Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

Перша всеукраїнська науково-практична конференція

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

07 вересня 2015 року

Збірник тез

Одеса
ОНАЗ
2015

Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

Перша всеукраїнська науково-практична конференція

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

07 вересня 2015 року

Збірник тез

Одеса
ОНАЗ
2015

УДК 004.056.5

Перспективні напрями захисту інформації: матеріали першої всеукраїнської наук.-пр. конф. м. Одеса 7 – 9 вересня 2015 р. – Одеса: ОНАЗ, 2015. – 124 с.

Даний збірник містить тези матеріалів, що представлені на першу всеукраїнську науково-практичну конференцію "**Перспективні напрями захисту інформації**", що проводиться 7 – 9 вересня 2015 р. в Одеській національній академії зв'язку ім. О.С. Попова.

У збірник включені тези доповідей за такими напрямками:

- організаційно-правові методи захисту інформації;
- системи квантової криптографії;
- технічні засоби виявлення каналів витоку інформації;
- засоби захисту інформації в інформаційних і телекомунікаційних системах;
- елементи і компоненти для систем захисту інформації;
- методи та засоби захисту господарських об'єктів.

Робочі мови конференції – українська, російська, англійська.

© ОНАЗ ім. О.С. Попова, 2015

ЗМІСТ

Литература

1. Твердохліб М. Чому окупанти України боялися мови її народу? [Електронний ресурс] // URL:http://www.pravda.com.ua/columns/2010/10/20/5494003/ (дата звернення: 17.05.15).
2. Мейс, Джеймс. Геноцид — найтяжчий злочин проти людства і людяності. / Д. Мейс // Українська мова та література. — 2006. — № 3-4. — С. 3-6.
3. Шаповал Юрій Іванович. У ті трагічні роки: Сталінізм на Україні / Інститут політичних досліджень. — К. : Політвидав України, 1990. — 142с.
4. Кульчицький С. В. Демографічні наслідки голодомору 1933 р. в Україні / С. В. Кульчицький. – К. : Ін-т історії України, НАН України, 2003. – 192с.
5. Волкогонов Д. А. Тріумф і трагедія: політичний портрет Й. В. Сталіна: у 2 кн. — К.: Політвидав України, 1989. — Кн. 1. — 597 с.

УДК 004.056.5

Дрейс Ю.О. к.т.н., доц..
Житомирський військовий інститут імені С.П. Корольова
DreisYuri@gmail.com

ЗАХОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

Анотація. *Проведено аналіз основних і додаткових заходів захисту персональних даних під час їх обробки в інформаційних (автоматизованих) системах з метою попередження й нейтралізації потенційних і реальних загроз (від випадкової втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до цих персональних даних).*

У відповідності до вимог статті 7 розділу 2 "Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних" [1], статті 24 Закону України "Про захист персональних даних" [2], рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" [3] уведеного в дію Указом Президента України № 449/2014 від 1 травня 2014 року під час автоматизованої обробки персональних даних повинні вживатися *відповідні заходи* безпеки, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій утраті, несанкціонованому доступу, зміні або поширенню [1, 2], а також *додаткові заходи* щодо захисту інформації з обмеженим доступом (ІзОД) (насамперед тих персональних даних, що належать до конфіденційної інформації) з метою попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері [3].

Персональні дані (ПД) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2]. До ПД відносяться [4] відомості про: расове, етнічне та національне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості; стан здоров'я; статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності; застосування щодо особи заходів в рамках досудового розслідування; вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»; вчинення щодо особи тих чи інших видів насильства; місцеперебування та/або шляхи пересування особи.

Відповідні (або основні) заходи безпеки [3] застосовуються згідно до вимог чинного законодавства України у сфері захисту ПД суб'єктами відносин, пов'язаних із ПД, тобто

суб'єктом ПД; володільцем ПД; розпорядником ПД; третьою особою; Уповноваженим Верховною Радою України з прав людини (далі – Уповноважений). Володілець, розпорядник ПД вживають заходів щодо забезпечення захисту ПД на всіх етапах їх обробки, у тому числі за допомогою *організаційних* та *технічних заходів*. Так, наприклад, в органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках ПД, що здійснюють обробку ПД, яка підлягає повідомленню, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом ПД при їх обробці, а саме [2]: 1) інформує та консультує володільця або розпорядника ПД з питань додержання законодавства про захист ПД; 2) взаємодіє з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист ПД. З метою виконання вказаних завдань відповідальна особа/структурний підрозділ: забезпечує реалізацію прав суб'єктів ПД; користується доступом до будь-яких даних, які обробляються володільцем/розпорядником та до всіх приміщень володільця/розпорядника, де здійснюється така обробка; у разі виявлення порушень законодавства про захист ПД [2] та/або Порядку [4] повідомляє про це керівника володільця/розпорядника з метою вжиття необхідних заходів; аналізує загрози безпеці ПД.

Також *організаційні* заходи охоплюють [4]: визначення порядку доступу до ПД працівників володільця або/та розпорядника; визначення порядку ведення обліку операцій, пов'язаних з обробкою ПД суб'єкта та доступом до них; розробку плану дій на випадок несанкціонованого доступу до ПД, пошкодження технічного обладнання, виникнення *надзвичайних ситуацій*; *регулярне навчання співробітників, які працюють з ПД*.

Слід відмітити, що ***до обробки ПД*** відноситься [3] будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення ПД, у тому числі з використанням інформаційних (автоматизованих) систем.

Зокрема, під ***інформаційною (автоматизованою) системою*** (ІС/АС) розуміється [5] організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

До окремих *технічних* заходів відносяться [6]: застосування АС мережевого захисту від несанкціонованого доступу під час обробки ПД; впровадження процедур авторизації працівників; забезпечення антивірусного захисту; використання технічних заходів безперебійного живлення елементів АС, яка здійснює обробку ПД; ведення журналу реєстрації подій та інші заходи. Наприклад, до засобів мережевого захисту відносять [6]: міжмережеві екрани, системи виявлення вторгнень (втручань); засоби створення віртуальних приватних мереж; засоби аналізу захищеності тощо.

Володілець, розпорядник ПД самостійно визначають перелік і склад цих заходів, спрямованих на безпеку обробки ПД, з урахуванням вимог законодавства у сферах захисту ПД, інформаційної безпеки, а також інших чинників таких як: можливий рівень ризику, пов'язаний з обробкою ПД [7-10]; природа та обсяги ПД, що обробляються в АС; вартість робіт, щодо впровадження заходів та засобів захисту ПД (наприклад, у цілому щодо комплексної системи захисту інформації (КСЗІ) або щодо комплексу засобів захисту (КЗЗ) чи окремих засобів технічного/криптографічного захисту інформації (ТЗІ/КЗІ)); оцінка можливої шкоди у разі витоку ПД та наслідки щодо можливої за це відповідальності й відшкодування збитків.

Натомість, фізичні особи - підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист ПД дотримуючись вимог законодавства. Окремо, дозволяється обробка ПД без застосування відповідних заходів безпеки [2], якщо така обробка здійснюється фізичною особою виключно для особистих чи побутових потреб або виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів.

Додаткові заходи вживаються коли ПД відносяться до ІзОД або становлять державні інформаційні ресурси (ДІР). Відомо [11], що розголошення інформації, яка становить державну таємницю, або іншої ІзОД, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави є загрозою національним інтересам і національній безпеці України. У такому випадку такі ПД, що є ІзОД (чи ДІР) повинні оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю за результатами державної експертизи в порядку, встановленому законодавством. Для створення комплексної системи захисту ДІР або ІзОД використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ та/або КЗІ [5].

Комплексною системою захисту інформації (КСЗІ) є взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [5]. Відомо, що базовим етапом побудови КСЗІ є створення політики безпеки, методологія якої включає: розробку концепції інформаційної безпеки в ІС, аналіз ризиків; визначення вимог до заходів, методів та засобів захисту; вибір основних рішень для забезпечення інформаційної безпеки; організацію виконання відновлювальних робіт і забезпечення безперебійного функціонування ІС; оформлення політики безпеки. Для аналізу ризиків необхідно [7-10]: визначити базові складові ІС та скласти реєстр ресурсів, що циркулюють і враховуються при аналізі; ідентифікувати загрози об'єктам захисту; оцінити ризики та величину можливих збитків пов'язаних з реалізацією загроз; визначити варіанти і витрати на побудову КСЗІ. Тому, аналіз і оцінка ризиків захисту ПД при розробці КСЗІ для державних ІС, де циркулює КІ (така як ПД), що обробляється у базах ПД (БПД) в інтересах визначених законодавством є *актуальним науковим завданням*.

Висновок. Наразі застосування відповідних (основних) чи додаткових заходів захисту ПД залежать конкретно до якої інформації вони відносяться: якщо до відкритої, то володілець, розпорядник ПД самостійно визначає перелік та склад необхідних заходів захисту, але не менше ніж їх визначено законодавством; якщо ж до ДІР чи ІзОД, вимога щодо захисту якої визначена законодавством, то відповідно – КСЗІ.

Література

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних / Рада Європи; Конвенція, Міжнародний документ від 28.01.1981 // [Режим доступу]: http://zakon2.rada.gov.ua/laws/show/994_326
2. Про захист персональних даних / Верховна Рада України; Закон №2297-VI від 01.06.2010 // [Режим доступу]: http://zakon2.rada.gov.ua/laws/show/2297-17/page2
3. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки [...] РНБО; Рішення від 28.04.2014// [Режим доступу]: http://zakon4.rada.gov.ua/laws/show/n0004525-14
4. Про затвердження документів у сфері захисту персональних даних / Уповноважений ВР з прав людини; Наказ, Порядок, Форма типовогодокумента [...] від 08.01.2014 № 1/02-14 // [Режим доступу]: http://zakon4.rada.gov.ua/laws/show/v1_02715-14
5. Про захист інформації в інформаційно-телекомунікаційних системах / Верховна Рада України; Закон від 05.07.1994 № 80/94-ВР // [Режим доступу]: http://zakon4.rada.gov.ua/laws/show/80/94-вр
6. Мервінський О. 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 науково-технічного збірника НТУУ «КПІ», Випуск – 25, 2013 // [Електронний ресурс. – Режим доступу]: http://pnzzi.kpi.ua/25/25_p33.pdf
7. Підхід до аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах / Ю.О. Дрейс, А.О. Дейсан, Д.Ю. Бєляк / 68-ма наук.-техн. конф.

професорсько-викладацького складу, науковців, аспір. та студ.: Матеріали конф., 4-6.12.2013 р., Част.3. – Одеса.: ОНАЗ ім. О.С. Попова, 2013. – С.117-120.

8. Дрейс Ю.О. Базові параметри представлення ризику захисту персональних даних в державних АС / «Інформаційна безпека держави, суспільства та особистості»: Збірник тез доповідей Всеукр. наук.-практ. конф., 16 квітня 2015 р., м.Кіровоград. – КНТУ, 2015. – С.118.

9. Дрейс Ю.О. Модель аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах / «ABIA-2015»: Матеріали XII Міжнародної наук.-практ. конф., 28-29 квітня 2015 р., м.Київ. – К.: НАУ, 2015. – С.15-16.

10. Дрейс Ю.О. Програмна реалізація оцінювання ризиків захисту персональних даних в державних автоматизованих системах / «ITSEC-2015»: Матеріали V Міжнародної наук.-техн. конф., 19-22 травня 2015 р., м.Київ.– К.: НАУ, 2015. – С.68.

11. Про основи національної безпеки України / Верховна Рада України; Закон від 19.06.2003 № 964-IV // [Режим доступу]: http://zakon4.rada.gov.ua/laws/show/964-15

УДК 004.056.5: 534.78: 621.391.883

Касьянов Ю.І.
Національний університет кораблебудування імені адмірала Макарова.
yukas@mail.ru

УРАХУВАННЯ ПРОФЕСІЙНО-СЛЕНГОВОЇ ПІДГОТОВКИ ЗЛОВМИСНИКА В ОЦІНЦІ ЗАХИЩЕНОСТІ МОВНОЇ ІНФОРМАЦІЇ

Анотація. *Сформульовано задачу урахування професійно-сленгової підготовки зловмисника в оцінці захищеності мовної інформації за критерієм розбірливості мови. Визначено основні параметри та порядок проведення експерименту для оцінки впливу професійно-сленгової підготовки на розбірливість мовного повідомлення.*

Захист мовної інформації досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів. Використання тих або інших методів і засобів визначається характеристиками об'єкта захисту, можливостями зловмисника, а також вимогами, що висуваються до захищеності мовної інформації. Важливою задачею при цьому є об'єктивна оцінка ефективності цих заходів та ступеня захищеності, яка проводиться при атестаційних випробуваннях та в процесі оперативного контролю.

Наразі загальноприйнятим критерієм захищеності мовної інформації є відповідність нормам відношення сигнал/шум, виміряного в контрольних точках можливого знімання інформації [1, 2]. Однак, останнім часом набуває широкого вжитку критерій розбірливості мови, який дозволяє враховувати особливості мовного сигналу і більш точно відобразити сприйняття смислової складової мовного повідомлення й ефективність прийнятих заходів захисту мовної інформації існуючим загрозам.

Даний критерій вже давно використовується для оцінки якості каналів мовного зв'язку та акустики приміщень і нормований рядом стандартів - ГОСТ 16600-72, ГОСТ Р 50840-95, ГОСТ 25902-83, ГОСТ Р 51061-97, ANSI S3.5-1997, ISO/TR 4870:1991 тощо. При цьому використовуються різні суб'єктивні та об'єктивні методи визначення розбірливості мови [3, 4]. Але, при використанні цих методів в задачах оцінювання захищеності мовної інформації, слід враховувати, що якість каналу зв'язку та захищеність інформації залежать від розбірливості мови прямо протилежно, а рівні мовного сигналу в точці прийому в даному випадку будуть сумірними або нижчими рівня фонових шумів.

Для оцінювання захищеності мовної інформації від витоку акустичним каналом наразі практично використовуються лише методи, основані на формантній теорії мови, що володіють високою точністю і оперативністю. На базі цього підходу та результатів досліджень Н.Б. Покровського [3] створено методику оцінки захищеності мовної інформації [5, 6], яка рекомендована Держтехкомісією Росії до використання. За критерій в

Підписано до друку 02.09.2015 р.
Формат 60/88/16. Обсяг 7,75 друк. арк.
Тираж 60 прим. Зам. № 5679.
Віддруковано у редакційно-видавничому центрі ОНАЗ ім. О.С. Попова
м. Одеса, вул. Ковалевського, 5
тел. 70-50-494
© **ОНАЗ, 2015**