разі потреби окремих приміщень з охоронною сигналізацією та пропускною системою (Оп);

– розмежування завдань між виконавцями щодо випуску документації (Рз);

– присвоєння грифів секретності матеріалам та документації і збереження їх під охороною у виділених приміщеннях з урахуванням та контролем доступу виконавців (Пг);

– постійний контроль за дотриманням виконавцями режиму та відповідних інструкцій (Пк);

– розроблення математичного, програмного, інформаційного чи лінгвістичного забезпечення (Мз);

– інші заходи, що встановлюються в конкретних системах (Із).

Організаційні заходи КСЗІ в процесі створення системи (СС) можна описати у такому вигляді:

$$CC = \{Зп, Бп, Пі, Оп, Рз, Пг, Пк, Мз, Із\} \qquad (1)$$

Показником ефективності, тобто мірою ступеня досягнення цілі, є ймовірність P, яка називається ймовірністю виконання завдання КСЗІ.

Максимальна ймовірність експертної оцінки в процесі СС рівна:

$$P_{CC_{\max}} = 1. \qquad (2)$$

Сумарна допустима оцінка, отримана в результаті експериментальних даних:

$$\sum_{i=1}^{9} P_i \le 1. \qquad (3)$$

Якщо підприємство велике, то для надійного захисту використовуються всі організаційні заходи, для яких сумарна допустима ймовірність буде рівна 0,82.

На рис. 1 показано максимальну та допустиму оцінку якості організаційних заходів методом експертних оцінок у процесі створення КСЗІ.

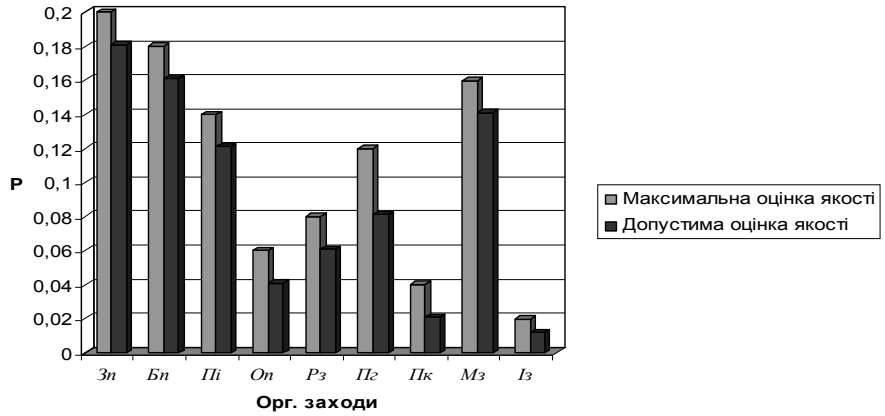

Рис. 1. Оцінка організаційних заходів у процесі створення КСЗІ

Якщо ж підприємство невелике, то використовується частина заходів, тому задано поріг, за якого можливе вилучення деяких організаційних заходів. У даному випадку, задавши поріг 0,025, можна не враховувати: розмежування завдань між виконавцями щодо випуску документації (Рз), інші заходи, що встановлюються в конкретних системах (Із). Звідси, сумарна допустима ймовірність знизиться до 0,787 (рис. 2).

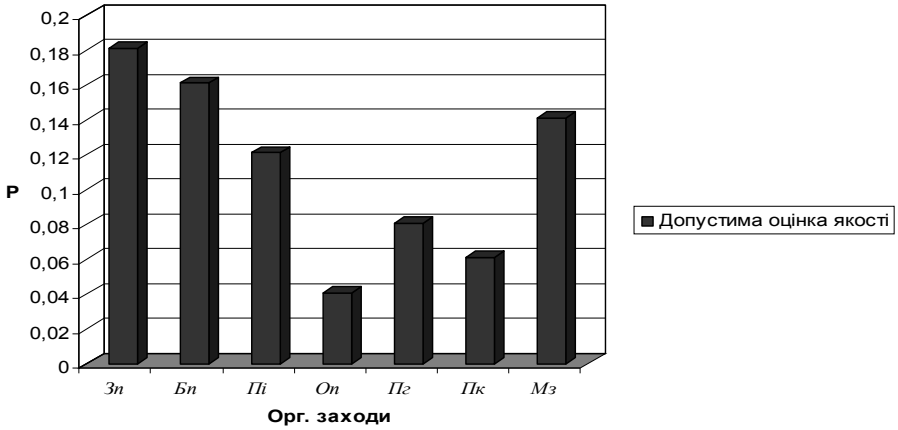

Рис. 2. Допустима оцінка організаційних заходів за заданого порогу ймовірності у процесі створення КСЗІ

У процесі підготовки системи до експлуатації необхідно:

– визначити контрольовану зону навколо об'єктів при виділенні території, будинків та приміщень (Кз);

– встановити та устаткувати охоронну сигналізацію у межах контрольованої зони (Ос);

– організувати контрольно-перепускну систему (Кс);

– розподілити реквізити розмежування доступу (паролі, уповноваження і т.д.) (Рд);

– перевірити схеми розміщення та місця установлення об'єктів КСЗІ (Ср);

– перевірити стан системи життєзабезпечення людей, умови функціонування системи та збереження документації (Зд);

– організувати монтаж та налаштування обладнання (Мо);

– організувати автоматизоване опрацювання інформації (Оі);

– організувати ведення протоколів (Вп);

– підібрати персонал для обслуговування об'єктів КСЗІ і створити централізовану службу безпеки (СБ) при керівництві (Оо);

– провести навчання персоналу (Нп);

– організувати розподіл функціональних обов'язків і відповідальності посадових осіб (Ро);

– встановити повноваження посадових осіб щодо доступу до об'єктів та інформації (По);

– розробити посадові інструкції щодо виконання функціональних обов'язків персоналу всіх категорій, включаючи СБ (Пі);

– розробити план заходів щодо захисту інформації (Пз);

– розробити план участі у семінарах, конференціях з проблем безпеки (Пс).

Організаційні заходи КСЗІ в процесі підготовки системи (ПС) до експлуатації можна подати так:

$$ПС = \{Кз, Ос, Кс, Рд, Ср, Зд, Мо, Оі, Вп, Оо, Нп, Ро, По, Пі, Пз, Пс\}. \quad (4)$$

Максимальна ймовірність експертної оцінки $P_{ПС_{\max}}$ в процесі ПС рівна:

$$P_{ПС_{\max}} = 1. \quad (5)$$

Сумарна допустима оцінка, отримана в результаті експериментальних даних:

$$\sum_{j=1}^{16} P_j \le 1. \quad (6)$$

Для надійного захисту використовуються всі організаційні заходи, для яких сумарна допустима ймовірність буде рівна 0,8716.

На рис. 3 показано максимальну та допустиму оцінку якості організаційних заходів методом експертних оцінок у процесі підготовки КСЗІ до експлуатації.

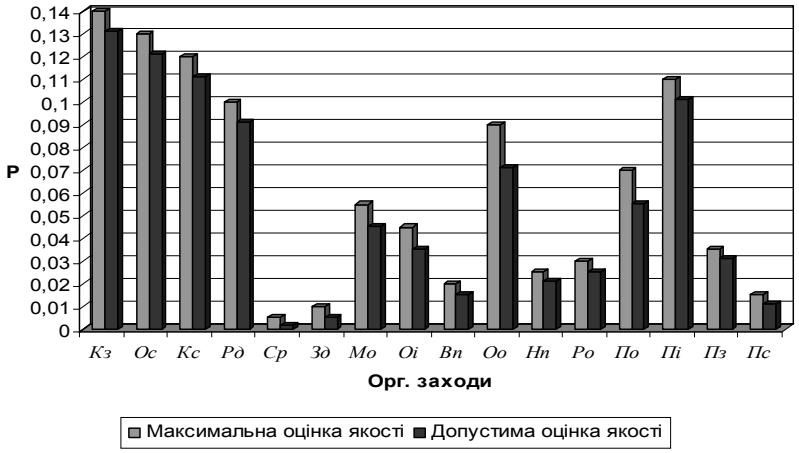

Рис. 3. Оцінка організаційних заходів у процесі підготовки КСЗІ до експлуатації

У даному випадку, задавши поріг (при якому можливе вилучення деяких організаційних заходів) 0,025, можна не враховувати: перевірку схеми розміщення та місця установлення об'єктів КС (Ср), перевірку стану системи життєзабезпечення людей, умови функціонування системи та збереження документації (Зд), організацію ведення протоколів (Вп), проведення навчання персоналу (Нп), розроблення плану участі у семінарах, конференціях з проблем безпеки (Пс). Звідси, сумарна допустима ймовірність знизиться до 0,8174 (рис. 4).

У процесі експлуатації системи необхідно здійснювати централізований контроль доступу до інформації за допомогою технічних та організаційних заходів. Основна частина цих заходів входить до функцій СБ. Перелік основних організаційних заходів КСЗІ у процесі експлуатації:

– визначення порядку обліку, надання, використання і зберігання змінних магнітних носіїв інформації, які містять еталонні та резервні копії програм і масивів інформації, архівні дані і т.п. (Он);

– організація обліку, зберігання, використання і знищення документів і носіїв з закритою інформацією (Од);

– організація за дотриманням всіма посадовими особами вимог щодо забезпечення безпеки опрацювання інформації (Вз);

– визначення переліку необхідних заходів щодо забезпечення неперервної роботи системи в критичних ситуаціях, які виникли в результаті несанкціонованого доступу (НСД), збоїв і відмов засобів обчислювальної техніки, помилок в програмах і діях персоналу, стихійних лих і т.п. (Зз);

– періодичний аналіз стану і оцінювання ефективності заходів щодо захисту інформації (Ое);

– перерозподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.) (Рд);

– аналіз системних журналів, вжиття заходів щодо виявлення порушених правил роботи (Сж);

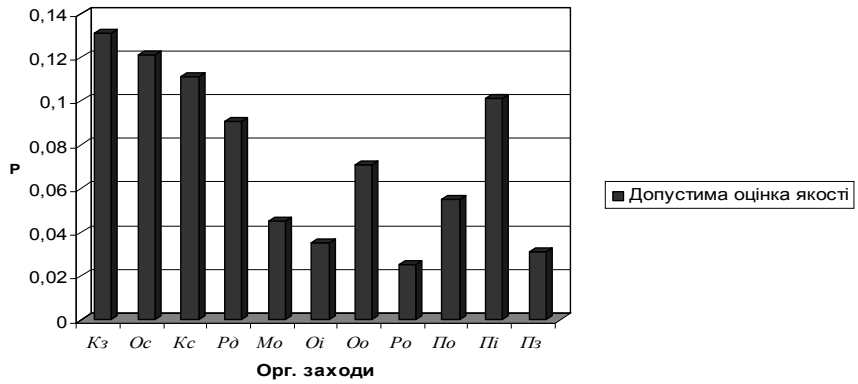

Рис. 4. Допустима оцінка організаційних заходів за заданого порогу ймовірності у процесі підготовки КСЗІ до експлуатації

– організація періодичного, із залученням сторонніх спеціалістів, аналізу стану та оцінювання використаних засобів захисту. На основі отриманої в результаті такого аналізу інформації приймати необхідні заходи з удосконалення системи захисту (Ас);

– організація розгляду та затвердження всіх змін в обладнанні системи, перевірка їх на виконання вимог захисту, документальне відображення змін і т.п. (Зс);

– перевірка осіб, яких приймають на роботу, навчання їх правилам роботи з інформацією, ознайомлення з заходами відповідальності за порушення правил захисту, навчання, створення умов, за яких персоналу було б не вигідно порушувати свої обов'язки (Зв);

– визначення переліку файлів і баз даних, які містять відомості, які становлять комерційну і службову таємницю, а також вимоги до рівня їх захисту від НСД при передаванні, зберіганні і опрацюванні в КСЗІ (Пф);

– виявлення найімовірніших загроз для даної КСЗІ, виявлення вразливих місць процесу опрацювання інформації і каналів доступу до неї (Йз);

– оцінювання можливих втрат, яке викликане порушенням безпеки інформації, розроблення адекватних вимог щодо основних напрямків захисту (Мв).

Організаційні заходи КСЗІ в процесі експлуатації системи (ЕС) можна описати у такому вигляді:

$$EC = \{Он, Од, Вз, Зз, Ое, Рд, Сж, Ас, Зс, Зв, Пф, Йз, Мв\}. \quad (7)$$

Максимальна ймовірність експертної оцінки $P_{EC_{\max}}$ у процесі ЕС рівна:

$$P_{EC_{\max}} = 1. \quad (8)$$

Сумарна допустима оцінка отримана в результаті експериментальних даних:

$$\sum_{k=1}^{13} P_k \le 1. \quad (9)$$

Для надійного захисту використовуються всі організаційні заходи, для яких сумарна допустима ймовірність буде рівна 0,877. На рис. 5 показано максимальну та допустиму оцінку якості організаційних заходів КСЗІ методом експертних оцінок у процесі експлуатації КСЗІ.

У даному випадку, задавши поріг (при якому можливе вилучення деяких організаційних заходів) 0,025, можна не враховувати: аналіз системних журналів, вжиття заходів щодо виявлення порушених правил роботи (Сж); організацію періодичного, із залученням сторонніх спеціалістів, аналізу стану та оцінювання використаних засобів захисту.

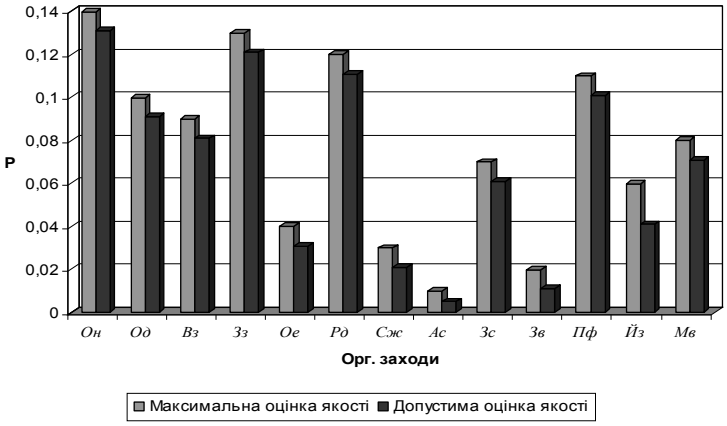

Рис. 5. Оцінка організаційних заходів у процесі експлуатації КСЗІ

На основі отриманої в результаті такого аналізу інформації приймати необхідні заходи з удосконалення системи захисту (Ас); перевірку осіб, яких приймають на роботу, навчання їх правилам роботи з інформацією, ознайомлення з заходами відповідальності за порушення правил захисту, навчання, створення умов, за яких персоналу було б не вигідно порушувати свої обов'язки (Зв). Звідси, сумарна допустима ймовірність знизиться до 0,8174 (рис. 6).

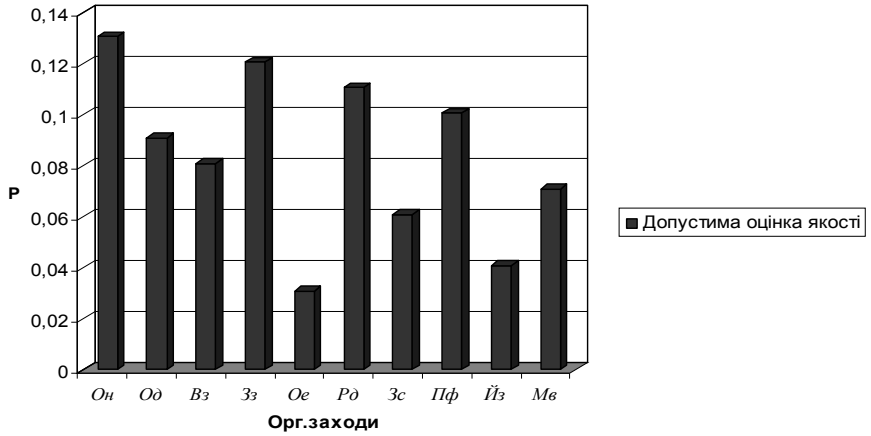

Рис. 6. Допустима оцінка організаційних заходів за заданого порогу ймовірності у процесі експлуатації КСЗІ

Висновки. Оцінено якість організаційних заходів захисту інформації у КСЗІ, наведено приклади експертного оцінювання цих заходів у процесі створення КСЗІ, підготовки її до експлуатації та в процесі експлуатації. Визначено допустимі значення оцінок якості для організаційних заходів при врахуванні заданого порогу.

ЛІТЕРАТУРА

[1]. Грибунин В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр "Академия", 2009. – 416 с.

[2]. Купалова Г.І. Теорія економічного аналізу: навч. посіб. / Г.І. Купалова – К.: Знання, 2008. – 639 с.

[3]. Пігур Н.В. Основні підходи до оцінювання ефективності комплексних систем захисту інформації / Н.В. Пігур, В.Д. Погребенник // Вісник Черкаського державного технологічного університету. Серія: технічні науки. – Черкаси, 2012. – № 2. – С. 42-47.

[4]. Антонюк А.О. Основи захисту інформації в автоматизованих системах: навч. посіб. / А.О. Антонюк. – К.: Академія, 2003. – 240 с.

REFERENCES

[1]. V.G. Gribunin and V.V. Chudovskij, Kompleksnaja sistema zashhity informacii na predprijatii [Complex information protection system on the enterprise]. Moskva: Akademija Publ., 2009, p. 416.

[2]. H.I. Kupalova, Ed., Teoriia ekonomichnoho analizu: navchalnyi posibnyk [Theory of economic analysis: tutorial book]. Kyiv: Znannia Publ., 2008, p. 639.

[3]. N.V. Pihur and V.D. Pohrebennyk, "Osnovni pidkhody do otsiniuvannia efektyvnosti kompleksnykh system zakhystu informatsii" ["The main ways to effectivity of complex information protection systems estimation"] Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: tekhnichni nauky – Cherkassy state technology univercity announcer. Series: technical sciences, vol. 2, pp. 42–47, May 2012.

[4]. A.O. Antoniuk, Ed., Osnovy zakhystu informatsii v avtomatyzovanykh systemakh: navchalnyi posibnyk [The foundations of information protection in automatic system: tutorial book]. Kyiv: Akademiia Publ., 2003, p. 240.

ОЦЕНИВАНИЕ КАЧЕСТВА ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ МЕТОДОМ ЭКСПЕРТНЫХ ОЦЕНОК В КОМПЛЕКСНОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

Для построения комплексной системы защиты информации необходимо использовать комплекс мер по обеспечению безопасности на трех уровнях: правовом, организационном и техническом. На организационном уровне, существует много компонентов защиты что приводит к тому, что необходимо оценить их качество. Оценка качества организационных мероприятий методом экспертных оценок является важным, поскольку задавая определенный порог (при котором возможно изъятие некоторых мероприятий) можно уменьшить их количество, что приведет к уменьшению расходов, следовательно и к уменьшению стоимости системы. Оценено качество организационных мер защиты, приведены примеры экспертного оценивания этих мероприятий в процессе создания системы, подготовки ее к эксплуатации и в процессе эксплуатации системы.

Ключевые слова: комплексная система защиты информации, организационные мероприятия, безопасность информации, оценка качества, метод экспертных оценок.

ORGANIZATION ACTIONS QUALITY ESTIMATION BY THE EXPERT ESTIMATION METHOD IN COMPLEX INFORMATION PROTECTION SYSTEM

For complex information protection system creation it is necessary to use complex of actions on safety ensurance in three levels: legal, organizational and technical. On organization level there exists a lot of protection components, that leads to the necessity of their quality estimation. Organization actions quality estimation by the expert estimation method is important, because while setting some threshold (on which is possible to remove some actions) we can reduce their quantity, that will lead to expenses reduction, and also to system cost reduction. There was estimated organizational protection actions quality, there was given examples of this actions expert estimation in system creation process, it's preparing to exploitation and in process of system exploitation.

Keywords: complex information protection system, organizational actions, information protection, quality estimation, expert estimations method.

Пігур Наталія Володимирівна, аспірант кафедри екологічної безпеки та аудиту Інституту екології, природоохоронної діяльності та туризму ім. В. Чорновола Національного університету «Львівська політехніка»
E-mail: pigur_natik@ukr.net

Пигур Наталия Владимировна, аспирант кафедры экологической безопасности и аудита Института экологии, природоохранной деятельности и туризма им. В. Чорновола Национального университета «Львовская политехника»

Pihur Natalia, postgraduate environmental security and audit Institute of ecology, environmental protection and tourism of Chornovil University of National University «Lviv Polytechnic»

Погребенник Володимир Дмитрович, доктор технічних наук, професор, зав. кафедри екологічної безпеки та аудиту Інституту екології, природоохоронної діяльності та туризму ім. В. Чорновола Національного університету «Львівська політехніка»
E-mail: vpohreb@gmail.com

Погребенник Владимимир Дмитрович, доктор технических наук, профессор, зав. кафедры экологической безопасности и аудита Института экологии, природоохранной деятельности и туризма им. В. Чорновола Национального университета «Львовская политехника»

Pohrebennyk Vladimir, Dr, Professor, Head of the Department of Environmental Protection and Audit, Institute of Ecology, environmental protection and tourism of Chornovil University of National University «Lviv Polytechnic».

УДК 004.891:65.012.8(045)

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМИ ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Юрій Дрейс

Державний експерт з питань таємниць при віднесенні інформації до державної таємниці проводить обґрунтування та визначення величини можливої шкоди національній безпеці у разі її розголошення чи втрати матеріальних носіїв цієї інформації. Існуючі засоби розрахунку такої шкоди в переважній більшості базуються на отримання умовної (бальної) оцінки її прогнозованої величини. У роботі представлено алгоритм функціонування та експериментальне дослідження розробленої системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці, яка основана на моделі інтегрованого представлення параметрів шкоди, існуючих засобів забезпечення даної сфери та методу аналізу і оцінки величини можливої шкоди як в умовних (бальних) одиницях, так і в вартісній (грошовій) величині збитку. Система використовує інтегровані бази даних, що містять основні параметри та показники засобів забезпечення процедури віднесення інформації до державної таємниці та має можливість автоматизованого формування звіту за результатами проведеного оцінювання.

Ключові слова: *розголошення державної таємниці, втрата матеріальних носіїв секретної інформації, система оцінювання шкоди національній безпеці, сфера охорони державної таємниці, національна безпека.*