УДК 65.012.8+34

АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО ЗАХИСТУ ВІДКРИТОЇ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЇ ПРО ОСОБУ

Віталій Носов, Олександр Манжай
Харківський національний університет внутрішніх справ

Анотація: **Досліджуються актуальні питання законодавчого закріплення в Україні захисту відкритої інформації та інформації про особу.**
Summary: **The actual questions of the legislative fixing in Ukraine of protection of opened information and information about a person are explored.**
Ключові слова: **Відкрита інформація, конфіденційна інформація, інформація про особу.**

I Вступ

Інформація в сучасному світі є однією з найважливіших складових суспільного життя. В сучасному світі як ніколи актуальною стає теза: «Хто володіє інформацією – володіє світом». На початку XXI століття об'єми інформації в суспільстві досягли великих обсягів. В той же час з розвитком інформаційних відносин почали активно розвиватися негативні прояви, спрямовані на знищення, перекручення, модифікацію і т. ін., інформації, що циркулює в певній системі. З метою протидії цим негативним проявам на рівні держави проводиться відповідна політика з забезпечення безпеки державних інформаційних ресурсів.

Захист інформації є складовою частиною забезпечення національної безпеки України. Організація захисту інформації забезпечується правовими, організаційними і інженерно-технічними заходами. Правові заходи захисту інформації є базисом, на який спираються організаційні і інженерно-технічні заходи. Існуюча нормативно-правова база в галузі захисту інформації для збереження відповідності реальним суспільним процесам постійно потребує вдосконалення.

В статті розглядаються неврегульовані законодавством України питання правового захисту відкритої інформації та інформації про особу і пропонуються відповідні зміни до законодавства України.

II Деякі питання правових заходів захисту інформації

В результаті детального вивчення деяких нормативних актів, зокрема закону України «Про інформацію» (далі Закону), можна дійти висновку про недостатнє врегулювання цього питання. Хоча цей закон є базовим регулятором інформаційних відносин в Україні – після Конституції та ратифікованих Верховною Радою України міжнародних договорів.

Серед властивостей інформації, які їй притаманні в розрізі захисту, можна виділити наступні:

- цілісність (або достовірність);
- доступність;
- конфіденційність.

Цілісність інформації полягає в тому, що інформація повинна відповідати певним якісним показникам, зокрема таким, як достовірність і вміщувати в собі той сенс, який заклав у неї її власник. Цілісність передбачає незмінність інформації в будь-який проміжок часу від моменту їх породження. Інформація зберігає цілісність, якщо дотримується встановлена режимна адекватність (відповідне виконання правил доступу) щодо її модифікації (видалення).

Доступність інформації зумовлена нормальною взаємодією між її носієм та одержувачем, тобто доступність розуміється як можливість користування інформацією в довільний проміжок часу. Інформація зберігає доступність, якщо не втрачається комунікабельність носія або одержувача інформації при їх взаємодії. Комунікабельність в даному разі означає здатність до взаємодії з метою передачі чи отримання інформації.

Конфіденційність інформації визначається встановленням відповідного режиму доступу до неї. Конфіденційність розуміється як недоступність інформації для користувачів, яким апріорно не задана можливість її використання. Інформація зберігає конфіденційність, якщо дотримується режимна адекватність при ознайомленні з нею.

Виходячи з означених властивостей інформації виділяють відповідні загрози: цілісності, доступності, конфіденційності. Такий підхід до визначення загроз інформації дозволяє більш чітко окреслити напрямки її захисту.

Ст. 5 Закону визначає основні принципи інформаційних відносин, якими є:

- гарантованість права на інформацію;
- відкритість, доступність інформації та свобода її обміну;
- об'єктивність, вірогідність інформації;
- повнота і точність інформації;
- законність одержання, використання, поширення та зберігання інформації.

Основні принципи, які відображені в цій нормі, прямо чи опосередковано вміщують в собі вищезгадані властивості інформації.

Відповідно до ч. 2 ст. 28 Закону за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Остання в свою чергу поділяється на конфіденційну та таємну, тобто таку, що вміщує державну таємницю (ст. 30 Закону).

Ч. 5 ст. 31 Закону встановлює, що громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Вищезгадана інформація підпадає під термін конфіденційна інформація, що окреслений у ч. 2 тієї ж статті: конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Для таємної інформації передбачений окремий механізм її обігу та захисту, окреслений в законі України «Про державну таємницю».

Таким чином, Законом передбачений захист інформації з обмеженим доступом. Проте нічого не сказано про захист відкритої інформації від загроз її цілісності та доступності.

Наведемо приклад. У м. Ф сталася техногенна аварія, про це надійшло повідомлення до засобу масової інформації (ЗМІ) К., який повинен оприлюднити інформацію за допомогою радіо чи телевізійного мовлення з використанням відповідної радіопередавальної станції. Зловмисник пошкодив антенну систему станції, тим самим реалізувавши загрозу доступності інформації про аварію. Багато людей не змогли вчасно евакуюватися, як наслідок сталося лихо державного масштабу. Або зловмисник перехопив повідомлення, що повинно було надійти до ЗМІ К., та замінив в ньому місце, де сталася аварія. Таким чином успішно реалізована загроза цілісності інформації. Наслідки очевидні.

З наведеного вище бачимо, що відкрита інформація, насамперед державна, потребує захисту від загроз її цілісності та доступності. Вимоги щодо захисту відкритої інформації містяться в деяких підзаконних актах. Зокрема, захист відкритої інформації в державних органах регламентують:

и) концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету міністрів України № 112 6 від 8 жовтня 1997 р.;

к) правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету міністрів України № 373 від 29 березня 2006 р. (далі Правила).

Згідно з Концепцією технічного захисту інформації в Україні одним з принципів формування і проведення державної політики в сфері технічного захисту інформації (ТЗІ) є обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також **відкритої інформації, важливої для особи та суспільства**, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях.

Віднесення тієї чи іншої інформації до категорії відкритої проводиться згідно з законом «Про інформацію» та Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

До відкритої інформації, що підлягає захисту, відносять статистичну, правову, соціологічну інформацію, інформацію довідково-енциклопедичного характеру, яка використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформацію про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (п. 4 Правил).

Взагалі під захистом інформації будемо розуміти сукупність організаційно-технічних заходів і

правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованим системам та особам, які користуються інформацією.

Між Концепцією технічного захисту інформації та Правилами є певна неузгодженість, оскільки перша наголошує на необхідності захисту відкритої інформації**, важливої для особи та суспільства.** Правила ж зобов'язують захищати **всю відкриту інформацію**, що є важко виконуваним на практиці і, відповідно, економічно недоцільним. Постає питання – чи є доцільним обов'язковість захисту відкритої інформації**,** важливої для особи та суспільства, та за яким критерієм відносити відкриту інформацію до цієї категорії? На нашу думку є два можливих підходи.

1. Законом України "Про державну таємницю" визначено порядок віднесення інформації до державної таємниці, який визначається як "процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України в разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього".

   - За аналогією з цим порядком, шляхом прийняття відповідного нормативного акту, можна створити інститут державних експертів з питань визначення відкритої інформації, важливої для особи та суспільства. На цих експертів покладалося б:

   – визначення підстав та доцільність віднесення відкритої інформації до "важливої для особи та суспільства" із зазначенням категорій державних установ, в яких вона циркулює (це важливо);

   – надання обґрунтованого висновку щодо шкоди національній безпеці України у разі порушення цілісності та доступності конкретної інформації;

   – складання зводу та розгорнутих переліків відомостей, що становлять відкриту інформацію**,** важливу для особи та суспільства.

   Наявність зводу та розгорнутих переліків відомостей, що становлять відкриту інформацію, важливу для особи та суспільства, повністю зняло б проблему невизначеності цієї категорії інформації, і відповідно, на практиці зрушився б процес захисту цієї інформації.
2. Альтернативний підхід полягає в можливій децентралізації процесу визначення та віднесення інформації до категорії "важлива для особи та суспільства". Необхідно нормативно закріпити перелік категорій державних установ, в яких потрібно проводити експертну оцінку наявності відкритої інформації**,** важливої для особи та суспільства. Оприлюднити методики та критерії такого оцінювання. І далі, конкретна державна установа організує цю експертизу силами свого підрозділу ТЗІ (якщо він існує), чи залучає організації, які мають відповідну ліцензію на проведення такої експертизи.

   - Суть такої експертизи полягає в оцінці ризиків (ймовірність реалізації інформаційних загроз та можливі збитки від цього) для інформаційної системи. Один з можливих методів оцінки ризиків для інформаційної системи організації було викладено в [2].

Ще одним важливим питанням захисту інформації є захист інформації про особу. Адже залишається невизначеним, яка інформація про особу є відкритою, а яка конфіденційною.

"Інформація про особу" є одним з найменш урегульованих понять в українському законодавстві. На відміну від України більшістю європейських країн були ухвалені спеціальні закони про захист персональної інформації: Австрія (1978 р.), ФРН (1977 р.), Великобританія (1984 р.), Франція (1987 р.), Норвегія (1988 р.), Португалія (1991 р.), Бельгія (1992 р.), Іспанія (1993 р.) та ін.

Радою Європи прийнято Конвенцію про захист особи у зв'язку з автоматизованою обробкою персональних даних (1981 р.), 15 директив та рекомендацій у галузі захисту даних, у тому числі про захист персональних даних у приватному (1973 р.) та державному (1974 р.) секторах; даних, що використовуються у медичних цілях (1981 р.), наукових дослідженнях та статистиці (1983 р.), прямому маркетингу (1985 р.), соціальному забезпеченні (1986 р.), правоохоронній сфері (1987 р.), даних у галузях зайнятості (1981 р.), платежів (1990 р.) тощо. Нормативні акти та рекомендації в указаній сфері прийняті також Європейським Союзом (95/46/CE), Організацією економічного співробітництва та розвитку [3, с. 29].

Зараз в Україні існує проект Закону «Про захист персональних даних», проте він є недосконалим, у зв'язку з чим був відхилений Президентом та направлений до Верховної ради України для доопрацювання.

Одним з пунктів пропозицій Президента щодо доопрацювання Закону про необхідність поділу персональних даних на *загальні персональні дані*, під якими розуміються прізвище, ім'я, по батькові, громадянство, місце проживання особи, та на *вразливі персональні дані*, до яких належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Такий поділ є

необхідним для встановлення спеціального режиму захисту вразливих персональних даних.

Спираючись на діюче законодавство України можна стверджувати наступне.

1. Відповідно до ст. 32 Закону України «Про інформацію» від 02. 10. 1992 р. інформація про особу – це сукупність документованих або публічно оголошених відомостей про особу. Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.
2. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.
   - Інформацію про особу можна поділити на:
   - **загальну**, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до п. 3 ст. 296 ЦК допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звіти, стенограми, протоколи, аудіо-, відеозаписи, архівні матеріали тощо).
   - **вразливі персональні дані (конфіденційна інформація про особу)**, що є інформацією з обмеженим доступом. Саме про такі дані йдеться в ст. 32 Конституції України від 28. 06. 1996 р., та в ст. 302 ЦК: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних відносяться, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К. Г. Устименка) від 30 жовтня 1997 року до конфіденційної інформації про особу, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).
3. Відповідно до ст. 38 Закону України «Про інформацію» від 02. 10. 1992 р. інформація, створена на кошти державного бюджету, є державною власністю.

   - Згідно з Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затвердженою Постановою Кабінету міністрів України від 27 листопада 1998 р. № 1893 орієнтовні критерії віднесення інформації до конфіденційної наступні.

   - *Інформація, що включається до переліків відомостей, які містять конфіденційну інформацію, що є власністю держави, повинна відповідати таким вимогам:*

   а) створюватися за кошти державного бюджету або перебувати у володінні, користуванні чи розпорядженні організації;

   б) використовуватися з метою забезпечення національних інтересів держави;

   в) не належати до державної таємниці;

   г) внаслідок розголошення такої інформації можливе:
   - *порушення конституційних прав і свобод людини та громадянина;*
   - *настання негативних наслідків у внутрішньополітичній, зовнішньополітичній, економічній, військовій, соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону;*
   - *створення перешкод у роботі державних органів.*

Водночас у п. 18 цієї ж Інструкції зазначається, що оброблення, зберігання, а також друкування документів з грифом "Для службового користування" та конфіденційної інформації, що є власністю держави, з використанням автоматизованих систем (АС) дозволяється тільки за наявності виданого в установленому порядку Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ атестата відповідності комплексної системи захисту інформації в цій АС вимогам щодо захисту інформації.

Виходячи з того, що інформаційне наповнення більшості державних органів зроблено за державний кошт, а також те, що частина цієї інформації про особу відповідає критеріям конфіденційності, можна стверджувати, що ця частина інформації є такою, яка належить до «конфіденційної інформації, що є

власністю держави»[1].

4. П. 4 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету міністрів України від 29 березня 2006 р. № 373 встановлює, що захисту в системі підлягає:
   - відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;
   - конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;
   - інформація, що становить державну або іншу передбачену законом таємницю.

Виходячи з викладеного, відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету міністрів України від 29 березня 2006 р. № 373, та інших нормативних актів в сфері захисту інформації встановлено:

загальна інформація про особу, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані -** як конфіденційна інформація, що є власністю держави відповідно до вимог чинного законодавства.

III Пропозиції щодо внесення змін до законодавства України

Відповідно до вищенаведеного пропонується внести наступні зміни до Закону України «Про інформацію» від 02. 10. 1992 р.

1. Ст. 10 Закону після абзацу сьомого доповнити новим абзацом такого змісту:

- «захистом інформації, яка є власністю держави, від загроз основним принципам інформаційних відносин»;

2. Доповнити Закон статтею 28^1 такого змісту:

- Стаття 28^1. Захист інформації

- Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованим системам та осіб, які користуються інформацією.»

3. Ст. 29 Закону після абзацу сьомого доповнити новим абзацом такого змісту:

- «Громадяни, юридичні особи, які володіють відкритою інформацією, встановлюють для неї систему (способи) захисту від загроз основним принципам інформаційних відносин».

Окрім вищеокреслених змін необхідною є зміна Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету міністрів України від 29 березня 2006 р. № 373. Зокрема, п. 4 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету міністрів України від 29 березня 2006 р. № 37, необхідно викласти в такій редакції:

Захисту в системі підлягає:

відкрита інформація, важлива для особи та суспільства, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

[1] Слід зазначити, що відповідно до п. 1 Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затвердженою Постановою Кабінету міністрів України від 27 листопада 1998 р № 1893 "Переліки відомостей, які містять конфіденційну інформацію, що є власністю держави, і яким надається гриф обмеження доступу "Для службового користування", розробляються експертними комісіями згідно з орієнтовними критеріями віднесення інформації до конфіденційної і затверджуються міністерствами, іншими центральними органами виконавчої влади, Радою міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими держадміністраціями, в яких утворюються або у володінні, користуванні чи розпорядженні яких перебувають ці відомості.

конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі – конфіденційна інформація);

інформація, що становить державну або іншу передбачену законом таємницю (далі – таємна інформація).

Важливість відкритої інформації визначається шляхом оцінки відповідних ризиків. Порядок та методика оцінки ризиків визначаються Державною службою спеціального зв'язку та захисту інформації України.

IV Висновки

Ширше бачення проблеми захисту інформації дозволяє більш активно та ефективно вирішувати її, перш за все, на концептуальному рівні. Держава повинна йти в ногу з розвитком сучасної науки. Саме внесення перспективних змін до законодавства України допоможе більш чітко визначитися з загальною концепцією побудови системи захисту інформації в державі, що в свою чергу сприятиме не тільки декларуванню необхідності вирішення проблеми захисту інформації, але й розв'язанню її по суті, що стає актуальним в умовах розвитку кібертероризму.

*Література: **1**. Общая парадигма защиты информации / П. И. Орлов, И. А. Громыко, В. В. Носов и др. // Защита информации. Конфидент. - 2003. - № 1(49).-С. 14 – 17. **2**. Носов В. В., Манжай А. В. Метод проектирования оптимальной системы защиты информации. // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", Київ, 2004, вип. 9, с. 94 – 102 **3**. Капица Ю. Проблемы правовой охраны конфиденциальной информации в Украине (часть 2) // Інтелектуальна власність № 3, Київ, 2004, с. 27 – 33. **4**. Конституція України від 26. 06. 96 // Відомості Верховної Ради України, 1996, № 30 (23. 07. 96), ст. 141 **5**. Закон України «Про інформацію» від 02. 10. 92 // Відомості Верховної Ради України, 1992, № 48 (01. 12. 92), ст. 650 **6**. Закон України «Про державну таємницю» від 21. 01. 94 // Відомості Верховної Ради України, 1994, № 16 (19. 04. 94), ст. 93 **7**. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05. 07. 94 // Відомості Верховної Ради України, 1994, N 31 (02. 08. 94), ст. 286 **8**. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджена Постановою Кабінету міністрів України № 1893 від 27 листопада 1998 р. // Офіційний вісник України, 1998, № 48 (17. 12. 98), ст. 1764. **9**. «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Затверджені Постановою Кабінету міністрів України № 373 від 29 березня 2006 р. // Офіційний вісник України, 2006, № 13 (12. 04. 2006), ст. 878. **10**. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К. Г. Устименка) від 30 жовтня 1997 року // Офіційний вісник України, 1997, число 46 (02. 12. 97), №с. 126. **11.** «Концепція технічного захисту інформації в Україні». Затверджена Постановою Кабінету міністрів України № 1126 від 8 жовтня 1997 р.*

УДК 65.012.8:004.05

АВТОМАТИЗАЦІЯ КОНФІГУРАЦІЇ ПАРАМЕТРІВ БЕЗПЕКИ ОС MICROSOFT WINDOWS XP PROFESSIONAL SP2

Віталій Носов, Максим Кулік*, Олександр Манжай

*Харківський національний університет внутрішніх справ, *Науково-дослідний експертно-криміналістичний центр при УМВС України в м. Севастополі*

Анотація: **Наведено результати досліджень способів конфігурування параметрів безпеки ОС Microsoft Windows XP Professional SP2 та опис утиліти автоматизації конфігурування.**

Summary: **In the article are considered methods of configuration services security Microsoft Windows XP Professional SP2 and described utility for automation configuration.**

Ключові слова: **Інформаційна безпека, параметри безпеки операційної системи, Microsoft Windows XP Professional SP2, автоматизація конфігурації.**

I Вступ

В 2005 році Департамент спеціальних телекомунікаційних систем та захисту інформації Служби