УДК 004.056.5

МОДЕЛЬ ТА МЕТОД ОЦІНКИ РИЗИКІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ЇХ ОБРОБКИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Олександр Корченко, Юрій Дрейс, Ірина Лозова

Розглядається питання необхідності захисту персональних даних, які створюються і обробляються прикладним програмним забезпеченням в автоматизованих системах. Аналіз існуючого законодавства вказує на обов'язковість захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої визначена законом. Так як персональні дані можуть бути віднесені до конфіденційної інформації про особу, то вони потребують захисту на рівні застосування комплексної системи захисту інформації. Її впровадження передбачає проведення оцінки ризиків загроз на етапі розробки політики безпеки в частині визначення необхідних заходів та засобів захисту інформації. Запропоновано базову модель представлення параметрів ризику, які визначені на установлених законодавством критеріях у сфері забезпечення захисту персональних даних. Розроблено метод оцінки ризиків за результатами якого надаються рекомендації щодо вибору політики безпеки для захисту персональних даних, доповнення стандартного функціонального профілю захищеності необхідними послугами безпеки, визначення величини нанесеної шкоди людині, суспільству, державі у разі втрати таких персональних даних.

Ключові слова: *персональні дані, оцінка ризиків, політика захисту персональних даних, оцінка шкоди у разі втрати персональних даних.*

Актуальність. Розвиток інформаційних технологій призводить до стрімкого зростання кількості інцидентів, атак та загроз щодо окремих інформаційних ресурсів. Згідно з вимогами закону України «Про захист інформації в інформаційно-телекомунікаційних системах» для забезпечення безпеки оброблюваних в автоматизованій системі (АС) державних інформаційних ресурсів (ДІР) або інформації з обмеженим доступом (ІзОД), необхідно розробляти комплексну систему захисту інформації (КСЗІ). Проте прогрес у сфері розробки та впровадження програмного забезпечення, активність у формуванні баз персональних даних (БПД), надзвичайно загострили проблему захисту приватного життя фізичних осіб та інших основних прав і свобод людини. Часті випадки із посяганням на приватну інформацію піднімають проблему відсутності адекватних гарантій захисту персональних даних під час їх обробки в АС.

З огляду останніх подій, а саме факту несанкціонованого втручання в роботу АС Міністерства юстиції України через блокування інформації і порушення встановленого порядку її маршрутизації, що призвело до припинення функціонування Державних та Єдиних реєстрів інформаційної мережі, виникають питання до належного та гарантованого захисту окремих ДІР. Це стосується саме тих ресурсів, які містять дані про фізичних осіб, що обробляються без їх згоди в інтересах національної безпеки, економічного добробуту та прав людини, тобто, *персональних даних* (ПД) (як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована) розпорядником яких є держава. Отже ПД, крім знеособлених, за режимом доступу є ІзОД, а саме конфіденційною інформацією (доступ до якої обмежено її власником). Тому держава, як розпорядник ПД, якому за законом України «Про захист персональних даних» надано право обробляти ці дані від імені володільця, повинна не тільки визначати склад цих ПД, мету і процедуру їх обробки, але й забезпечувати захист такої КІ у власних системах [1].

Метою статті є розробка моделі та методу оцінки ризиків захисту ПД за результатами якого надаються рекомендації щодо вибору політики безпеки для захисту ПД, доповнення стандартного функціонального профілю захищеності необхідними послугами безпеки, визначення величини нанесеної шкоди людині, суспільству, державі у разі втрати таких ПД.

Основна частина. Сьогодні забезпечення захисту ПД потребує неабиякої уваги, про що наголошується у рішенні Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року. А саме у необхідності вживання додаткових заходів щодо захисту ІзОД (насамперед ПД, що належать до конфіденційної інформації) під час її обробки в АС [2].

Слід відмітити, що у багатьох країнах для аналізу і оцінки ризиків використовують статистичні дані про інциденти та загрози інформаційної безпеки. В Україні відсутня відповідна державна політика відносно застосування такої статистичної інформації, особливо щодо порушень у сфері захисту ПД, які обробляються в АС. Наразі існує Типовий порядком обробки ПД (далі – Порядок) [3] за яким визначено загальні вимоги до обробки та захисту ПД суб'єктів ПД, що обробляються повні-

стю чи частково із застосуванням АС. Тобто встановлено типовий (мінімальний) перелік організації заходів, які необхідно реалізувати володільцю ПД для їх захисту. Відповідальність за забезпечення захисту ПД на всіх етапах їх обробки в АС діючим законодавством покладено на володільців, розпорядників ПД і власників цих систем шляхом вжиття необхідних заходів, у тому числі, організаційних та технічних (наприклад, у [4] пропонується застосування в ІТС/АС мережевого захисту (міжмережеві екрани, системи виявлення втручань (вторгнень), засоби створення VPN, засоби оцінки захищеності) від несанкціонованого доступу під час обробки ПД, впровадження процедур авторизації користувачів, забезпечення антивірусного захисту, а також використання технічних засобів безперебійного живлення елементів АС, яка здійснює обробку ПД). Конкретних способів, методів і засобів захисту, та достатність їх застосування для досягнення необхідного рівня захищеності ПД оброблюваних в АС законодавством невизначено. Тому, залишається відкритим питання щодо остаточного вибору заходів захисту, технічних рішень та стандартів, якими необхідно керуватися, архітектури ІТС/АС і покладається в межах компетенції на володільців, розпорядників і власників цих систем разом з безпосередньою оцінкою ризиків порушень безпеки даних, тобто захисту ПД. Слід зазначити, що Порядком [3] взагалі не передбачається застосування КСЗІ для захисту ПД під час їх обробки в АС. Це суперечить вимогам законодавства щодо умов обробки та захисту ДІР або ІзОД в АС, а також варіантів застосування КСЗІ, приведених у таблиці 1.

Для визначення вхідних, вихідних та внутрішніх параметрів забезпечення захисту ПД, які використовуються для оцінки ризиків, проведено дослідження міжнародних стандартів та існуючих методик [5] на основі яких розроблено модель оцінки ризиків захисту ПД під час їх обробки в АС. Дана модель [6] містить набір параметрів представлення ризиків захисту ПД [7], що обробляються в АС, має типову структуру і реалізується методом [8] шляхом виконання 6 етапів (рис. 1).

Таблиця 1

Варіанти застосування атестованої КСЗІ

Форма власності	**Режим доступу**	
	Відкрита інформація	**Інформація з обмеженим доступом**
Державна	*Атестовану КСЗІ треба застосовувати завжди*	*Атестовану КСЗІ треба застосовувати завжди*
Недержавна (приватна)	*Застосування атестованої КСЗІ не вимагається*	*Атестовану КСЗІ треба застосовувати тільки тоді, коли захисту цієї інформації вимагає закон*

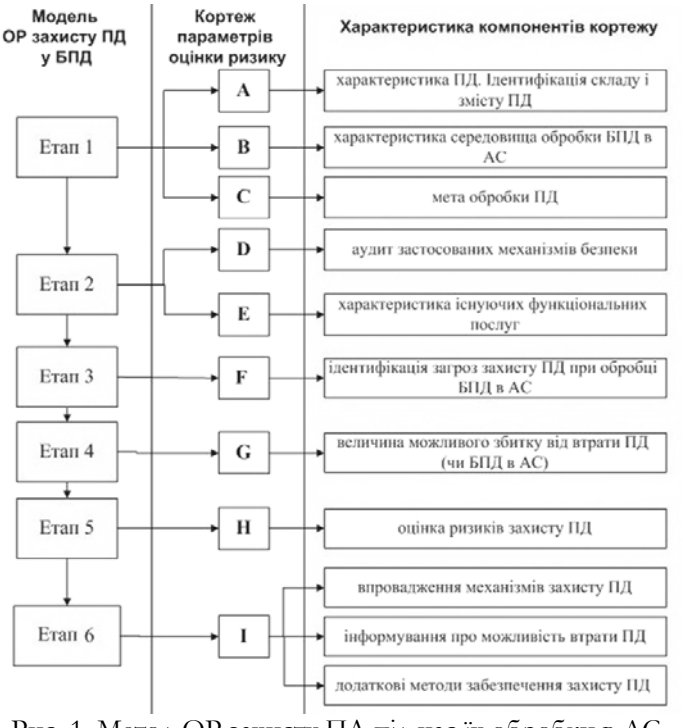

Рис. 1. Метод ОР захисту ПД під час їх обробки в АС

Інтегроване представлення параметрів ризику з відображенням на сферу захисту ПД в АС здійснюється у вигляді кортежу [8], який можна представити у наступному вигляді: ***<A, B, C, D, E, F, G, H, I>***, де *A* – характеристика ПД (ідентифікація їх складу та змісту); *B* – характеристика середовища обробки БПД в АС; *C* – мета обробки ПД; *D* – аудит застосованих механізмів безпеки; *E* – характеристика існуючих функціональних послуг безпеки; *F* – ідентифікація загроз безпеці ПД при обробці БПД в АС; *G* – величина можливих збитків від втрати ПД; *H* – оцінка ризику захисту ПД в АС; *I* – керування ризиком та досягнення необхідного рівня гарантій захисту ПД.

Перший наведений в кортежі компонент – *характеристика та ідентифікація складу і змісту ПД* **(A)**. Законодавством визначено [3], що до ПД відносять відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. Розглянемо загальновідомі ПД склад та зміст яких можна відобразити у вигляді символьної змінної A_n, що приймає одне й те саме значення кінцевої множини ідентифікаторів $A_n \in \{A_1, A_2, A_3, A_4, A_5, A_6, A_7 \dots A_n\}$ (індекс *n* – номер ідентифікатору матеріального носія, що містить такі ПД (наприклад, документу). До складу зазначених ПД належать відомості про: A_1 = «Прізвище, ім'я, по батькові»; A_2 = «Дата і місце народження»; A_3 = «Відомості про освіту»; A_4 = «Ідентифікаційний код»; A_5 = «Відомості з військового квитка»; A_6 = «Відомості з водійських прав»; A_7 = «Відомості з свідоцтва про народження (одруження, тощо)»; A_8 = «Паспортні дані»; A_9 = «Відомості про склад сім'ї»; A_{10} = «Відомості про стан здоров'я»; A_i = «Інші дані (видані на ім'я особи, тощо)». Приклад загальновідомих документів, що містять ПД та їх коефіцієнти важливості (K_{vd}) (або цінності для власника) приведено у таблиці 2.

Таблиця 2

Приклад документів, що містять ПД та їх важливість

Параметр	**Документ, що містить персональні дані**	**Коефіцієнт важливості (K_{vd})**
A_1	*Паспорт (в т.ч. закордонний)*	*0,9*
A_2	*Військовий квиток*	*0,8*
A_3	*Свідоцтво про народження*	*0,7*
A_4	*Ідентифікаційний код*	*0,6*
A_5	*Водійські права*	*0,6*
A_6	*Свідоцтво про шлюб*	*0,5*
A_7	*Трудова книжка*	*0,5*
A_8	*Медична картка*	*0,4*
A_i	*Інші документи*	*[0 ÷ 1]*

Під другим компонентом кортежу – середовищем обробки БПД (B), слід розуміти програмне забезпечення (ПЗ) у якому виконувалися будь-які дії, пов'язані з внесенням, модифікацією, знищенням ПД у БПД. У таблиці 3 наведено перелік такого ПЗ та його рівень функціональної складності (K_vp) для користувача.

Таблиця 3

Середовище обробки ПД та його складність

Параметр	**Середовище обробки**	**Рівень складності (K_{vp})**
B_1	*«MS Word»*	*0,3*
B_2	*«MS Excel»*	*0,4*
B_3	*«MS Access»;*	*0,5*
B_4	*«Кадри»*	*0,6*
B_5	*«Працівники»*	*0,7*
B_6	*«Парус»*	*0,8*
B_7	*«1С»*	*0,9*
B_i	*«Інші засоби»*	*[0 ÷ 1]*

Третій параметр оцінювання ризику – *мета обробки ПД* **(C)**. Мета обробки ПД визначається в залежності від того, саме де та для якого очікуваного кінцевого результату такі ПД будуть оброблятися. Даний параметр представляється у вигляді множини ідентифікаторів згідно до законодавства: $C_n \in \{C_1, C_2, C_3, C_4, C_5, C_6 \dots C_i\}$: C_1 = «Забезпечення реалізації трудових, соціально-трудових відносин, відносин у сфері управління персоналом, військового обліку»; C_2 = «Забезпечення адміністративно-правових відносин»; C_3 = «Забезпечення відносин у сфері бухгалтерського і податкового обліку»; C_4 = «Забезпечення національної безпеки, економічного добробуту та прав людини»; C_5 = «Захист прав і свобод фізичних осіб, ПД яких обробляються, чи прав інших суб'єктів відносин, пов'яза-

них із ПД, а також з метою боротьби із злочинністю»; C_6 = «Забезпечення суб'єктів відносин, пов'язаних із ПД, зведеною знеособленою інформацією щодо ПД згідно закону»; C_i = «Інша мета».

Наступним компонентом кортежу є *аудит застосованих механізмів безпеки* **(D)**. Даний компонент описується набором елементів $D_n \in \{D_1, D_2, D_3, D_4, D_5 \dots D_i\}$ та визначається перевіркою наявних в АС організаційно-правових та програмно-технічних заходів та механізмів захисту ПД оброблюваних в АС, до яких можна віднести: D_1 = «Наявність згоди суб'єкта ПД на їх обробку в АС»; D_2 = «Ідентифіковано володільця чи розпорядника БПД, третю особу та встановлено Типовий порядку обробки ПД у БПД»; D_3 = «Отримано Свідоцтво про реєстрації БПД уповноваженим органом з питань захисту ПД у Державному реєстрі БПД»; D_4 = «Призначено відповідальну особу за обробку та захист ПД або створено службу захисту інформації (з обов'язками захисту ПД)»; D_5 = «Застосовано систему управління (менеджменту) інформаційною безпекою або атестовану КСЗІ з реалізованим стандартним профілем *х.КІ.х*, *х.КД.х*, *х.КЦД.х* (за додатком А НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»)»; D_n = «Інші механізми захисту».

Після проведення аудиту застосованих механізмів безпеки, доцільним є *визначення наявних послуг безпеки* **(E),** як п'ятого елементу кортежу, що визначаються множиною ідентифікаторів $E_n \in \{E_1, E_2, E_3, E_4\}$. З урахуванням того, що у сфері захисту інформації ризик пов'язаний з такими базовими характеристиками безпеки як конфіденційність, цілісність, доступність і спостережність, то на даному етапі слід встановити існуючі в АС критерії захищеності [4, 5]: E_1 = «Конфіденційність {*КА, КВ*}»; E_2 = «Цілісність {*ЦА, ЦВ*}»; E_3 = «Доступність {*ДС*}»; E_4 = «Спостережність {*НР, НІ, НО, НВ, НА, НП, НК*}».

Шостим параметром є *ідентифікація загроз безпеці ПД при обробці БПД в АС* **(F)**. Перелік можливих загроз визначається існуючими стандартами та методиками аналізу і оцінки ризиків інформаційної безпеки [6] і може доповнюватись самостійно. Даний параметр наводиться у вигляді набору елементів відомих загроз безпеці ПД, а саме [3]: $F_n \in \{F_1, F_2, F_3, F_4, F_5, F_6 \dots F_i\}$: F_1 = «Шпигунство»; F_2 = «Неумисні помилки користувачів»; F_3 = «Несанкціонований доступ (збирання, видалення, пошкодження, модифікація, поширення тощо)»; F_4 = «Блокування інформації і порушення встановленого порядку її маршрутизації»; F_5 = «Збій у роботі обладнання та внутрішня відмова АС»; F_6 = «Неналежна передача ПД третій особі; F_i = «Інші можливі загрози».

По відношенню до визначених загроз визначається ймовірність їх реалізації (настання) **(P)** як: «низька» (P_{r_1}), «середня» (P_{r_2}) та «висока» (P_{r_3}), що приведено формулою (1):

$$P_{riv\_zag} = \left\{\cup_{i=1}^{n} P_{r_i}\right\} = \left\{P_{r_1}, P_{r_2}, P_{r_3}, \dots, P_{r_i}\right\},\ R_{riv\_zag} \in \left\{R_{riv_{zag\,i\,max}}\right\}, (i = \overrightarrow{1,n}), \quad (1)$$

де n – кількість запропонованих загроз, і – номер загрози.

Сьомий параметр кортежу – *величина нанесених збитків* **(G)**, може визначатися як кількісними так і якісними показниками. Оцінка збитків проводиться за шкалами відомих методик, що характеризують матеріальну чи моральну шкоду, шкоду національній безпеці [9], шкоду від порушення прав і свобод людини тощо. Шкали величини можливих збитків від втрати ПД приведені у таблиці 4.

Таблиця 4

Шкали величини можливих збитків від втрати ПД

Величина збитку (G)	Інтервальна шкала (І)	Бальна шкала	Відсоткова шкала	Грошова шкала
G_1	*0 ÷ 0,1*	*1*	*0 – 10%*	*0 – 100$*
G_2	*0,11 ÷ 0,3*	*2*	*11% – 30%*	*100– 1000$*
G_3	*0,31 ÷ 0,6*	*3*	*31% – 60%*	*1000– 10000$*
G_4	*0,61 ÷ 0,8*	*4*	*61% – 80%*	*10000– 100000$*
G_5	*0,81 ÷ 1,0*	*5*	*81 % – 100%*	*>100000$*

Після визначення загальних параметрів, переходимо безпосередньо до восьмого параметра кортежу – оцінки ризику захисту ПД в АС (H). Під ризиком захисту ПД під час їх обробки в АС розуміється функція ймовірності реалізації загрози до виду і величини завданих збитків від можливої втрати ПД при наявності уразливостей та ступеня їх прийнятності для експлуатації АС, що визначається за формулою:

$$H=P\times G, \quad (2)$$

де P – ймовірність реалізації загрози; G – величина завданих збитків.

Завершальним етапом є визначення останнього параметру кортежу – керування ризиком та досягнення необхідного рівня захищеності ПД в АС (I). На даному етапі за допомогою таблиці відповідності отриманих значень параметрів P та G (табл. 5) визначається необхідний рівень захищеності ПД в АС від 1 до 5 балів для застосування рекомендованої політики безпеки.

Таблиця 5

Оцінка рівня захищеності ПД в АС

Величина завданих збитків (G)	**Ймовірність реалізації певної загрози (P)**				
	0-0,1	*0,1-0,3*	*0,3-0,6*	*0,6-0,8*	*0,8-1,0*
0-100$	*1*	*1*	*2*	*3*	*3*
100-1000$	*1*	*2*	*2*	*3*	*4*
1000-10000$	*2*	*2*	*3*	*4*	*4*
10000-1000000$	*3*	*2*	*4*	*4*	*5*
>1000000$	*3*	*4*	*4*	*5*	*5*

Рекомендовані політики безпеки, що сформовані за результатами аналізу вимог законодавства України у сфері забезпечення захисту ПД, приведені у таблиці 6.

Таблиця 6

Рекомендовані політики безпеки

Рівень в балах	**Рекомендовані політики безпеки**
1	*Виконання ОЗЗІ (організаційно-провових заходів захисту інформації)*
2	*Створення СЗІ (служби ЗІ) або призначення відповідальної особи*
3	*Використання ТЗІ/КЗІ (технічного та/або криптографічного ЗІ)*
4	*Використання КЗЗ (комплексу засобів захисту)*
5	*Застосування КСЗІ (комплексної системи захисту інформації)*

Передбачається перегляд сукупності заходів щодо оцінки ризику, вибору, реалізації і впровадження заходів (механізмів) захисту ПД у БПД в АС, що проводяться протягом всього життєвого циклу АС і спрямовані на досягнення прийнятного рівня залишкового ризику. Проводиться необхідне інформування про можливість несанкціонованого доступу або втрати ПД уповноваженого державного органу з питань захисту ПД. Вживаються додаткові заходи щодо забезпечення захисту ПД (обов'язкові чи вибіркові) [10, 11], спеціальні засоби технічного та криптографічного захисту інформації (шифрування даних) згідно з політикою безпеки. Далі, в основі рекомендованої політики безпеки, передбачено застосування необхідних заходів та засобів [10-12] через їх впровадження в АС для підвищення рівня захищеності ПД.

Приклад роботи методу

Етап 1. Визначаємо документи у яких наявні ПД та коефіцієнт їх важливості, відповідно до табл. 2: паспорт (A_1), $K_{vd1}=0{,}9$; військовий квиток (A_2), $K_{vd2}=0{,}8$; свідоцтво про народження (A_3), $K_{vd3}=0{,}7$; свідоцтво про шлюб (A_6), $K_{vd6}=0{,}5$; трудова книжка (A_7), $K_{vd7}=0{,}5$. Сумарна величина коефіцієнтів важливості визначається за формулами (3),(4):

$$K_{vd}=\sum_{i=1}^{n}K_{vdn}\ ,n=\overrightarrow{1{,}5}\ ; \quad (3)$$

$$K_{vd}=K_{vd1}+K_{vd2}+K_{vd3}+K_{vd6}+K_{vd7}=3{,}4.$$

Нехай під загрозою знаходяться документи A_1 A_3 та A_6, тоді за формулою (3):

$$K_{vdr}=K_{vd1}+K_{vd3}+K_{vd6}=2{,}1.$$

Наступним кроком відбувається визначення середовища обробки ПД, що містяться у вказаних документах, відповідно до таблиці 3: Word (B_1), $K_{vp1}=0{,}3$; Excel (B_2), $K_{vp2}=0{,}4$; Access (B_3), $K_{vp3}=0{,}5$; «Працівники» (B_5), $K_{vp5}=0{,}7$; «1С» (B_7), $K_{vp7}=0{,}9$. Нехай ПД обробляються ПЗ B_2 та B_5. Аналогічно, за формулою (3), визначаються коефіцієнти K_v та K_{vr} для ПЗ обробки ПД. Таким чином, значення $K_{vp}=2{,}8$ та $K_{vpr}=1{,}1$. Визначення максимально можливого розрахункового значення ризику (R_{max}), знаходиться за відношенням суми коефіцієнтів важливості всіх об'єктів (документів та ПЗ), що знаходяться під загрозою, до сумарної величини коефіцієнтів важливості об'єктів та визначається за формулою:

$$R_{max} = \frac{K_{vdr} + K_{vpr}}{K_{vd} + K_{vp}} = \frac{2{,}1 + 1{,}1}{3{,}4 + 2{,}8} = 0{,}52. \quad (4)$$

Проте, для оцінки ризику захисту ПД, необхідно дослідити використані в АС механізми безпеки ПД, існуючі загрози захисту ПД та визначити відповідний їм рівень реалізації.

Етап 2. На даному етапі проводиться аналіз функціонуючих механізмів безпеки. Кожен із запропонованих механізмів безпеки в моделі забезпечує корегування визначеного максимально можливого розрахункового значення ризику на коефіцієнт 0,2. Нехай в АС наявні 3 механізми безпеки (D_i, i=1÷3), тоді сумарний коефіцієнт $K_m = 3 \times 0{,}2 = 0{,}6$.

Етап 3. Передбачається ідентифікація можливих загроз захисту ПД при обробці БПД в АС. Перелік цих загроз (F) визначається запропонованим методом аналізу і оцінки ризиків ПД в БПД. Згідно формули (1), якщо у всіх обраних загрозах було визначено «низький» рівень загрози, то $P_{riv\_zag} = 0{,}3$, якщо встановлено хоча б один «середній» рівень», то $P_{riv\_zag} = 0{,}6$ та хоча б один «високий» – $P_{riv\_zag} = 1$. Тоді розрахункове значення ризику з урахуванням рівня реалізації загроз корегується ($R_{zag_{corr}}$) і визначатиметься за формулою:

$$R_{zag_{corr}} = P_{riv\_zag} \times R_{max}. \quad (5)$$

Нехай, в прикладі визначено загрози з «низькими» та «середніми» рівнями, то відповідно $P_{riv\_zag} = 0{,}6$, тоді:

$$R_{zag_{corr}} = 0{,}6 \times 0{,}52 = 0{,}31. \quad (6)$$

Після розрахунку $R_{zag_{corr}}$, визначимо розрахунковий інтервал – в межах якого і знаходиться реальний ризик захисту ПД. Весь інтервал $I \in (I_{min}, I_{max})$ згідно таблиці 4 поділено на підінтервали [0÷0,1], [0,1÷0,3], [0,3÷0,6], [0,6÷0,8], [0,8÷1].

Етап 4. Визначення величини можливого збитку від витоку ПД (чи БПД в АС) може визначатися як кількісними, так і якісними показниками. Оскільки $R_{zag_{corr}}$= 0,31, то згідно до розробленого методу аналізу і оцінки ризиків ПД в БПД, а саме таблиці 4, наведено шкали показників величин можливих збитків: розрахунковий інтервал ризику можливого витоку ПД – [0,31÷0,6]; грошовий еквівалент ризику можливих збитків – (1000÷10000 $); бальна оцінка ризику втрати ПД – 3 бали.

Етап 5. Проводиться оцінка ризиків захисту ПД. На даному етапі визначається корекція ймовірності з врахуванням механізмів захисту (R_{C_corr}) за формулою:

$$R_{C\_corr} = \left(I_{min} + (I_{max} - I_{min}) \times (1 - K_m)\right). \quad (7)$$

У даному випадку R_{C_corr}, де $I \in (I_{min}, I_{max})$, $I \in (0{,}3 \div 0{,}6)$:

$$R_{C\_corr} = \left(0{,}31 + (0{,}6 - 0{,}31) \times (1 - 0{,}6)\right) = 0{,}426.$$

Даний інтервал витоку ПД визначається збитками в грошовому еквіваленті на рівні $G \in (G_{min}, G_{max})$, $G \in$ (1000 ÷ 10000 $). Таким чином ймовірні збитки в грошах, визначаються як:

$$Rg = G_{min} + (G_{max} - G_{min}) \times R_{C_{corr}}, \quad (8)$$

$$Rg = 1000 + (10000 - 1000) \times 0{,}426 = 4834\ \$.$$

Етап 6. Керування ризиком захисту ПД. Після проведення аналізу та оцінки ризиків ПД в БПД, можна сформувати кінцеві висновки про стан рівня захищеності ПД в конкретній АС. А отже, можна надати рекомендації щодо підвищення цього стану, а саме через впровадження тих чи інших механізмів безпеки, що запропоновані в таблиці 6. Оскільки було визначено ризик витоку ПД у 3 бали, то згідно до таблиці 6, в АС необхідно – використати ТЗІ/КЗІ (технічний та/або криптографічний ЗІ). Таким чином проведено оцінку ризиків захисту ПД у БПД в АС на конкретному прикладі.

Верифікація методу. Для проведення верифікації розробленого методу було обрано 2 випадки з наступними умовами:

1) ПД (A_i) обробляються ПЗ B_2 та B_5 при $K_{vd} = 3{,}4$; $K_{vp} = 2{,}8$; $K_{vpr} = 1{,}1$; $K_m = 0{,}6$; $P_{riv\_zag} = 0{,}6$, отримані результати приведені у таблиці 7.

2) ПД (A_i) обробляються ПЗ B_2, B_5, B_7 при $K_{vd} = 3{,}4$; $K_{vp} = 2{,}8$; $K_{vpr} = 1{,}1$; $K_m = 0{,}6$; $P_{riv\_zag} = 1$, отримані результати приведені у таблиці 8.

Таблиця 7

Документи	K_{vdr}	R_{max}	$R_{zag_{corr}}$	Інтервал	Бали	Грошовий еквівалент	R_{C_corr}	Rg
A_6	0,5	0,26	0,15	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
...	...	...	...	...	...	...	...	...
A_1	0,9	0,32	0,19	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
A_1, A_6	1,4	0,40	0,24	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
...	...	...	...	...	...	...	...	...
A_1, A_2	1,7	0,45	0,27	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
A_2, A_3, A_6	2	0,50	0,30	0,11 ÷ 0,3	2	100-1000$	0,186	267,4
...	...	...	...	...	...	...	...	...
A_1, A_2, A_3	2,4	0,56	0,34	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
A_2, A_3, A_6, A_7	2,5	0,58	0,35	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
...	...	...	...	...	...	...	...	...
A_1, A_2, A_3, A_6	2,9	0,65	0,39	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
...	...	...	...	...	...	...	...	...
A_1, A_2, A_3, A_6, A_7	3,4	0,73	0,44	0,31 ÷ 0,6	3	1000-10000$	0,426	4834

Таблиця 8

Документи	K_{vdr}	R_{max}	$R_{zag_{corr}}$	Інтервал	Бали	Грошовий еквівалент	R_{C_corr}	Rg
A_6	0,5	0,40	0,40	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
...	...	...	...	...	...	...	...	...
A_1	0,9	0,47	0,47	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
A_1, A_6	1,4	0,55	0,55	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
...	...	...	...	...	...	...	...	...
A_1, A_2	1,7	0,60	0,60	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
A_2, A_3, A_6	2	0,65	0,65	0,31 ÷ 0,6	3	1000-10000$	0,426	4834
...	...	...	...	...	...	...	...	...
A_1, A_2, A_3	2,4	0,71	0,71	0,61 ÷ 0,8	4	10000-100000$	0,686	71740
A_2, A_3, A_6, A_7	2,5	0,73	0,73	0,61 ÷ 0,8	4	10000-100000$	0,686	71740
...	...	...	...	...	...	...	...	...
A_1, A_2, A_3, A_6	2,9	0,79	0,79	0,61 ÷ 0,8	4	10000-100000$	0,686	71740
...	...	...	...	...	...	...	...	...
A_1, A_2, A_3, A_6, A_7	3,4	0,87	0,87	0,81 ÷ 1	5	100000-1000000$	0,426	897400

Висновки. У роботі розроблено базову модель та метод оцінки ризиків захисту персональних даних в АС, який оснований на положеннях міжнародного стандарту ISO/IEC 27005:2008 (Information technology – Security techniques – Information security risk management) у відповідності до вимог діючого законодавства України. Так як в державних АС інформація повинна оброблятися із застосуванням КСЗІ, то на етапі її впровадження, а саме при розробці політики безпеки необхідно провести оцінку ризиків загроз (наприклад, до ПД) через відсутність наразі встановленої методики, можна застосувати саме цей метод. Розроблений метод аналізу і оцінки ризиків захисту ПД в державних АС, який орієнтований на те, що власником системи є держава і в цих системах обробляється інформація з обмеженим доступом (насамперед, ПД), дає можливість визначити достатні заходи та способи (механізми) захисту для забезпечення необхідного рівня захищеності за допустимих затратах і заданому рівні обмежень видів інформаційної діяльності.

Окремо розроблений метод може бути додатковим заходом до комплексу існуючих щодо захисту державних інформаційних ресурсів або інформації з обмеженим доступом (насамперед ПД, що належать до конфіденційної інформації) під час її обробки в інформаційних системах при виконанні п. 2 рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки» від 28.04.2014 р. введеного Указом Президента України № 449/2014 від 1.05.2014 р.

ЛІТЕРАТУРА

[1]. Дрейс Ю.О. Аналіз стану захисту персональних даних в державних інформаційних системах / «Інтегровані інтелектуальні робототехнічні комплекси» (ІРТК-2014): Матеріали VII міжнародної науково-практичної конференції, 19-20 травня 2014 р. – К.: НАУ, 2014. – С.335-336.

[2]. Корченко О.Г. Державне регулювання у сфері забезпечення захисту персональних даних / О.Г. Корченко, Ю.О. Дрейс // «Актуальні про-

блеми забезпечення інформаційної безпеки держави»: Матеріали науково-технічної конференції студентів, аспірантів, викладачів та науковців, 18 грудня 2014 р. – Київ: ДУТ, 2014. – (132 с.) – С.27.

[3]. Про затвердження документів у сфері захисту персональних даних / Уповноважений ВР з прав людини; Наказ, Порядок, Форма типового документа [...] від 08.01.2014 р. №1/02-14 // [Електронний ресурс. – Режим доступу]: zakon2.rada.gov.ua/

[4]. Деякі практичні аспекти реалізації заходів захисту персональних даних під час їх обробки в інформаційних (автоматизованих) системах / О. Мервінський, М. Щербак / «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», сайт наук.-техн. зб. НТУУ «КПІ», Вип. – 25, 2013 // [Електронний ресурс. – Режим доступу]: pnzzi.kpi.ua/

[5]. Анализ и оценивание рисков информационной безопасности: монография / [Корченко А.Г., Архипов А.Е., Казмирчук С.В.]. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

[6]. Дрейс Ю.О. Базові параметри представлення ризику захисту персональних даних в державних АС / «Інформаційна безпека держави, суспільства та особистості»: Збірник тез доповідей всеукраїнської науково-практичної конференції, 16 квітня 2015 р., м. Кіровоград: КНТУ, 2015. – С.118.

[7]. Дрейс Ю.О. Модель аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах / «АВІА-2015» : Матеріали XII міжнародної науково-практичної конференції, 28-29 квітня 2015 р. – К.: НАУ, 2015. – С.15-16.

[8]. Підхід до аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах / Ю.О. Дрейс, А.О. Дейсан, Д.Ю. Бєляк / «68-ма науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів»: Матеріали конференції, 4-6 грудня 2013 р., Част. 3. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – С.117-120.

[9]. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія / [Корченко О.Г., Архипов О.Є., Дрейс Ю.О.]. –К.: Наук.-вид. центр НА СБ України, 2014. – 332 с. – ISBN 978-617-7092-26-0

[10]. Дрейс Ю.О. Заходи захисту персональних даних в інформаційних (автоматизованих) системах / «Перспективні напрями захисту інформації»: Матеріали І всеукраїнської науково-практичної конференції, 7-9 вересня 2015 р. – Одеса: ОНАЗ ім. О.С. Попова, 2015. – (124с.) – С.29-32.

[11]. Дрейс Ю.О. Програмна реалізація оцінювання ризиків захисту персональних даних в державних автоматизованих системах / «ITSEC»: Матеріали V міжнародної науково-технічної конференції, 19-22 травня 2015 р. – К.: НАУ, 2015. – (124с.). – С.31.

[12]. Комп'ютерна програма «Оцінювання ризиків захисту персональних даних в державних автоматизованих системах» / О.Г. Корченко, Ю.О. Дрейс, А.О. Дейсан, А.О. Корченко/ Державна служба інтелектуальної власності України: Свідоцтво про реєстрацію авторського права на твір №59269 від 15.04.2015.

REFERENCES

[1]. Dreis Y.A. Analysis of the state protecting personal data in the state information systems, «Integrated intellectual robot technical complexes (IIRTC-2014)»: Collection of articies 5-th International Scientific and Technical conf., 19-20 may 2014, Kiev, Ukraine – K.: NAU, 2014. – pp.335-336.

[2]. Korchenko A.G., Dreis Y.A. State regulation in the sphere of protecting personal data, «Actual problems ensuring of the state information security»: Materials of Scientific and Technical conf. of students, graduates, teachers and academics, 18 dec. 2014, Kiev, Ukraine – K.: SUT, 2014. – pp.27.

[3]. On approving documents for the personal data protection / Ombudsman for Human Rights; Order, order, typical form of [...] on 01.08.2014 p., №1/02-14, [electronic resource. - Access]: zakon2.rada.gov.ua/

[4]. Mervinskyy A., Shcherbak M. Some practical aspects of realization of measures for the protection personal data when their processing in information (automated) systems, Legal, normative and metrological support system of information protection in Ukraine, Vol. 25, 2013, [electronic resource. - Access]: pnzzi.kpi.ua/

[5]. Korchenko A.G., Arkhipov A.E., Kazmirchuk S.V. Analysis and assessment of information security risks, Monograph., K.: LLC «Lazurit -Polygraph», 2013, 275 p.

[6]. Dreis Y.A. The base parameters of represent a risk for personal data protection in the state automated systems, «Information security of the state, society and personality»: Materials of Ukrainian Scientific and Technical conf., 16 april 2015, Kirovograd, Ukraine – Kirovograd: KNTU, 2015. – pp.118.

[7]. Dreis Y.A. The model of analysis and assessment risks to protecting personal data in the state automated systems. «AVIA-2015»: Materials of 12-th International Scientific and Technical conf., 19-20 april 2015, Kiev, Ukraine – K.: NAU, 2015. – pp.15-16.

[8]. Dreis Y.A., Deisan A.A., Belyak D.Y. The approach to analysis and risk assessment of protection personal data in the state automated systems, Materials of 68-th Scientific and Technical conf. of the teaching staff, researchers and students, 4-6 dec. 2013, Odessa, Ukraine. – Odessa: ONAC, 2013. – Part 3. – pp.117-120.

[9]. Korchenko A.G., Arkhipov A.E., Dreis Y.A. Assessment harm to the Ukraine national security in case of leakage state secrets, Monograph., K.: Scientific Publishing Center of NA SSS Ukraine, 2014, 332 p. – ISBN 978-617-7092-26-0

[10]. Dreis Y.A. The measures of protection for personal data in information (automated) systems, «Perspective directions of information protection»: Materials of Ukrainian Scientific and Technical conf., 4-6 sep. 2015, Odessa, Ukraine. – Odessa: ONAC, 2015. – pp. 29-32.

[11]. Dreis Y.A. Program realization of risk assessment for personal data protection in the state automated systems, «ITSEC»: Materials of 5-th International Scientific and Technical conf., 19-22 may 2015, Kiev, Ukraine – K.: NAU, 2015. – pp. 31.

[12]. Computer program «Risk assessment for personal data protection in the state automated systems», Korchenko A.G., Dreis Y.A., Deisan A.A., Korchenko A.A., State Intellectual Property Service of Ukraine, Cvidotstvo of registration copyright №59269, 15.04.2015.

МОДЕЛЬ И МЕТОД ОЦЕНКИ РИСКОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Рассматривается вопрос о необходимости защиты персональных данных, которые создаются и обрабатываются прикладным программным обеспечением в автоматизированных системах. Анализ существующего законодательства указывает на обязательность защиты государственных информационных ресурсов или информации с ограниченным доступом, требование относительно защиты которой определена законом. Так как персональные данные могут быть отнесены к конфиденциальной информации о лице, то они нуждаются в защите на уровне применения комплексной системы защиты информации. Ее внедрение предусматривает проведение оценки рисков угроз на этапе разработки политики безопасности в части определения необходимых мер и средств защиты информации. Предложено базовую модель представления параметров риска, которые определены на установленных законодательством условиях в сфере обеспечения защиты персональных данных. Разработан метод оценки рисков по результатам которого даются рекомендации по выбору политики защиты персональных данных, дополнения стандартного функционального профиля защищенности необходимыми услугами безопасности, определения величины нанесенного ущерба человеку, обществу, государству в случае потери таких персональных данных.

Ключевые слова: персональные данные, оценка рисков, политика защиты персональных данных, оценка ущерба в случае потери персональных данных.

MODEL AND METHOD OF ASSESSMENT RISKS PROTECTION OF PERSONAL DATA DURING THEIR PROCESSING AT THE AUTOMATED SYSTEM

The question of the need to protect personal data created and processed by application software in automated systems. Analysis of the existing legislation indicates mandatory protection of state information resources or classified information, protection of which is defined by law. Since personal data can be attributed to confidential information about a person, they need protection at the application of the integrated system of information security. Its implementation involves a risk assessment of threats during the development of security policy in the definition of necessary measures and information security. A basic model presenting risk parameters defined criteria in the legislation in the field of personal data protection. The method of risk assessment which resulted in recommendations for selecting the policy of personal data protection, addition of standard functional profile protection security services as required, determination of the damage caused to a person, society and state in case of loss this personal data.

Index Terms: personal data, risk assessment, policy for personal data protection, assessment of damages in case of loss personal data.

Корченко Олександр Григорович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua

Корченко Александр Григорьевич, доктор технических наук, профессор, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.

Korchenko Alexander, Professor, Doctor of Science in Eng., Head of IT-Security Academic Department, National Aviation University (Kyiv, Ukraine).

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри дистанційного навчання Національного авіаційного університету.
E-mail: y.dreis@nau.edu.ua

Дрейс Юрий Александрович, кандидат технических наук, доцент, заведующий кафедрой дистанционного обучения Национального авиационного университета.

Dreis Yurii, PhD in Eng., Associate Professor, Head of Distance e-Learning Academic Department, National Aviation University (Kyiv, Ukraine).

Лозова Ірина Леонідівна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: kira1983@yandex.ru

Лозовая Ирина Леонидовна, старший преподаватель кафедры безопасности информационных технологий Национального авиационного университета.

Lozova Iryna, Senior lector of IT-Security Academic Department, National Aviation University (Kyiv, Ukraine)