of applied mathematics and information technologies–Al–Khorezmiy 2012». Volume № 2, Tashkent, 2014, pp. 32–36.
[14]. Tuychiev G.N. About networks PES32–8, PES32–4, PES32–2 and PES32–1, created on the basis of network PES32–16, Ukrainian Scientific Journal of Information Security. 2014, vol. 20, issue 2, p.164–168.
[15]. Tuychiev G.N. About networks RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 and RFWKPES32–1, created on the basis of network PES32–16, Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions», Tashkent, 2014.
[16]. Lai X., Massey J.L. A proposal for a new block encryption standard, Advances in Cryptology, Proc. Eurocrypt'90, LNCS 473, Springer–Verlag, 1991, pp. 389–404.
[17]. Lai X., Massey J.L. On the design and security of block cipher, ETH series in information processing, v.1, Konstanz: Hartung–Gorre Verlag, 1992.

ПРО МЕРЕЖІ PES16–4, PES16–2 І PES16–1, СТВОРЕНІ НА ОСНОВІ МЕРЕЖІ PES16–8

У статті на основі мережі PES16–8 розроблені мережі PES16–4, PES16–2 і PES16–1, які складаються з чотирьох, двох і однієї раундових функцій. Основна перевага запропонованих мереж в тому, що при зашифровані і розшифровані використовується один і той же алгоритм, а також як раундові функції можна використовувати будь-які перетворення. В розроблених мережах довжина підблоков дорівнює 8, 16 і 32 бітам і на основі цієї мережі можна створити алгоритм шифрування довжиною блоку 128, 256 і 512 бітам. Крім цього, алгебраїчні операції є змінними, в якості цих операцій можна використовувати операції додавання і множення по модулю і XOR.

Ключові слова: мережа Фейстеля, схема Лай–Мессі, раундова функція, зашифрування, розшифрування, мультиплікативна інверсія, аддитивная інверсія.

ABOUT NETWORKS PES16–4, PES16–2 AND PES16–1, CREATED ON THE BASIS NETWORK PES16–8

In the paper on the basis of the network PES16–8 developed networks PES16–4, PES16–2 and PES16–1 consisting of four, two, and one round function. The main advantage of the proposed network that during encryption and decryption using the same algorithm as well as a round function can be any transformation. In the network PES16-8 length of subblock is 8, 16 and 32 bits and basis on the network can create the encryption algorithm a length of subblock 128, 256 and 512 bits. In a network PES16-8 algebraic operations are variable, as these operations can use the operations of addition and multiplication modulo and XOR.

Index terms: Feistel network, Lai–Massey scheme, round function, encryption, decryption, multiplicative inverse, additive inverse.

Туйчиев Гулом Нумонович, кандидат технических наук, преподаватель Национального университета Узбекистана.
E-mail: blasterjon@gmail.com.
Туйчіїв Гулом Нумович, кандидат технічних наук, викладач Національного університету Узбекистану.
Gulom Tuychiev, PhD, Associate Professor, National university of Uzbekistan.

УДК 004.056.53

РОЗШИРЕННЯ ЕКОНОМІКО-ВАРТІСНИХ МОДЕЛЕЙ ІНФОРМАЦІЙНИХ РИЗИКІВ ЗА РАХУНОК ВИКОРИСТАННЯ СОЦІАЛЬНО-ПСИХОЛОГІЧНИХ ТИПІВ ЗЛОВМИСНИКА

Олександр Архипов, Андрій Скиба, Олена Хоріна

Розглядаються соціально-психологічні характеристики зловмисника та їх застосування з економіко-вартісними моделями з метою оцінювання інформаційних ризиків і оптимальних інвестицій в інформаційну безпеку. Для проведення адекватного оцінювання інформаційних ризиків та визначення оптимальних інвестицій у сферу захисту інформації існуючі економіко-вартісні моделі потребують розширення з урахуванням соціально-психологічних характеристик зловмисника, які істотно впливають на оцінювання ризиків. Сучасні методи оцінювання інформаційних ризиків, які спираються на існуючі нормативно-правові документи, не враховують соціально-психологічні характеристики зловмисників, що призводить до некоректного проведення оцінювання та зменшення точності отриманих оцінок. Запропоноване розширення економіко-вартісної моделі з урахуванням соціально-психологічних характеристик зловмисника дає можливість підвищити точність оцінок інформаційних ризиків та оптимізувати інвестиції в інформаційну без-

пеку. Запропоновано 10 соціально-психологічних типів зловмисника, використання яких дозволяє розширити застосування та підвищити точність оцінки економіко-вартісної моделі при проведенні оцінки інформаційних ризиків.

Ключові слова: *інформаційна безпека, оцінка ризику, економіко-вартісні моделі, соціально-психологічні типи зловмисників, психотип, класифікації психотипів інформаційної безпеки.*

Вступ. На сьогоднішній день в управлінні інформаційною безпекою найпопулярнішими засобами контролю безпеки є методи визначення і контролю ризиків. Застосовні в цій сфері сучасні методи та моделі визначаються сучасною нормативною базою, яка спирається на два основні стандарти: ISO 27005 [1] та BS 31100 [2]. Дані стандарти є найкращим узагальненням світових практик, як з інформаційної безпеки, так і в галузі управління, про що свідчить їх бібліографічний перелік та еволюція стандартів інформаційної безпеки в огляді авторів [3].

Активний розвиток стандартів та узагальнення найкращих практик дозволяє враховувати все більше деталей в процесі аналізу та оцінювання інформаційних ризиків. Однак стандарти носять переважно рекомендаційний характер і не описують практичних застосувань та можливих сценаріїв розвитку ситуації, тому вся процедура дослідження інформаційних ризиків спирається на оцінки експертів, їх розуміння обставин, факторів, що визначають характер та рівень небезпек на об'єкті ризику. Існуючі сучасні кількісні методи дають оцінку в цифрах, але системна оцінка залежить від експерта та його компетентності. Якщо компетентність експертів недостатня, зростає ймовірність виникнення похибок в процесі оцінювання рівня небезпеки. В практиці аналізу та дослідження ризиків застосування будь-якого методу не може гарантувати високої точності кінцевих результатів при посередній якості оцінок експертів.

Однак кількість компетентних експертів об'єктивно обмежена, оскільки підготовка такого експерта є дуже затратною і, зокрема, потребує значних часових ресурсів, бо рівень розвитку аналітичних можливостей експерта ґрунтується перш за все на набутті ним необхідного практичного досвіду.

Існуючий стан справ спонукає фахівців в сфері аналізу та оцінювання ризиків до пошуку нових ефективних рішень в менеджменті ризиків, які б обмежили залежність оцінок ризиків від експерта, зокрема, його компетентності та мінімізували кінцеві похибки процесу управління ризиками. Розв'язок цієї задачі може бути отриманий у різний спосіб наприклад, шляхом розробки спеціальних додатків, доповнень (розширень) до стандарту, які б містили рекомендації та настанови експертам з структурування то впорядкування їх дій і рішень впродовж процесу експертизи, наприклад, використання певних моделей, обмежувальних співвідношень, логічних умов, які б дали змогу перейти від чисто евристичних оцінок і рішень до аналітико-евристичних частково-прозорих чи частково-керованих процедур експертизи.

Одна з перших спроб мінімізувати залежність результату оцінки ризиків від суб'єктивного впливу експертів належить американським дослідникам Гордону та Лоебу, якими була запропонована модель, призначена для визначення економічно обґрунтованого інвестування в інформаційну безпеку, та її розширення [4, 5, 6]. Їхня ідея використання економічних моделей в інформаційній безпеці полягала в оперуванні фінансовими характеристиками організації, які організація надає шляхом внутрішнього або зовнішнього аудиту. Без залучення експерта. Таким чином, автори започаткували напрямок економічної оцінки інформаційних ризиків інформаційної безпеки, яка спирається виключно на фінансові характеристики. Всім елементам та етапам надаються кількісні значення в фінансових умовних одиницях. Таке фінансове представлення має велику перевагу для керівників організацій, оскільки на початкових етапах їм не потрібно розбиратися в деталях, а можна з легкістю прийняти рішення на основі фінансових показників.

Іншою спробою є економіко-вартісні моделі для оцінки інформаційних ризиків [7, 8, 9], які меншою мірою залежні від фінансових показників і також можуть застосовуватися для коригування оцінок і рішень експертів. Також в економіко-вартісних моделях закладена можливість обробки та нормалізації даних, що дозволяє уникнути багатьох помилок при проведені експертизи.

При порівнянні двох моделей виявлено як переваги, так і недоліки кожної з них. Зокрема, запропоновані моделі не враховують ряд чинників, які є важливими для отримання максимально ефективних оцінок ризиків. Проведений аналіз моделей дав змогу зробити розширену структуру чинників для подальшого розвитку оцінки ризиків інформації [3].

Спираючись на розроблену структуру та вибравши один з найважливіших чинників – соціально-психологічні типи зловмисників, який не враховується на сьогоднішній день існуючими моделями, методами та стандартами, запропоновано подальше розвинення структури економіко-вартісних моделей шляхом її розширення за рахунок врахування соціально-психологічних характеристик зловмисника. Такі характеристики не включені в жодну з відомих нині моделей. Доцільність та способи такого розширення розглянуто в цій статті.

Аналіз існуючих класифікацій соціально-психологічних типів особистості. Досліджуючи соціально-психологічні типи зловмисників, насамперед розглянемо ряд психологічних типологій і поведінкових стереотипів, запропонованих К. Юнгом, Г. Айзенком, Ч. Ломброзо, Е. Кречмером та іншими дослідниками. Психологічна типологія і поведінковий стереотип представляється авторами як комплекс психологічних характеристик особистості. Психологічні характеристики людини дозволяють скласти найбільш вичерпне уявлення про цю людину. Проте психологічні характеристики не дозволяють робити припущення відносно конкретних проявів намірів чи дій цієї людини в різних життєвих та/або професійних ситуаціях. Іноді самі люди не можуть виявити закономірностей прояву своїх почуттів, думок і поведінки в різних обставинах, важко пояснюють свої вчинки. Тобто у людини, у процесі її взаємодії і спілкування з іншими людьми можуть виявлятися різні характеристики, вивченням яких займаються фахівці із соціальної психології. Якщо припустити, що стан інформаційної безпеки об'єкту ризику залежить від загроз, існування яких пов'язане лише з діями людини (далі називатимемо її зловмисником), є підстави говорити про певну взаємодію зловмисника і організації, відповідальної за інформаційну безпеку. В цьому контексті варто розглядати саме соціально-психологічні характеристики зловмисника, зокрема, його мотивацію, і спосіб порушення інформаційної безпеки. Причому слід говорити про усвідомлену мотивацію і спосіб порушення інформаційної безпеки і неусвідомлену мотивацію і відповідний спосіб порушення інформаційної безпеки. Попри наявні успішні спроби багатьох дослідників детермінувати закономірності вчинків людей і чинників впливу на них, як внутрішніх, притаманних людині, так і зовнішніх, з боку середовища/інших людей, практично завжди існують такі сполучення внутрішніх і зовнішніх чинників, які унеможливлюють отримання детермінованого прогнозу. Саме ці сполучення становлять інтерес в сенсі аналізу ризику. Умовно їх можна позначити, як ситуаційні. В такому випадку фахівці розглядають психологічні характеристики людей, наприклад характер/акцентуації дій людини, які вірогідно можуть пояснювати або давати змогу прогнозувати певну кількість варіантів вчинків за тих чи інших обставин. Будь-яка спроба класифікувати або типологізувати людей має сенс, коли йдеться про визначення ймовірних варіантів (тенденцій) розвитку подій.

Спроби дослідників системно описати особистість з метою кращого її розуміння і прогнозування подальшого розвитку можна умовно розділити на 4 етапи. Зокрема, класифікації, розроблені до 20 сторіччя, класифікації першої і другої половини 20 сторіччя, класифікації, створені в 21 ст.

1. Класифікації, розроблені до 20 ст. Класифікації, що розроблені до 20 століття, включають класифікації типів темпераменту за Гіппократом [10] і «злочинного типу» Чезаре Ломброзо [11]. Що стосується «злочинного типу» Ч. Ломброзо, то він більшою мірою характеризує тих, хто вже вчинив злочинну дію, тобто це детермінуюча ознака.

Існуюча класифікація типів темпераменту: холерик, сангвінік, флегматик, меланхолік не є вичерпною і визначальною для пояснення і прогнозування намірів зловмисника. Однак цілком реальним видається припущення, що тип темпераменту може впливати на формування злочинних намірів людини, тобто цей показник більшою мірою вказує на стиль формування і можливої реалізації злочинного наміру, а також на стиль взаємодії з іншими людьми, включеними в організацію/реалізацію такого наміру. Зважаючи, що при аналізі ризиків важливо виявити тенденції на рівні злочинних намірів, міркувань, доцільно включити блок соціально-психологічних характеристик зловмисників до економіко-вартісних моделей інформаційних ризиків з метою підвищення їх ефективності.

2. Класифікації, розроблені в першій половині 20 ст. До класифікацій психологічних типів першої половини 20 століття належить теорія характеру, запропонована німецьким психологом Ернстом Кречмером [12]. Відповідно до цієї теорії, характер залежить від статури, автор використовує фізичну характеристику людини для психологічної класифікації Кречмер описав три типи статури і відповідні їм три типи характеру. Ця класифікація не може бути використана для нашого дослідження, оскільки експерт з інформаційної безпеки при оцінці ризику достовірно не може знати всіх фізичних параметрів зловмисника. Це додає невизначеності при проектуванні соціально-психологічних характеристик зловмисника на матрицю зловмисника, що більш детально описана в наступному розділі.

Подібною до класифікації Кречмера є класифікація за типами темпераменту У.Г. Шелдона

[13], де автор також використовує статуру та фізичні характеристики.

Теорія характеру Кречмера і типи темпераментів по У.Г. Шелдону подібні за змістовим насиченням. Вважаємо ці класифікації неприйнятними для оцінки ризиків інформаційної безпеки через необхідність використання фізичних ознак.

Важливою класифікацією для інформаційної безпеки є класифікація особистісних типів за Карлом Юнгом [14]: екстраверт – інтроверт, так як ці типи максимально чітко описують модель інформаційних процесів збору та аналізу інформації. Розвитком класифікаторів особистісних типів за Юнгом стала типологія Майерс-Бріггс (MBTI) [15]. У звіті ФБР і ЦРУ за 2006 рік [16] детально описано інсайдера як портрет зловмисника, що діє в середині організації. Його соціально-психологічні характеристики запропоновано визначати за допомогою теорії особистості Юнга і типології Майерс-Бріггс (MBTI). Також у звіті запропоновано адаптований варіант методики «Визначник темпераменту» (Keirsey Temperament Sorter) Д. Кірсі. Методика Кірсі [17] - це друга еволюція типології Майерс-Бріггс, яка в наш час має достатньо критики, оскільки наукова частина типології викликає сумніви, пов'язані з відсутністю кваліфікації і освіти у розробників в області психометрії, сумніви стосовно типологічної моделі класифікатора. Хоча для подальших досліджень вона має певні перспективи для застосування, з нашого досліджені модель виключена, так як була перевірена відомими спеціалістами Гордоном і Лоебоєм у дослідженні, замовленому для ФБР і ЦРУ. Автори на сьогоднішній день не рекомендують широке застосування даної типології в моделях, з якими вони працюють.

Досить відомою класифікацією є типи акцентуацій особистості К. Леонгарда [18]. Ця класифікація перебуває в суперечності з іншими, а саме: класифікаціями Айзенка [19], Майерс-Бріггс та соціонікою. Класифікація К. Леонгарда використовується в психіатрії, однак її впровадження в інформаційній безпеці стикається з певними обмеженнями.

Останньою моделлю першої половини 20 століття є психологічні типи по П.Б. Ганнушкину [20], який описав ознаки поведінкової патології у вигляді схильності до дезадаптації, тотальності і стабільності. У другій половині 20 століття ці ознаки були в розвинуті А.Є. Личком і пізніше стали відомі як класифікація А.Є. Личка [21].

3. Класифікації другої половини 20 ст. Класифікації другої половини 20 століття представлені меншою кількістю і більшою мірою спираються на попередні дослідження, є удосконаленнями попередніх класифікацій або їхньою більш сучасною інтерпретацією. Автор Джуліан Роттер [22] запропонував класифікацію інтернального - екстернального типу. Вона базується на визначенні рівня суб'єктивного контролю (інтернальності), який свідчить про здатність людини приймати відповідальність за значущі події свого життя, бути їх автором, а не покладатися на ризики, наслідки дій інших людей або вплив обставин. Рівень вимірюється за допомогою опитувальника з 44 запитань, де високий РСК притаманний інтернальній особистості, низький - екстернальній. Ця класифікація допомагає зрозуміти вектор мотивації зловмисника, витоки злочинного наміру і об'єкт, якому приписується відповідальність за злочин, в разі його реалізації. Наприклад, якщо співробітник організації мав певні очікування від працедавця, не проговорив їх, не отримав підтвердження від працедавця, що очікування справдяться безумовно, або за певних умов, то можна говорити, що співробітник має екстернальний локус контролю. Тобто покладає відповідальність за свої непроговорені очікування на працедавця. Якщо очікування не справдилися з різних причин, то такий співробітник вважає, що відбулася несправедливість, і він постраждав, тобто винна організація. В такому випадку він може запланувати спосіб відтворення справедливості, наприклад, нанесення шкоди інформаційній безпеці організації, у вигляді крадіжки інформації, її продажу, або передачі конфіденційної інформації комусь, хто її використає проти організації, тощо. Тобто, екстернальний локус контролю може вказати на суб'єктивне «обґрунтування» злочинного наміру «постраждалого» в його уявленнях стосовно ситуації.

В 70-80 роках XX століття в СРСР Аушра Аугустинавичюте [23], базуючись на типології Юнга, запропонувала низку гіпотез про психологічні типи, назвавши свою типологію «соціоніка». Соціоніка є прикладним інструментом відділу кадрів і популярним інструментом визначення соціального типу людини. Достатньо простий тест, який набув широкого застосування, а також це більш доступна інтерпретація типології Юнга. Можна вважати дану класифікацію однією з найкращих, але в наше дослідження вона не була включена оскільки ґрунтується на теорії Юнга.

Відомою класифікацією психотипів є класифікація А.Є. Личка, який створив власну типологію особистостей на базі патологій П.Б. Ганнушкина та акцентуацій К. Леонгарда Основу цієї класифікації складає розгляд соціально-психологічних факторів, які впливають на людину, формуючи особливості її характеру, мислення, поведінкових проявів людини. Потрібно зазначити, що ця класифікація спирається на роботу В.Н. Мясищева [24] про «індивідуальні чутливості» до психічних травм, включає в себе ситуативність, індивідуальну реакцію на внутрішні та зовнішні фактори впливу, інтелектуальні здібності особистості, що відповідає критеріям оцінки соціально-психологічних характеристик зловмисника в інформаційній безпеці.

4. Класифікації, розроблені в 21 ст. Серед відомих класифікацій 21 століття можемо відмітити психологічний тест Н.І. Козлова «Що ви за птах?» (аналог тесту в діловий сфері «червоний-синій-зелений») [25], класифікацію «Чотири стихії» [26], типологію керівників І. Адизеса [27], класифікацію Еннеаграма [28]. Найбільш цікавою б могла бути еннеграма особистості, яка досить широко використовується в бізнес-моделях міжнародних компаній Avon Products, General Motors, Alitalia Airlines, KLM Airlines, Kodak, Hewlett Packard, Toyota, Procter & Gamble, Reebok, Motorola, Sony, American Press Institute, Coca Cola (Mexico) та інших, але, на жаль, вона не має належного наукового обгрунтування.

За результатами огляду та аналізу відомих класифікацій психологічних типів, у підсумковій формі стисло наведених вище, було обрано класифікацію А.Є. Личка. На нашу думку, ця класифікація в достатній мірі задовольняє вимогам щодо можливості її використання для визначення і прогнозування соціально-психологічних характеристик зловмисника, зокрема, на її основі буде побудований перехід до соціально-психологічних характеристик зловмисника, які варто включити до економіко-вартісних моделей інформаційної безпеки. Крім того, що дуже важливо у плані прикладного застосування методики А.Є. Личка, на поточний момент існує достатня кількість розробок (опитувальники, тести, довідниково-інтерпретаційні матеріали), орієнтованих на безпосередньо практичне використання класифікація А.Е. Личка.

Опис формальних соціально-психологічних моделей зловмисника для визначення інформаційних ризиків. Типовим та загально прийнятим у бізнес середовищі є класифікації, які нараховують 4-5 типів зловмисників, що найчастіше покривають весь спектр загроз інформаційної безпеки. В результаті аналізу типових ситуацій виникнення загроз та проведення атак на інформаційну безпеку було виділено 10 соціально-психологічних портретів зловмисників, які враховують:

1) його статус стосовно організації;

2) мотивацію усвідомлену або неусвідомлену, матеріальну та/або психологічну;

3) наявність зовнішнього/внутрішнього замовника порушення інформаційної безпеки;

4) наявні та /або запозичені ресурси.

Дана класифікація є приведеною до нормованого вигляду даних про можливі типи зловмисників та дає змогу повністю покрити всі можливі варіанти ситуаційного розвитку подій. В цій статті пропонується матриця зловмисника, побудована на чотирьох вищенаведених показниках. Її можна використовувати для класифікації типів зловмисників і оцінки загроз інформаційної безпеки. Такий розподіл повністю враховує можливості, як інсайдера (того, хто діє в середині організації), так і аутсайдера (того хто діє ззовні організації), а також інсайдера-аутсайдера, того, хто працював в організації, але на момент скоєння злочину вже не працює. Саме цей тип не враховують або упускають і тоді оцінка ризиків є неповною, а відтак - неефективною.

Аутсайдер. Аутсайдер – типовий зловмисник, який проводить протиправні дії ззовні, не може мати інформацію про організацію з середини і не може бути учасником внутрішніх процесів компанії. Аутсайдери за показником наявності внутрішнього замовника злочинного наміру, є виконавцями власних замовлень, мають внутрішню усвідомлену мотивацію матеріального і психологічного характеру. В разі наявності зовнішнього замовника злочинного наміру, позиція внутрішнього замовника аутсайдера співпадає або посилюється за рахунок іншої особи. Аналогічна ситуація із ресурсом власним та/або запозиченим, втому числі і людським. Таким чином, аутсайдери розрізняються за статусом: працюю на когось або на себе, я є організатором злочинного наміру, або хтось, а я - виконавець.

Детальний опис типів аутсайдерів. Аутсайдер – найманий професіонал – особа, що є професіоналом у сфері інформаційних технологій, яка виконує протиправні дії за наймом для певної фізичної/юридичної особи (Замовника), причому для проведення протиправних дій використовує ресурси Замовника. Даний тип зловмисника отримує матеріальну вигоду, яка в даному випадку визначається як погоджена вартість за обсяг робіт або – «виграш зловмисника». Цей тип є найбільш небезпечним, оскільки він може отримати від Замовника необхідний та наднеобхідний обсяг ресурсів для проведення протиправних дій. Це може бути критичним для атакованого об'єкта.

Аутсайдер – самозайнятий професіонал – особа, що є професіоналом у сфері інформаційних технологій, яка працює на себе і витрачає свої власні ресурси для проведення протиправних дій з метою отримання матеріальної вигоди. Замовлення або об'єкт для проведення протиправних дій знаходить самостійно. Проведення протиправних дій цього зловмисника може бути обмеженим тільки необхідністю ресурсів, які потрібні як інвестиції для проведення протиправних дій та/або відсутністю необхідного обсягу специфічних навичок та знань для проведення протиправних дій. В [3, 7] цей тип зловмисника отримав назву «зловмисник-прагматик».

Аутсайдер – менеджер власного угруповання – особа-професіонал, яка працює на себе і витрачає свої власні ресурси для проведення протиправних дій з метою отримання матеріальної вигоди, залучає та утримує за свій кошт професіоналів різного рівня, які складають його команду. Замовлення або об'єкт для проведення протиправних дій знаходить самостійно. Даний тип зловмисника виконує протиправні дії для отримання матеріальної вигоди, яка в даному випадку визначається як «виграш зловмисника» з вирахуванням витрат на команду. Цей тип зловмисника небезпечний тим, що для отримання більшого виграшу може братися до виконання найскладніших завдань, причому рівень цих завдань, як і можливість їх успішного виконання обмежуються тільки реальним нестатком ресурсів, потрібних для проведення протиправних дій.

Аутсайдер – менеджер організованого угрупування – особа-професіонал, яка виконує протиправні дії за наймом, для проведення протиправних дій використовує ресурси Замовника, які витрачає на збір команди професіоналів високого рівня. Даний тип зловмисника виконує протиправні дії для отримання матеріальної вигоди, яка в даному випадку визначається як погоджена вартість за обсяг робіт або – «виграш зловмисника». Даний тип зловмисника є найбільш небезпечним оскільки він може отримати необхідний та наднеобхідний об'єм ресурсів для проведення протиправних дій. Це може бути критично для атакованого об'єкта. В склад команди можуть бути включені найкращі професіонали, що збільшує коефіцієнт небезпеки.

Інсайдери-аутсайдери. Інсайдер-аутсайдер – комбінований тип зловмисника. Таким зловмисником є особа, яка мала відношення до організації в минулому та за перебігом певних обставин і з наявним знанням про організацію приймає рішення щодо власної участі і проведення протиправних дій.

Детальний опис типів інсайдерів/аутсайдерів:

Інсайдер/аутсайдер – шкідник – особа, яка в минулому мала відношення до організації, але у зв'язку з різними обставинами на момент проведення протиправних дій не має відношення до неї. Таким типом зловмисника є особи, які мали причини невдоволення стосовно організації і за збігом обставин бажають задовольнити своє внутрішнє невдоволення. Протиправні дії зловмисників такого типу мають характер шкоди, помсти.

Інсайдер/аутсайдер – «свояк» - особа, яка в минулому мала відношення до організації, але у зв'язку з різними обставинами на момент проведення протиправних дій не має відношення до неї. Даний тип зловмисників представлений особами, які мають інформацію про організацію і використовують ці знання, коли з'являється можливість отримати додаткову матеріальну винагороду. Протиправні дії зловмисника можуть нанести організації шкоду і привести до краху організації.

Інсайдер/аутсайдер – ненавмисний - особа, яка в минулому мала відношення до організації, але у зв'язку з різними обставинами на момент проведення протиправних дій не має відношення до неї. Даний тип зловмисників представлений особами, які мають інформацію про організацію і використовують ці знання випадково («так склалися обставини»), не маючи на меті нанести шкоду організації. Протиправні дії зловмисника можуть нанести організації шкоду і привести до її краху.

Інсайдер. В основу визначення інсайдер покладемо загально прийняту термінологію, зважаючи на те, що вона використовується для всіх чотирьох приведених нижче типів. Отже, інсайдер - особа, яка має доступ до конфіденційної інформації організації завдяки своєму службовому становищу, участі в роботі організації, родинним зв'язкам і має можливість використовувати своє становище у власних інтересах.

Детальний опис типів інсайдерів:

Інса́йдер – незадоволений шкідник – особа, причини незадоволеності якої обумовлені умовами праці та побуту (зміст і організація праці, система матеріального і морального стимулювання, організація виробництва та управління, взаємини в колективі, система професійного зростання, забезпеченість житлом, санітарно-гігієнічні умови праці і т.д.). Дані причини вкарбовуються у свідомість особи, що і породжує бажання зробити протиправні дії з метою нанесення шкоди своєму «кривднику» (частіше за все – це організація в цілому, чи хтось з її керівництва) для встановлення «справедливості». Дії даного інсайдера не є цілеспрямованими чи спеціально зорієнтованими на нанесення шкоди організації у сфері виробництва (послуг), збуту або конкурентної боротьби і т.п., ці дії часто мають спонтанний, не прогнозований характер й спрямовані виключно на здійснення помсти та отримання власного внутрішнього задоволення. За термінологією [3] цей тип зловмисника має назву «зловмисник-месник».

Інса́йдер – зловмисник (фактично, аутсайдер, який входить до складу організації) – особа, яку впроваджено до складу працівників (службовців) певної організації з метою отримання доступу до необхідної інформації для того, щоб скоїти протиправні дії та отримати матеріальну винагороду. Дії даного типу інсайдера спрямовані для нанесення прямої шкоди організації (у сфері виробництва, ринково-конкурентній, політичній тощо). Ці дії можуть мати непрямий характер, але матимуть пост-фактор для організації.

Інса́йдер – випадковець – особа, яка працює в організації і скоює протиправні дії в разі, коли в неї з'являється авантюрна пропозиція. В більшості випадків даний тип інсайдера не спрямований на нанесення шкоди свідомо, просто планується використати інформацію для отримання матеріальної вигоди для себе, але без наслідків для організації.

Інса́йдер – ненавмисний – особа, яка працює в організації і скоює протиправні дії, виконуючи свої стандартні посадові інструкції. В більшості випадків даний тип інсайдера не спрямований на свідоме нанесення шкоди організації, просто при виконанні своїх посадових обов'язків він через неуважність або незнання робить дії, які приносять шкоду організації.

Визначення соціально-психологічного типу зловмисника у сфері інформаційної безпеки на основі типів акцентуацій особистості за А.Є. Личко. Для проведення оцінки інформаційних ризиків в організації в першу чергу треба визначити коло співробітників, які мають справу з інформаційними потоками та інформацією. Після виявлення таких співробітників з ними працює психолог та за допомогою відповідного тестування й проведення додаткового усного опитування визначає ймовірність/вірогідність «переходу» цих працівників з ролі співробітника до ролі зловмисника. Для класифікації соціально-психологічного типу вибрано типи акцентуацій характеру за А.Є. Личком. Для прикладу, після проходження тестування та додаткового опитування психологом згідно типів акцентуацій за А.Є. Личком, уявний співробітник П. буде мати тип акцентуації сенсетивний, а співробітник І. – шизоїдний.

Наступним кроком в проведенні оцінки, є співвідношення між типом акцентуації особистості співробітника і його можливим соціально-психологічним типом зловмисника. Провівши детальний аналіз типології та тестування можливих варіантів співвідношення, отримано таблицю переходу від типу акцентуації особистості за А.Є. Личком до соціально-психологічного типу зловмисника інформаційної безпеки (табл. 1). Дані, представлені в таблиці, дають можливість конвертувати тип акцентуації особистості в соціально-психологічний тип зловмисника у сфері інформаційної безпеки, що дозволяє застосувати кількісні оцінки при визначенні ризиків інформаційної безпеки. Оскільки будь-якому типу акцентуації особистості може бути поставлено у відповідність кілька соціально-психологічний тип зловмисника, тобто проекція типу акцентуації особистості на соціально-психологічний тип зловмисника відбувається як один до багатьох, то при проведенні оцінювання типу акцентуацій особистості відповідно до соціально-психологічного типу зловмисника варто залучати психологів, які в своєму професійному арсеналі мають різноманітний інструментарій для вирішення задач оцінювання та прогнозування. Якщо економіко-вартісні моделі інформаційної безпеки розширюються за рахунок оцінки соціально-психологічного типу зловмисника, варто розглядати безпосередню участь психологів в розробці програмного продукту у вигляді експертної системи, або опосередковану участь через розробку ними інструкції та інструментарію для проведення тренінгу тих, хто буде займатися оцінкою соціально-психологічних характеристик співробітників.

Запропонований підхід для визначення соціально-психологічного типу зловмисника використаний при визначенні комплексної оцінки інформаційної безпеки організації за допомогою економіко-вартісних моделей, що дозволяє підвищити точність оцінки інформаційних ризиків, шляхом врахування «людського» та ситуаційного чинників.

Визначення кількісних показників формальних моделей соціально-психологічних типів зловмисника у сфері інформаційної безпеки. Визначивши можливі соціально-психологічні типи зловмисників за допомогою соціально-психологічних типів особистостей на основі класифікації А.Є. Личка, звернемося до варіанту переходу від соціально-психологічної оцінки зловмисника до його кількісної оцінки для подальшого застосування в оцінюванні інформаційних ризиків за допомогою використання економіко-вартісних моделей.

Таблиця 1

Таблиця переходу від типу акцентуації особистості за А.Є. Личком
до соціально-психологічного типу зловмисника інформаційної безпеки

Типи акцентуацій характеру за А.Є. Личком	*Соціально-психологічні типи зловмисників*
Гипертимний	аутсайдер, організатор угрупування; інсайдер - шкідник
Циклоїдний	інсайдер-аутсайдер (шкідник і ненавмисний), інсайдер ненавмисний
Лабільний	інсайдер-незадоволений шкідник і ненавмисний
Астено-невротичний	інсайдер випадковець, ненавмисний
Сенситивний	інсайдер-шкідник і ненавмисний
Психастенічний	інсайдер ненавмисний
Шизоїдний	потенційно можуть бути всі, крім аутсайдерів - керівників злочинних угруповань; вони можуть створити схему злочину, організовувати/керувати буде, наприклад гіпертимний, а команду збере істероїдний
Епілептоїдний	інсайдер-аутсайдер; інсайдер - шкідник, -«свояк»
Істероїдний	інсайдер/аутсайдер - шкідник, -«свояк»; інсайдер-незадоволений шкідник, - випадковець
Нестійкий	інсайдер/аутсайдер, крім ненавмисного, інсайдер, крім ненавмисного
Конформний	інсайдер/аутсайдер «свояк», ненавмисний, інсайдер випадковець, ненавмисний

Для надання кількісної оцінки конкретному соціально-психологічному типу зловмисника запропоновано розширену матрицю зловмисників (табл. 2).

Таблиця 2

Кількісні оцінки для соціально-психологічних типів зловмисників в сфері інформаційної безпеки

Тип зломисника	Характеристи												Оцінка
	Внутрішній замовник	Зовнішній замовник	Власні ресури	Запозичені рерурси	Необхідні технічні навики	Працює сам	Працює з командою	Матеріальна мотивація	Мотивація шкоди	Мотивація помсти	Мотивація неусвідомлення	Мотивація свідома	
Кількість балів	1	2	3	4	5	6	7	8	9	10	11	12	
Аутсайдер - найманий профессіонал	0	1	0	1	1	1	0	1	1	0	0	1	0,58
Аутсайдер - самонайнятий професіонал	1	0	1	0	0,5	1	0	1	1	0	0	1	0,54
Аутсайдер - менеджер власного угруповування	1	0	1	0	0,5	1	1	1	1	0	0	1	0,63
Аутсайдер - менеджер організованого угруповування	0	1	0	1	1	1	1	1	1	0	0	1	0,67
Інс/аутсайдер - шкідник	1	0	1	0	0	1	0	0	0,5	0,5	0	1	0,42
Інс/аутсайдер - свояк	0	1	1	0	0	1	0	1	0,5	0	0	1	0,46
Інс/аутсайдер - ненавмисний	0	0	0	0	0	1	0	0	0	0	1	0	0,17
Інс/аутсайдер - зловмисник	0	1	0	1	1	0,5	0,5	1	1	0	0	1	0,58
Інсайдер - шкідник	1	0	0	0	0	1	0	0	0,5	0,5	0	1	0,33
Інсайдер - випадковець	0	1	1	0	0	1	0	0,5	0	0	0	1	0,38
Інсайдер - ненавмисний	0	0	0	0	0	1	0	0	0	0	1	0	0,17

В даній табл. приведена кількісна оцінка для всіх соціально-психологічних типів зловмисника в сфері інформаційної безпеки. Для визначення кількісної оцінки були використані соціально-психологічні характеристики зловмисника, які описують його за $n = 12$ основними показниками X_j, $j = \overline{1,12}$. Всім характеристикам, за якими проводиться оцінка, надається вага. В нашому випадку всім характеристикам X_j надається вага 1, якщо така характеристика є в цього типу зловмисника і 0, якщо ця характеристика для даного типу зловмисника відсутня; крім того, в таблиці зустрічається варіант X_j =0,5 - якщо характеристика зловмисника вважається суперечливою або не домінуючою. Вирішення даного суперечливого запитання отримуємо за допомогою спілкування з психологом, який для кожного співробітника може скоригувати оцінку або прибрати невизначеність. Кількісна характеристика зловмисника визначається як сума всіх оцінок характеристик за типом зловмисника, поділена на загальну кількість оцінок за характеристиками. Тобто якщо в нас з 12 характеристик зловмисника присутні (дорівнюють одиниці) тільки 6, то кількісне значення даного соціально-психологічного типу зловмисника інформаційної безпеки дорівнює 0,5, що можна обрахувати за наступною формулою:

$$Ph = \frac{1}{n}\sum_{j=1}^{n} X_j . \quad (1)$$

Під отриманим кількісним значенням *Ph*, розуміємо коефіцієнт небезпеки конкретного зловмисника. У загальному випадку оцінки X_j, $j = \overline{1,12}$ можуть не мати однакових ваг, то ж їм можна буде присвоїти інакші ваги для кожної з характеристик. Для зменшення похибок оцінок можна використовувати експертний метод, де оцінки для певного типу зловмисника буде проставлятися декількома експертами, а потім нормуватиметься за правилами приведення оцінок із врахуванням рівнів компетентності експертів.

Таким чином, можна отримати кількісні оцінки коефіцієнту небезпеки зловмисника для кожного типу соціально-психологічних характеристик, що допоможе розширити економіко-вартісні моделі оцінювання ризиків з урахуванням небезпеки від внутрішніх і від зовнішніх зловмисників з урахуванням їх соціально-психологічних характеристик.

Використання коефіцієнту небезпеки зловмисника для розширення економіковартісних моделей для оцінки інформаційних ризиків. Розглянемо ситуацію, що виникає при реалізації атакуючою стороною А (зловмисник) загрози *T* відносно деякого інформаційного ресурсу *I*, який належить стороні В [3, 7, 8]. Вважатимемо, що *D* – загальна вартість витрат атакуючої сторони А на реалізацію загрози *T*, *g* – отриманий при цьому «виграш», величина якого обумовлюється цінністю ресурсу *I* для зловмисника. Збитки, яких зазнала в цій ситуації сторона В (власник ресурсу *I*), тобто вартість критичної інформації с точки зору її власника, оцінюється ним як *q*, а загальна вартість реалізованого в ІС комплексу захисних заходів дорівнює *c*.

Наведені дані дають вартісну характеристику ситуації «атака-захист». На базі цих відомостей можна побудувати логіко-евристичну схему експертного оцінювання ймовірнісних характеристик, що використовуються для обчислення інформаційних ризиків.

Чистий прибуток зловмисника в разі успішної реалізації загрози *T* складає:

$$Q = g - D. \quad (2)$$

Якщо цінність ресурсу *I* для атакуючої сторони А значна, інтенсивність потоку спроб доступу зловмисника до ресурсу *I* буде дуже високою. Зокрема, якщо *g*>>*D*, можна припустити, що ймовірність P_t активації (виникнення) загрози *T* буде практично дорівнювати 1, тобто зловмисник спробує використати будь-які шанси для реалізації цієї загрози. Навпаки, для малих значень *g* економічні мотиви виникнення загрози *T* практично відсутні: при *Q*=0 (або ж *g*=*D*) атака ресурсу *I* стає недоцільною, в цьому випадку $P_t = 0$. Для *g*<*D* спроба реалізації загрози *T* втрачає будь-який економічний сенс. Виходячи з цих міркувань, в [7, 8] для оцінювання значень ймовірності активації (виникнення) загрози *T* запропоновано співвідношення:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}. \quad (3)$$

Однак в виразі (2) ніяк не враховується рівень індивідуальних мотиваційних характеристик зловмисника. Тому більш гнучким є варіант оцінювання ймовірності P_t:

$$P_t = \frac{\gamma g - D}{\gamma g} = 1 - \frac{D}{\gamma g}, \quad (4)$$

де введено коефіцієнт мотивації γ, що відображає ступінь впливу величини «виграшу» *g* на дії сторони А з активації загрози *T*.

Залежно від індивідуальних властивостей зловмисника коефіцієнт мотивації γ може бути як більше 1 (атакуючій стороні А властивий азарт, авантюризм, впевненість у своєму успіху), так і менший за 1 (зловмисник обережний, не гарячкує, воліє «мати синицю в руці, ніж журавля в небі»). Враховуючи, що значення ймовірності обмежуються діапазоном [0; 1], на область існування значень коефіцієнта мотивації γ накладається умова: $\gamma \geq (D/g)$.

Особливістю наведених вище результатів є те, що вони отримані для гіпотетичного зловмисника, який діє за принципом виключно економічної доцільності. Це типовий «зловмисник-прагматик», якому в першу чергу можуть відповідати три соціально-психологічні типи: аутсайдер – самозайнятий професіонал, аутсайдер – менеджер власного угруповання та інсайдер/аутсайдер – «свояк».

Однак окрім економічної доцільності можливі і інші варіанти мотивації виникнення загрози *T*, наприклад, ображений або мстивий зловмисник («зловмисник-месник»), домінантою дій якого є максимізація втрат *q* власника інформації за умов мінімальних особистих витрат *D*. Частіше за все причиною дій цього зловмисника є певні особисті мотиви, обумовлені непорозуміннями або конфліктними ситуаціями, що виникли за місцем роботи, служби, інше. Формула (4) в цьому випадку приймає вигляд:

$$P_t = \frac{\gamma q - D}{\gamma q} = 1 - \frac{D}{\gamma q}. \quad (5)$$

Очевидно, що «зловмиснику-меснику» можуть відповідати всі варіанти соціально-психологічного типу інсайдер (окрім інсайдера – зловмисника) та інсайдер/аутсайдер – шкідник.

Слід зазначити, що наведені вище формули (4), (5) фактично віддзеркалюють певні сценарії дій зловмисника, що визначаються, як це витікає з викладеного вище, його соціально-психологічним типом, причому рівень домінантної психологічної риси зловмисника, яка є причиною його асоціальної поведінки, оцінюється саме коефіцієнтом γ . Можна виділити декілька класів соціально-психологічних типів зловмисника, які охоплюють різні можливі випадки розвитку атаки та протиправних дій, на базі цих класів оцінити значення коригуючого коефіцієнта γ, уточнюючи таким чином оцінки ймовірності P_t, розраховані із економіко-вартісних моделей. Однак при практичній реалізації цього наміру виникають певні труднощі, обумовлені нелінійним характером залежності коефіцієнта γ від рівня мотивації, у зв'язку з чим спосіб завдання цієї залежності та її оцінювання потребують проведення окремих досліджень. З іншого боку, як це випливає із переліку соціально-психологічних типів зловмисника та їх змістовних характеристик, інформація, що може бути отримана з аналізу цих характеристик, значно ширше за оцінку лише рівня вмотивованості дій зловмисника, наприклад, спроможна віддзеркалити загальну характеристика його небезпечності (зокрема, введений вище коефіцієнт небезпеки конкретного зловмисника *Ph*). Розглянемо цей аспект дещо детальніше.

В загальному випадку ймовірність P_T реалізації загрози T – це добуток

$$P_T = P_t P_v, \tag{6}$$

де P_v – ймовірність вдалого використання зловмисником вразливостей інформаційної системи (ІС), що містить інформаційний ресурс *I*, тому цілком природною є спроба економіко-вартісної інтерпретації цієї ймовірності. За своєю суттю P_v – узагальнена (інтегрована) ймовірність успішного проведення комплексу атак, породжених існуванням сукупності вразливостей ІС (включно із вразливостями самої системи захисту інформації (СЗІ)). Тобто значення ймовірності P_v залежить від ступеню захищеності ІС, який в свою чергу зумовлюється обсягом інвестувань в СЗІ (величиною *c*), і певним чином враховується співвідношенням [3, 7]:

$$P_v = \frac{q}{q+sc}, \tag{7}$$

де *s* – коефіцієнт, можливий діапазон значень якого пов'язаний з існуючою у світовій практиці залежністю між рівнем інвестицій *c* у СЗІ та цінністю критичної інформації для її власника (сторона В). Так, для комерційної таємниці найчастіше $c = (0{,}05 \div 0{,}20)\ q$ [7, 8]. Зокрема для конкретних даних, наведених у [7, 8], маємо нижню межу для: $s \geq 10 \div 45$. З формули (6) очевидно, що за умов відсутності критичної інформації в ІС (тобто q=0) ймовірність P_v =0. При $q >> sc$, тобто при значному рівні критичності ресурсу *I* й низьких витратах на створення і функціонування СЗІ, наслідком чого є об'єктивна неможливість забезпечити адекватний рівень захисту критичної інформації в ІС, ймовірність $P_v \to 1$. В усіх інших випадках ймовірність P_v відмінна від 0, а її значення при q=*const* зростає із спадом рівня інвестицій в СЗІ.

Формула (6) звичайно застосовна разом із формулами (5), (7) для обчислення P_T для «зловмисника-прагматика» або «зловмисника-месника», однак, як показано в [3], вона може застосовуватися самостійно для оцінювання ймовірності реалізації загрози з боку так званого «зловмисника-виконавця». В останньому випадку вираз (6) трансформується у формулу [3]:

$$P_v = \frac{q}{q + s\dfrac{c^2}{D}}. \tag{8}$$

Слід зазначити, що «зловмисник-виконавець» – це, як правило професіонал, який за будь-яких обставин має виконувати поставлене перед ним завдання, тобто для нього ймовірність активації загрози $P_t \equiv 1$ і, відповідно, $P_T \equiv P_v$. Крім того, залежно від важливості поставленого перед ним завдання, «зловмисник-виконавець» у багатьох випадках може розраховувати на залучення для підтримки своїх дій певних додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних. На практиці це означає, що у випадку «зловмисника-виконавця» існує велика ймовірність застосування для реалізації загроз високовитратних атак. Зокрема, якщо $D \to \infty$, то $P_v \to 1$, тобто можна очікувати появу дуже високих значень $P_{v\max}$. Типовим прикладом подібної ситуації є виконання завдання розвідником спецслужби.

Очевидно, що «зловмисник-виконавець» інтегрує в собі цілий ряд соціально-психологічних типів зловмисника, описаних вище та представлених рядками таблиць 1, 2. Зокрема, розглядаючи цю інтеграцію у «вузькому» сенсі, отримуємо такого собі жорсткого «зловмисника-виконавця», який поєднує три соціально-психологічні типи: аутсайдер – найманий професіонал, аутсайдер – менеджер організованого угрупування, інсайдер – зловмисник; в разі інтеграції у «широкому» сенсі маємо більш розмиту модель, до якої можна додати соціально-психологічні типи аутсайдера – менеджера власного угруповання та інсайдера/аутсайдера – «свояка».

Таким чином, в загальному випадку, коли ймовірність успішної реалізації загрози визначається виразом (6), вона залежить від цілого комплексу соціально-психологічних характеристик зловмисника: вмотивованості, цілеспрямованості, енергійності, комунікабельності та контактності, лідерських якостей тощо. Тому можна запропонувати розширення економіко-вартісних моделей, яке врахує соціально-психологічний тип зловмисника:

$$z(\tau) = P_T(\tau)Ph(\tau) = P_t(\tau)P_v(\tau)Ph(\tau), \qquad (9)$$

де $z(\tau)$ - скорегована із врахуванням соціально-психологічного типу зловмисника оцінка ймовірності реалізації загрози T цим зловмисником, $P_T(\tau)$ - вихідне значення оцінки, отримане із економіко-вартісних міркувань, $Ph(\tau)$ - введений вище коефіцієнт небезпеки конкретного зловмисника. Введення параметра часу (змінна τ) до формули (9) відображає факт можливої зміни умов (мотивація зловмисника, загальний стан захищеності системи або об’єкта ризику за час реалізації загрози, зміна типу атаки, яку проводить зловмисник, реалізуючи загрозу T) за час реалізації загрози.

Висновок. Основною та найважливішою проблемою з відбору, оцінювання та обробки інформації, яка, застосовується у процесі аналізу та дослідження ризиків, сьогодні є уже не тільки надання кількісних характеристик параметрам ризиків та самим ризикам, але і визначення соціально-психологічного типу зловмисника та характеру його дій, що вагомо впливає на оцінки ризику та його параметрів. Застосовні нині у дослідженні ризиків економіко-вартісні моделі дають можливість детально проаналізувати стан об’єкту ризику, але не враховують особливості соціально-психологічного типу зловмисника та його ймовірну поведінку у процесі реалізації загрози. Тому для більш точного оцінювання ризику пропонується розширити існуючі економіко-вартісні моделі шляхом залучення до дослідження ризиків інформації про соціально-психологічні характеристики зловмисника. Дане розширення повинне вирішити проблему впливу особистих якостей зловмисників на оцінку інформаційних ризиків в будь-який сферах та галузях застосування аналізу ризиків.

Використання інформації про особливості соціально-психологічного типу зловмисника і його ймовірну поведінку має стати невід’ємною складовою формування нових стандартів в галузі інформаційної безпеки та закриття прогалин в існуючих стандартах.

ЛІТЕРАТУРА

[1]. ISO/IEC 27005 — Information security risk management.
[2]. BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000.
[3]. Архипов О.Є., Скиба А.В. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації // Захист інформації. – 2012. – Том15, №4. – С.366 – 375.
[4]. Gordon L.A., Loeb M.P. (2002), «The Economics of Information Security Investment», ACM Transaction on Information and System Security, Vol.5, No4, pp.438-457.
[5]. Willemson J. (2010), «Extending the Gordon & Loeb Model for Information Security Investment», The Fifth International Conference on Availability, Reliability and Security ARES 2010 , IEEE, 2010.
[6]. Huang, C.D., Hu, Q., and Behara R.S. (2006), «Economics of Information Security Investment in the Case of Simultaneous Attacks», Proceedings of the Fifth Workshop on the Economics of Information Security. June 26-28, Cambridge, England.
[7]. Архипов О.Є., Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков // Захист інформації – 2011. – №2 (51) – С. 69-76.
[8]. Архипов О.Є., Особенности анализа рисков в информационно-коммуникационных системах // Захист інформації – 2012. – №4 (57) – С.18-27.
[9]. Arkhypov O., Skyba A. (2014), "Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models." The Advanced Science Journal, Vol. 12, pp. 75-82.
[10]. Небиліцин В. Д. Темперамент. // Психологія індивідуальних відмінностей. Тексти. / За ред. Ю.Б. Гіппенрейтер, В.Я. Романова. — М.: Видавництво МГУ, 1982. — С. 153–159.
[11]. Щербак А.Е. Преступный человек по Lombroso. / А.Е. Щербак //Санкт-Петербург: типо-лит. П. И. Шмидта, 1889. — [2], 52, [1] с.
[12]. Кречмер, Э. Строение тела и характер / Э. Кречмер // Психологическая типология. – Минск : Харвест, М. : АСТ, 2000. – С. 127 165.
[13]. Шелдон У. Психология конституциональных различий / У. Шелдон // Психологическая типология. – Минск : Харвест, М. : АСТ, 2000. – С. 166-189.

[14]. Юнг К. Психологические типы / К. Юнг. Психологические типы // М. : Изд во Эксмо Пресс, 2001. – 480 с.
[15]. Майерс И., Майерс П. MBTI. Определение типов. У каждого свой дар / И. Майерс // М: Издательство: «Бизнес Психологи», 2010. - ISBN 978-5-91809-004-6, твердый переплет, 320 стр.
[16]. Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Richardson, R. (2006). 2006 CSI/FBI computer crime and security survey. Computer Security Journal, Vol. 22(3).
[17]. Овчинников Б.В., Павлов К.В., Владимирова И.М. Ваш психологический тип./ Б.В. Овчинников // СПБ.: «Андреев и сыновья», 1994. – 238 с.
[18]. Личко А. Е. Психопатии и акцентуации характера у подростков / Под ред. Ю. Б. Гиппенрейтер, В.Я. Романова. // Санкт-Петербург: Речь, 2009. — 256 с. — 1000 экз. — ISBN 978-5-9268-0828-6.
[19]. Айзенк Г. Дж. Коэффициент интеллекта. / Г. Дж. Айзенк // Киев: Гранд, 1994. — 112 с. — 50 000 экз. — ISBN 5-7707-3600-8.
[20]. Ганнушкин П.Б. Клиника психопатий, их статика, динамика, систематика./ П.Б. Ганнушкин // - Нижний Новгород: Издательство Нижегородской государственной медицинской академии, 1998. — 124 с. — 5000 экз. — ISBN 5-86093-015-1.
[21]. Личко Андрій Євгенович Психопатии и акцентуации характера у подростков / Під ред. Ю.Б. Гиппенрейтер, В.Я. Романова. // Санкт-Петербург: Речь, 2009. — 256 с. — 1000 прим. — ISBN 978-5-9268-0828-6.
[22]. Rotter J.B. Generalized expectancies for internal versus external control of reinforcement. / J.B. Rotter// Psychol. Monogr., 1966, V. 8, № 1 (Whole № 609).– СПб: Издательство «Питер», 1999.
[23]. Аугустинавичюте А. Соционика./ А. Аугустинавичюте // М.: «Чёрная белка», 2008. - 568 стр. - ISBN 978-5-98982-005-4.
[24]. Мясищев В.Н. Личность и неврозы / В.Н. Мясищев. // Л.: Изд-во ЛГУ, 1960. 426 с.
[25]. Базыма Б.А. Цветовой тест Макса Люшера. / Б.А. Базыма // М., 2001. – 135 с.
[26]. Егоров А. С. Эмпедокл и проблема греческого шаманизма/ А. С. Егоров // Вопросы философии. - 2007. - № 8. - С. 97-105.
[27]. Adize I. Leading The Leaders: How To Enrich Your Style of Management and Handle People Whose Style Is Different From Yours. / I. Adize // М.: «Альпина Паблишер», 2011. - С. 259. - ISBN 978-5-9614-1374-8.
[28]. Хадсон Р. Эннеаграмма. Тип личности как индивидуальность / Р. Хадсон // HR. – 1998. – № 6.

REFERENCES

[1]. ISO/IEC 27005 — Information security risk management.
[2]. BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000.
[3]. Arhupov A., Skyba A. (2012), «Information risk: research methods and techniques, models and methods of risk identification», Information Security Research Journal, Vol 15, №4, pp. 366 – 375.
[4]. Gordon L.A., Loeb M.P. (2002), «The Economics of Information Security Investment», ACM Transaction on Information and System Security, Vol.5, No4, pp. 438-457.
[5]. Willemson J. (2010), «Extending the Gordon & Loeb Model for Information Security Investment», The Fifth International Conference on Availability, Reliability and Security ARES 2010, IEEE, 2010
[6]. Huang C.D., Hu, Q., and Behara R.S. (2006), «Economics of Information Security Investment in the Case of Simultaneous Attacks», Proceedings of the Fifth Workshop on the Economics of Information Security. June 26-28, Cambridge, England.
[7]. Arhypov O. (2011), «Primenenie ekonomiko-motivatsionnyih sootnosheniy dlya otsenivaniya veroyatnostnyih parametrov informatsionnyih riskov», Ukrainian Information Security Research Journal, Vol. 2 (51), pp.69-76.
[8]. Arhypov A. (2012), «Features of the analysis of risks in information and communication systems», Information Security, Vol.4 (57), pp.18 -27.
[9]. Arhypov O., Skyba A. (2014), «Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models», The Advanced Science Journal, 2014, Vol. 2, pp. 75-82.
[10]. NebilItsin V.D. (1982), «Temperament. PsihologIya Individualnih vidminnostey. Teksti», M.: Vidavnitstvo MGU, pp. 153–159.
[11]. Scherbak A. (1889), «Prestupnyiy chelovek po Lombroso», Sankt-Peterburg: tipo-lit. P. I. Shmidta.
[12]. Krechmer E. (2000), «Stroenie tela i harakter», Minsk: Harvest, pp. 127-165.
[13]. Sheldon U. (2000) «Psihologiya konstitutsionalnyih razlichiy», Minsk: Harvest, pp. 166-189.
[14]. Yung K. (2001), «Psihologicheskie tipy», M.: Izd-vo Eksmo Press.
[15]. Mayers I., Mayers P. (2010), «MBTI. Opredelenie tipov. U kazhdogo svoy dar», M: Izdatelstvo: «Biznes Psihologi».
[16]. Gordon, L.A., Loeb, M.P., Lucyshyn W., Richardson R. (2006), «2006 CSI/FBI computer crime and security survey», Computer Security Journal, Vol. 22(3).
[17]. Ovchinnikov B.V., Pavlov K.V., Vladimirova I.M. (1994) «Vash psihologicheskiy tip», SPB.: «Andreev i syinovya».
[18]. Licko A. (2009), «Psyhopatyy accentuation nature and adolescents», SPB: Speech.
[19]. Ayzenk G. (1994), «Koeffitsient intellekta», Kiev: Grand.
[20]. Gannushkin P.B. (1998), «Klinika psihopatiy, ih statika, dinamika, sistematika», Nizhniy Novgorod: Izdatelstvo Nizhegorodskoy gosudarstvennoy meditsinskoy akademii.
[21]. Lichko A. (2009), «Psihopatii i aktsentuatsii haraktera u podrostkov».

[22]. Rotter J.B. (1999), «Generalized expectancies for internal versus external control of reinforcement», Psychol. Monogr., 1966, V. 8, № 1 (Whole № 609), SPB: Izdatelstvo «Piter».
[23]. Augustinavichyute A. (2008), «Sotsionika», M.: «Chornaya belka».
[24]. Myasischev V.N. (1960), «Lichnost i nevrozyi» Л.: Изд-во ЛГУ, 1960. 426 с.
[25]. Bazyima B.A. (2001), «Tsvetovoy test Maksa Lyushera», Moskov.
[26]. Egorov A. S. (2007), «Empedokl i problema grecheskogo shamanizma» / A. S. Egorov // Voprosyi filosofii Vol 8., pp. 97-105.
[27]. Adize I. (2011), «Leading The Leaders: How To Enrich Your Style of Management and Handle People Whose Style Is Different From Yours. « M.: «Альпина Паблишер», 2011, p. 259, ISBN 978-5-9614-1374-8.
[28]. Hadson R. (1998), «Enneagramma. Tip lichnosti kak individualnost».

РАСШИРЕНИЕ ЭКОНОМИКО-СТОИМОСТНЫХ МОДЕЛЕЙ ИНФОРМАЦИОННЫХ РИСКОВ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИХ ТИПОВ ЗЛОУМЫШЛЕННИКА

Рассматриваются социально-психологические характеристики злоумышленника и их применение с экономико-стоимостными моделями для оценки информационных рисков и оптимальных инвестиций в информационную безопасность. Для проведения адекватной оценки информационных рисков и определения оптимальных инвестиций существующие экономико-стоимостные модели требуют расширения с учетом социально-психологических характеристик злоумышленника, которые существенно влияют на оценку рисков. Современные методы оценки информационных рисков, которые опираются на существующие нормативно-правовые документы не учитывают социально-психологические характеристики злоумышленников, приводит к некорректному проведению оценки, уменьшая ее точность. Предложенное расширение экономико-стоимостной модели с учетом социально-психологических характеристик злоумышленника позволяет повысить оценку информационных рисков и оптимизировать инвестиции в информационную безопасность. Предложено 10 социально-психологических типов злоумышленника, использование которых позволяет расширить применение и повысить точность оценки экономико-стоимостной модели при проведении оценки информационных рисков.

Ключевые слова: информационная безопасность, оценка рисков, экономико-стоимостные модели, социально-психологические типы злоумышленников, психотип, классификации психотипов информационной безопасности.

THE EXTANDING OF ECONOMIC-COST MODEL OF INFORMATION SECURITY RISKS MANAGMENT BY THE USE OF SOCIAL-PSYCHOLOGICAL TYPES OF INTRUDERS

In this article we study the socio-psychological characteristics of the attacker and their use with economic-cost model for assessing information risks and optimal investment in information security. An adequate assessment of information risk and determining the optimal investment by existing economic and cost models require expansion with the socio-psychological characteristics of the attacker, which significantly affect the assessment of the risks. Modern methods of estimation of information risks, which are based on existing legal documents doesn't take into account the socio-psychological characteristics of the attackers, leading to incorrect assessment, reducing its accuracy. The proposed expansion of economic-cost model, taking into account the socio-psychological characteristics of the attacker, which increases the risk assessment of information and optimize investment in information security. We present 10 socio-psychological types of attacker for using with economic-cost models which allows to expand the use and improve the accuracy of estimates of economic-cost model in the evaluation of information risks.

Index terms: information security, risk assessment, economic and cost models, socio-psychological types of intruders, psycho, psycho-classification of information security.

Архипов Александр Евгеньевич, доктор технических наук, профессор кафедры информационной безопасности НТУУ «КПИ».
Email: sonet@zeos.net
Архипов Олександр Євгенійович, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ».
Oleksandr Arkhypov, Dr. Sci. Tech., professor at the Department of Information Defense at National Technical University of Ukraine «Kyiv Polytechnic Institute».

Скиба Андрій Володимирович, аспірант НТУУ «КПІ».
Email: andrewskyba@ukr.net
Скиба Андрей Владимирович, аспірант НТУУ «КПИ».
Andrii Skyba, PhD student NTUU «KPI».

Хоріна Олена Іванівна, молодший науковий співробітник Інституту соціальної та політичної психології НАПН України.
Email: olena_khorina@ukr.net
Хорина Елена Ивановна, младший научный сотрудник Института социальной и политической психологии НАПН Украины.
Olena Khorina, junior researcher of the Institute of Social and Political Psychology Academy of Pedagogical Sciences of Ukraine.