ІНФОРМАЦІЙНА БЕЗПЕКА:
ВИКЛИКИ І ЗАГРОЗИ
СУЧАСНОСТІ

ЗБІРНИК МАТЕРІАЛІВ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ,
5 квітня 2013 р., м. Київ

Київ
Центр навчально-наукових та науково-практичних видань
Національної академії СБ України
2013
ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Співголови: Щомоткін О.В., кандидат юридичних наук, професор, заслужений юрист України; Пилипчук В.Г., доктор юридичних наук, професор, член-кореспондент НАПрН України.

Заступники голови: Фурисов В.М., кандидат технічних наук, старший науковий співробітник, доцент; Хлевицький В.Б., кандидат юридичних наук, старший науковий співробітник.

Члени організаційного комітету:

Бровко В.Д., кандидат технічних наук; Марущак А.І., доктор юридичних наук, професор; Пачченко В.М., кандидат юридичних наук, старший науковий співробітник; Остроухов В.В., доктор філософських наук, професор; Мельник С.В., кандидат технічних наук; Левонов Д.Б., Філоненко І.О.


Укращено матеріали, підготовлені фахівцями та науковцями Служби безпеки України, Науково-дослідного інституту інформатики і права НАПрН України, Військового інституту Ківського національного університету імені Тараса Щепченка, Національного авіаційного університету, Національного університету оборони України, інших установ і організацій.

Тези доповідей публікуються в авторській редакції з незначними коректорськими правками.

© НА СВ України, 2013
ВИЗНАЧЕННЯ ВЕЛИЧИНИ МОЖЛИВОЇ ШКОДИ
У РАЗИ РОЗГОЛОШЕННЯ ІНФОРМАЦІЇ
З ОБМЕЖЕНИМ ДОСТУПОМ
ЧИ ВТРАТИ ЇЇ МАТЕРІАЛЬНИХ ПОСІВ

Сучасний інформаційний простір складається з відкритої інформації, яка вільно поприходить, обробляється і зберігається, та тієї, доступ до якої обмежено, — інформації з обмеженим доступом (ІзОД) [1]. Таке обмеження доступу здійснюється відповідно до закону [2], якщо вона містить конфіденційну, службову чи таємну інформацію при дотриманні сукупності вимог, коли розголошення такої інформації може завдати істотної шкоди інтересам національної безпеки або шкода від оприлюднення переважає суспільний інтерес в її отриманні та/чи. Тобто, можна стверджувати, що якщо немає завдання шкоди, то відсутні підстави для обмеження у доступі.

Наразі питання визначення величини цієї шкоди постає досить гостро. Адже саме її розмір повинен визначати, до якого виду ІзОД слід віднести інформацію, в різі її розголошення чи втрати матеріальних послів (МП), наприклад, до конфіденційної — якщо шкода завдається фізичній чи юридичній особі, крім суб’єктів владних пов-
новажень (наприклад, персональні дані [3]), і тому порядок його поширення визначений за їхнім бажанням відповідно до передбачених умов: до службовців — якщо школа здається суб’єктам владних повноважень у певному напрямі діяльності установи або при здійсненні контрольних, наглядових функцій органами державної влади, в процесі прийняття рішень, оперативно-розшукової, контр-розшукової діяльності, що передають публічному обговоренню; до таємної — якщо школа здається особі, суспільству й державі та інформація містить державну, професійну, охоронну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю, наприклад, таємницю усунення, лікарську таємницю тощо. Із перерахованих видів таємниць досить добре врегульовано державну таємницю (ДТ) [4], адже це питання забезпечення національної безпеки [5].

Як відомо, розмежування основних видів ІзОД відбувається за ступенем та грифом обмеження доступу для МНІ, що демонструє своєрідну нечіткість величини можливої шкоди, наприклад, для службової інформації — “для службового користування” (ДСК), а для таємної інформації, зокрема державної таємниці (за ступенем та грифом секретності) — “таємно” (Т), “шифром таємно” (ЦТ), “особливої важливості” (ОВ).

Питанням визначення величини можливої шкоди національний безпеці держави у разі розголошення ДТ чи втрати матеріальних носіїв секретної інформації (МНСІ) займається обмежене коло науковців України (Корченко О.Г., Архипов О.Є., Мурацов О.Є., Борошко В.П., Касперський І.П.).


Для прийняття рішення, наприклад, у судовому процесі, щодо визначення розміру збитків, завданого національній безпеці держави в разі розголошення ДТ чи втрати МНСІ необхідно за допомогою наявних засобів у сфері охорони ДТ (ОДТ) проводити аналіз і оцінювання розмірів можливої шкоди. Результат оцінювання величини шкоди має бути зрозумілим та вираженим у прийнятних показниках (громадам) для подальшого її відшкодування, тощо.

На основі проведеного дослідження розроблено базову модель інтегрованого представлення параметрів шкоди шляхом логіко-
лінгвістичного підходу та узагальнення ідентифікуючих і оціночних показників засобів у сфері ОДТ; метод [9]; методологію синтезу системи, систему аналізу й оцінювання величини можливої шкоди національній безпеці держави у разі розголошення ДГ чи втрати МНСІ та відповідно програмне забезпечення з можливістю автоматизованого формування звіту отриманих результатів.

Залишається актуальним питання визначення величини можливої шкоди в разі розголошення конфіденційної, наприклад персональних даних, чи службової інформації або втрати їх МНІ, де, наприклад, $0 < N < 1$ може бути критерієм для визначення ДСК.

**ЛІТЕРАТУРА**


Засядько А.А.,
доктор технічних наук, доцент,
Університет банківської справи НБУ, ЧВС, м. Черкаси

Клювак О.В.,
Університет банківської справи НБУ, ПБС, м. Львів

ПОСИЛЕННЯ БЕЗПЕКИ ЗДІЙСНЕННЯ ТРАНЗАКЦІЙ В ІНТЕРНЕТ-БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМАХ
Дрейс Ю.О.
Визначення величини можливої шкоди у разі розголошення інформації з обмеженим доступом чи втрати її матеріальних носіїв ................................................................. 235
Засядько А.А., Клювак О.В.
Посилення безпеки здійснення транзакцій в інтернет-відомчих платежних системах віртуальними картками ........................................ 238
Іванова О.С.
Формування дидактичного комплексу при викладанні математичних дисциплін для студентів та курсантів ......................................................... 241
Кузнецов О.О., Рябуха Ю.М., Колованова Е.П.
Дослідження сучасних режимів блокового симетричного шифрування .............................................................. 244
Куцій М.С., Гринь А.К.
Використання синергетичного підходу в моделюванні систем кібернетичної безпеки середнього бізнесу ......................................................... 246
Ланое Д.В.
Лінії трендів інформаційних операцій та їх відображення в інформаційному просторі ................................................................. 249
Мельник С.В., Клочук В.І.
Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави ......................................................... 253
Микол Ю.П.
Визначення підходів щодо захисту інформації під час організації служби прикордонних нарядів ................................................................. 255
Муратов О.Є.
Теоретико-ігрове бачення визначення цінності інформації ............ 258
Пермляков О.Ю., Варламов І.Д., Ляшенко І.О.
Методологічні аспекти захисту інформації в єдиній автоматизованій системі управління сектором безпеки й оборони України ......................................................... 261
Прохоровський Р.В., Бакута А.Ю.
Методи захисту від DDoS-атак ................................................................. 264
Решетніков О.В.
Методика підготовки фахівців з технічного захисту інформації ................................................................. 267
Ришевич О.І., Житніков П.І.
Використання АСУ "ТЕЗАУРУС" для оптимізації роботи об’єктів подійного призначення ................................................................. 269
Самарій В.П., Самарій Р.В.
Моделювання безпеки в теорії графів ................................................................. 272