УДК 004.056.5

Олег Олександрович Шкарлат [1]
Роман Михайлович Штонда [2]
Юлія Олександрівна Черниш [2]
Марія Володимирівна Сулімовська [3]

[1] ***Асоціація охоронно-юридичних фірм "Паладін", Київ, Україна***
[2] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[3] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ СУБ'ЄКТІВ ОХОРОННОЇ ДІЯЛЬНОСТІ

Інформаційна безпека суб'єкта охоронної діяльності, полягає в захищеності інтересів суб'єкту охоронної діяльності, пов'язаних із захистом від несанкціонованого доступу до тих відомостей, які є важливими в роботі суб'єкту охоронної діяльності. Критичні відомості можуть бути представлені сукупністю інформації, що здатна задовольняти інтерес власника, і його дії, спрямовані на оволодіння інформацією або приховування інформації. Ці відомості і захищаються від зовнішніх і внутрішніх загроз. У разі, коли суб'єкт охоронної діяльності не бачить необхідності в захисті своїх дій, наприклад, в зв'язку з тим, що це не окупається, зміст інформаційної безпеки може бути зведений до захищеності конкретної інформації, розкриття якої може принести помітний збиток в діяльності. Конфіденційна для суб'єкта охоронної діяльності інформація входить до сфери підвищеного інтересу конкуруючих компаній. Для недобросовісних конкурентів, корупціонерів та інших зловмисників особливу цікавість має інформація про склад менеджменту організації, її статус та діяльність. Подібна інформація зазвичай відноситься до комерційної таємниці. В деяких випадках навіть забезпечення викрадення 1/5 конфіденційної інформації може мати критичні наслідки для фінансової безпеки.

Ключові слова: *автоматизована система, інформаційна безпека, засоби захисту інформації, система інформаційної безпеки, суб'єкт охоронної діяльності.*

Вступ

Система захисту інформації, яка в автоматизованих системах суб'єктів охоронної діяльності функціонує у формі електронних документів, охоплює всі етапи розробки, впровадження й експлуатації програмного забезпечення, що застосовується в автоматизованих системах. Створення надійної та ефективної системи захисту інформації в організаціях відбувається в декілька етапів:

аналіз можливих загроз та втрат для автоматизованої системи полягає у виборі з безлічі можливих впливів на систему лише тих, які можуть реально виникати і наносити значні збитки системі;

розробка (планування) політики безпеки і системи захисту у вигляді єдиної сукупності заходів різного плану (правових, морально-етичних, адміністративних, технічних) для протидії можливим загрозам;

реалізація системи захисту з використанням організаційних і програмно-технічних засобів захисту інформації;

супроводження системи захисту під час експлуатації платіжної системи.

Усі етапи нерозривно пов'язані між собою. У процесі впровадження та експлуатації автоматизованих систем необхідно постійно аналізувати достатність системи захисту та можливість виникнення загроз, які не були враховані на попередніх етапах. Тому процес створення системи захисту інформації є постійним і потребує уваги та безперервного ретельного аналізу функціонування автоматизованої системи.

Постановка проблеми. В даний час відсутня будь-яка універсальна методика, що дозволяє чітко віднести ту чи іншу інформацію до категорії комерційної таємниці. Можна тільки порадити виходити з принципу економічної вигоди і безпеки підприємства – надмірна "засекреченість" призводить до необґрунтованого подорожання необхідних заходів щодо захисту інформації та не сприяє розвитку бізнесу, в той же час відкритість інформації може привести до великих фінансових втрат або розголошення комерційної таємниці.

Аналіз останніх досліджень і публікацій. Проблеми захисту інформації в автоматизованих системах суб'єктів господарювання і не тільки розглядали в своїх працях такі автори як Нашинець-Наумова А., Благодарний А.М., Пількевич І.А., Клеха О.В., Гавловський В. [1-5].

Метою статті є аналіз існуючих математичних моделей та методів для подальшого їх застосування в побудові систем захисту інформації в автоматизованих системах суб'єктів охоронної діяльності.

Виклад основного матеріалу дослідження

Конкретний зміст зазначених заходів для кожної окремої взятої організації може бути

різним за масштабами та формами. Це залежить в першу чергу від фінансових можливостей організації, від обсягів інформації і ступеня її важливості. Суттєвим є те, що весь перелік зазначених заходів обов'язково повинен плануватися і використовуватися з урахуванням особливостей функціонування автоматизованої системи організації.

В обґрунтуванні витрат на систему захисту інформації організації, існує два основні підходи.

Перший підхід полягає в тому, щоб освоїти, а потім і застосувати на практиці необхідний інструментарій вимірювання рівня захисту інформації. Для цього необхідно залучити керівництво організації (як її власника) до оцінки вартості інформаційних ресурсів, визначення оцінки потенційних збитків від порушень в області захисту інформації. Від результатів цих оцінок буде багато в чому залежати подальша діяльність керівників в області захисту інформації. Якщо інформація нічого не варта, істотних загроз для інформаційних активів компанії немає, а потенційний збиток мінімальний (керівництво це підтверджує), проблемою забезпечення захисту інформації можна не займатися. Якщо інформація має певну вартість, та існують загрози і потенційна шкода, тоді постає питання про внесення в бюджет організації витрат на систему захисту інформації. У цьому випадку виникає необхідність заручитися підтримкою керівництва компанії в усвідомленні проблем захисту інформації і побудові корпоративної системи захисту інформації.

Другий підхід, полягає в наступному: можна спробувати знайти варіант розумної вартості корпоративної системи захисту інформації. Адже існують аналогічні варіанти в інших областях, де значущі для бізнесу події носять імовірнісний характер. Наприклад, на ринку автострахування оцінка вартості цієї послуги становить - 5-15% від ринкової вартості автомобіля в залежності від локальних умов його експлуатації, стажу водія, інтенсивності руху, стану доріг тощо.

За аналогією, захистом інформації в компанії можна взагалі не займатися, і не виключений такий варіант, що прийнятий ризик себе цілком виправдає. А можна витратити на створення корпоративної системи захисту інформації чимало грошей, і при цьому залишиться деяка вразливість, яка рано чи пізно призведе до витоку інформації.

Ефективність захисту інформації в автоматизованих системах досягається застосуванням засобів захисту інформації (далі ЗЗІ). Під ЗЗІ розуміються технічні, програмні засоби або технічно-програмні засоби, які призначені для захисту інформації.

На даний момент часу на ринку представлена велика різноманітність ЗЗІ, які умовно можна розділити на декілька груп:

засоби, що забезпечують розмежування доступу до інформації в автоматизованих системах;

засоби, що забезпечують захист інформації при передачі її по каналах зв'язку;

засоби, що забезпечують захист від витоку інформації по різним технічним каналам під час функціонування автоматизованих систем;

засоби, що забезпечують захист від впливу програм-вірусів;

засоби, що забезпечують безпеку зберігання, транспортування носіїв інформації і захист їх від копіювання.

Основне призначення ЗЗІ першої групи – розмежування доступу до інформації в автоматизованих системах полягає в:

ідентифікації та аутентифікації користувачів автоматизованої системи;

розмежування доступу зареєстрованих користувачів до інформаційних ресурсів;

реєстрації дій користувачів;

захисті завантаження операційної системи;

контролі цілісності ЗЗІ та інформаційних ресурсів.

Розмежування доступу зареєстрованих користувачів до інформаційних ресурсів здійснюється ЗЗІ відповідно до встановлених для користувачів повноважень. Як правило, ЗЗІ забезпечують розмежування доступу до гнучких, жорстких дисків, портів та пристроїв. Повноваження користувачів встановлюються за допомогою спеціальних налаштувань ЗЗІ.

По відношенню до інформаційних ресурсів ЗЗІ можуть встановлюватися наступні повноваження: читання, запис, створення тощо. Системи захисту інформації передбачають ведення журналу, в якому реєструються певні події, пов'язані з діями користувачів, наприклад редагування (модифікацію) файлів, запуск програми, виведення на друк і інші, а також спроби несанкціонованого доступу до ресурсів.

Особливо варто відзначити наявність в ЗЗІ функції захисту інформації завантаження операційної системи з флеш-накопичувачів і CD-ROM, що дозволяє захистити систему від злому з використанням спеціальних технологій.

У різних ЗЗІ існують програмні та апаратно-програмні реалізації цього захисту, проте практика показує, що програмна реалізація не завжди та в повній мірі забезпечує необхідний захист.

Контроль цілісності файлів, які підлягають захисту полягає в підрахунку і порівнянні контрольних сум файлів. При цьому використовуються різної складності алгоритми підрахунку контрольних сум.

Оскільки на ринку представлена велика різноманітність ЗЗІ, вибір певного ЗЗІ залежить від наступних критеріїв:

умовами функціонування (операційне середовище, апаратна платформа, автономні персональні обчислювальні машини та обчислювальні мережі);

складністю налаштування і управління параметрами засобів захисту інформації;

типами ідентифікаторів, що використовуються;

переліком подій, що підлягають реєстрації;

вартістю засобів захисту.

З розвитком мережевих технологій з'явився новий тип ЗЗІ – міжмережеві екрани (firewalls), які забезпечують рішення таких задач, як захист підключень до зовнішніх мереж, розмежування доступу між сегментами корпоративної мережі, захист корпоративних потоків даних.

Захист інформації при передачі її по каналах зв'язку здійснюється засобами криптографічного захисту (далі – засіб КЗІ). Характерною особливістю цих засобів є те, що вони потенційно забезпечують найвищий захист переданої інформації від несанкціонованого доступу до неї. Крім цього, засоби КЗІ забезпечують захист інформації від модифікації.

Як правило, засоби КЗІ функціонують в автоматизованих системах як самостійний засіб, проте в окремих випадках засоби КЗІ можуть функціонувати в складі засобів розмежування доступу як функціональна підсистема для посилення захисних властивостей останніх.

Забезпечуючи високу ступінь захисту інформації, в той же час застосування засобів КЗІ спричиняє ряд незручностей:

стійкість засобів КЗІ є потенційною, тобто гарантується при дотриманні ряду додаткових вимог, реалізація яких на практиці здійснюється досить складно (створення і функціонування ключової системи, розподіл ключів, забезпечення збереження ключів, планування та організація заходів при компрометації ключової системи);

відносно висока експлуатаційна вартість таких засобів.

В організаціях для забезпечення фізичного захисту носіїв інформації встановлюються, як правило, наступні організаційні заходи: охорона приміщень, доступ до цих приміщень, встановлення порядку користування носіями інформації, а також закріплення технічних засобів за співробітниками та їх ремонт.

Вимоги щодо встановлення організаційних заходів в організаціях, установах тощо оформлюються у вигляді організаційно-розпорядчих документів і доводяться для ознайомлення до співробітників організації.

Обмеження доступу до інформації яка підлягає захисту сприяє створенню найбільш ефективних умов для її збереження. Необхідно чітко визначати коло співробітників організації, яким дозволено користуватися зазначеною інформацією.

Експерти-практики в галузі захисту інформації знайшли оптимальне рішення, при якому можна відчувати себе відносно впевнено – вартість системи захисту інформації повинна складати приблизно 10-20% від вартості автоматизованої системи. Це і є та сама оцінка на основі практичного досвіду (best practice), якою можна впевнено оперувати, якщо не відпрацьовувати детальні розрахунки.

Цей підхід, очевидно, не позбавлений недоліків. В даному випадку, швидше за все, не вдасться залучити керівництво в глибоке усвідомлення проблем захисту інформації. Але можливо обґрунтувати обсяг бюджету на захист інформації шляхом посилання на зрозумілі більшості власників інформаційних ресурсів загальноприйняті вимоги до забезпечення режиму інформаційної безпеки, формалізовані в ряді стандартів, наприклад ISO 17799.

Для ефективного функціонування системи захисту інформації підприємства її необхідно оснастити оптимальним комплексом апаратних і програмних засобів захисту від різних інформаційних загроз таким чином, щоб оптимізувати деякий критерій оптимальності створення системи захисту інформації. При цьому вважається, що інформаційні загрози між собою не пов'язані.

Нижче розглядаються моделі вирішення проблеми створення систем захисту інформації організації.

У загальному випадку вважаємо, що задано безліч інформаційних загроз (ІЗ), які можуть виникнути в автоматизованій системі організації і безліч апаратних і програмних засобів захисту (ЗЗ), за допомогою яких ці загрози можуть бути нейтралізовані. Причому для кожного поєднання ІЗ – ЗЗ визначено число r_1 (ij) – ефективність нейтралізації і-м ЗЗ j-й ІЗ. Для побудови математичної моделі введемо змінну y (i, j), що дорівнює 1, якщо j-а ІЗ нейтралізується за допомогою і-го ЗЗ, і нулю - в іншому випадку.

Для кращого розуміння дамо змістовну і формальну постановку завдань вибору оптимальної системи захисту інформації в термінах теорії графів, а також методи їх вирішення. Для цього побудуємо двочасткові графи G (X, U), ($X = uX_i$, i = 1,2) такий, що вершини безлічі в X_1 відповідають апаратним і програмним засобам захисту, а вершини множин в X_2 - відповідним інформаційним загрозам. Кожен елемент (вершина) безлічі X_1 характеризується ціною і ефективністю по нейтралізації інформаційних загроз. Кожній вершині безлічі $X \backslash X_2$ присвоюється вага, рівна вартості, що відповідає ЗЗ, а кожній дузі – $(i,j) \in U$ вага, z (i, j) = 1,0. Тоді завдання вибору оптимальної системи захисту інформації полягатиме в максимізації ефективності нейтралізації безлічі інформаційних загроз різними засобами захисту при обмеженнях на обсяг витрат Q. Формальна постановка задачі має наступний вигляд [6]:

$$\sum_{j=1}^{m}\sum_{i=1}^{n} r_1(ij)\,y(ij) \to \max$$

при обмеженнях

$$\sum_{i=1}^{n} r_2(i) * \operatorname{sing} \sum_{x_i \in X_2} y(ij) \le Q \qquad (1)$$

$$\forall x_i \in X_2,\ \sum_{x_i \in X_1}^{n} y(ij) = 1;$$

$$\forall(ij) \in U, y(ij) = 1{,}0$$

де $r_2(i)$ – витрати на купівлю і-го ЗЗ.

Якщо необхідно мінімізувати витрати на засоби захисту від інформаційних загроз в автоматизованих системах організацій при обмеженні на заданий рівень ефективності Р, то формальна постановка задачі буде мати вигляд:

$$\sum_{i=1}^{n} r_2(i) * \operatorname{sing} \sum_{j=1}^{m} y(ij) \to \min$$

$$\sum_{j=1}^{m} \sum_{i=1}^{n} r_l(ij) y(ij) / \sum_{i=1}^{n} (\max r_l(ij)) \le P \qquad (2)$$

$$\forall x_i \in X_2, \sum_{x_i \in X_1}^{j} y(ij) = 1$$

$$\forall(ij) \in U, y(ij) = 1{,}0$$

У моделі (2) передбачається, що найвищий рівень ефективності системи захисту інформації буде тоді, коли для нейтралізації кожної загрози буде обрано засіб захисту з максимальною ефективністю. Найвищий рівень ефективності системи захисту інформації дорівнює сумі максимальних елементів в кожному стовпці матриці r_l (ij).

До найбільш загальних закономірностей безпеки відноситься властивість, яка говорить про те, що "ступінь безпеки системи визначається ступенем безпеки її самого слабкого елемента". Якщо перефразувати цю властивість, то для нашого випадку рівень інформаційної безпеки буде визначатися ЗЗ з найменшою ефективністю, обраного нами з усієї безлічі засобів захисту. В цьому випадку формальна постановка задачі буде мати вигляд:

$$\min \sum_{i=1}^{n} r_l(ij) y(ij) \to \max$$

при обмеженнях

$$\sum_{i=1}^{n} r_2(i) * \operatorname{sing} \sum_{x_i \in X_2} y(ij) \le Q$$

$$\forall x_i \in X_{2,} \sum_{x_i \in X_1}^{n} y(ij) = 1; \qquad (3)$$

$$\forall(ij) \in U, y(ij) = 1{,}0$$

У тому випадку, коли інформаційні загрози не є незалежними, тобто поява однієї ІЗ є джерелом для іншої, то, позначаючи X_i з X_1 – підмножина вершин "лівої" частки, що відповідають ЗЗ, використання яких передує появі і-ї ІЗ, то (1) перетвориться до виду:

$$\sum_{x_k \in X_{2l}} \sum_{(ij) \in L(s,t_k)} r_l(ij) * z(ij) \to \max$$

$$\sum_{i=1}^{n} r_2(i) * \operatorname{sing} \sum_{x_i \in X_2} y(ij) \le Q \qquad (4)$$

$$\forall x_i \in X_2, \sum_{x_i \in X_i}^{n} y(ij) = 1;$$

$$\forall(ij) \in U, y(ij) = 1{,}0$$

В моделі (3) вважаємо, що для отримання інформації, необхідної для виконання j-ї загрози досить появи однієї з ІЗ, що відповідають X_i. L (s, t_k) – шлях з фіктивної вершини - джерела, дуги з якого заходять в усі вершини - джерела підмножини X_2, в вершину $x_{tk} \in X_2$.

Запропоновані вище формальні моделі відносяться до класу задач дискретного програмування для їх вирішення можуть бути використані різні типи алгоритмів.

Методи, що гарантують оптимальне рішення задачі. Як приклад візьмемо алгоритми Балаша і метод гілок і меж. Для того, щоб поєднати позитивні якості цих алгоритмів використовуємо побудову змішаних стратегій. Для аналізу змішаних стратегій введемо граф G (X, U), що визначає дерево рішень задачі, де X - безліч вершин і U - безліч дуг. Дерево рішень, побудоване алгоритмом типу гілок і меж, позначимо G_1 (X_1, U_1), а дерево, побудоване за допомогою алгоритму Балаша, позначимо G_2 (X_2, U_2). Справедливе наступне твердження. Дерево G_1 (X_1, U_1) є підпунктом дерева G_2 (X_2, U_2).

На основі наведеної теореми може бути побудований наступний алгоритм.

Крок 1. Визначаємо безліч висячих вершин першого ярусу дерева рішень X_1, де $|X_1| = 2$, і обчислюємо їх оцінки.

Крок 2. На безлічі отриманих оцінок виділяємо ліпшу і найближчу до неї.

Крок 3. Якщо базис вектора змінних, відповідний ліпшій оцінці, містить всі компоненти вектора змінних, то переходимо до кроку 15, якщо ні - то до кроку 4.

Крок 4. Рекорду R присвоюємо значення, рівне оцінці, найближчої до ліпшої.

Крок 5. Розширюємо базис, відповідний вершині з ліпшою оцінкою, і обчислюємо оцінку нового базису.

Крок 6. Якщо нова оцінка ліпшого рекорду, то переходимо до кроку 7, в іншому випадку – до кроку 9.

Крок 7. Якщо в базис введені всі змінні, то переходимо до кроку 8, в іншому випадку - до кроку 5.

Крок 8. Рекорду присвоюється значення, рівне ліпшій оцінці.

Крок 9. Замінюємо значення останньої змінної базису на зворотне і обчислюємо нову оцінку.

Крок 10. Якщо оцінка нового часткового плану ліпшого рекорду, то переходимо до кроку 7, якщо немає, то переходимо до кроку 11.

Крок 11. Базис піддається стиску, відповідну оцінку запам'ятовуємо і переходимо до кроку 12.

Крок 12. Якщо подальше стиснення базису неможливо, так як він відповідає вершині, що мала ліпшу оцінку на кроці 3 останньої ітерації, то

переходимо до кроку 13, в іншому випадку – до кроку 9.

Крок 13. Вершину дерева рішень, якій відповідає оцінка, рівна рекорду, вважаємо ліпшою.

Крок 14. На безлічі інших вершин дерева рішень вибираємо оцінку найближчу до ліпшої і переходимо до кроку 3.

Крок 15. Роздруковуємо вектор змінних. Закінчення дій алгоритму.

Перевагою методів типу гілок і меж в порівнянні з алгоритмом Балаша є менший обсяг перебору, за який доводиться платити жорсткими обмеженнями до пам'яті персонального комп'ютера і великим числом порівнянь. Скорочення числа операцій порівнянь можна досягти, поєднуючи спуск по дереву рішень в кращому напрямку, властивий методам типу гілок і меж, з перебором, реалізованим алгоритмом Балаша.

Експериментальна оцінка підтверджує ефективність поєднаної стратегії руху по дереву рішень.

Методи, що дають шанс на отримання оптимального рішення. Широке поширення алгоритмів пояснюється їх простотою, легкістю реалізації на персональному комп'ютері, можливістю в короткі терміни отримати досить хороші рішення, низькими вимогами до обсягу пам'яті персонального комп'ютера. Основною їх відмінністю від наведених вище детермінованих методів локальної оптимізації є випадковий вибір напрямку руху по дереву рішень на часткових планах, так і по векторній решітці на повних планах. Якщо всі напрямки вірогідні, то кажуть, що реалізується метод Монте-Карло, нас же буде цікавити підхід, при якому з великою ймовірністю вибираються ліпші напрями. Одним із способів реалізації такого підходу є наступна процедура: для безлічі $\{s\}$ сусідніх з s_0 планів обчислюються оцінки $\Delta(S_i)S_i \in \{S\}$ які зводяться до рівня q (q> = 0 для задач з максімізуючим функціоналом мети і q <= 0 для задач з мінімізуючим функціоналом мети), що називаються ступенем довіри оцінці. Потім частина числової осі від 0 до 1 розбивається на відрізки по числу обчислених оцінок, причому довжина і-го відрізка L_i дорівнює:

$$L_i = \Delta q(S_i) / \sum_i \Delta g(S_i) \qquad (5)$$

Береться випадкове число $0 \lhd \alpha \leq 1$ (рівномірний розподіл) і вибирається той відрізок, на який це число падає. Очевидно, що чим краще оцінка, тим ширше відповідний її відрізок і, отже, тим більша ймовірність її вибору. При q = 0 такий підхід полягає в методі Монте-Карло, $q \to \infty$ - в детермінованому пошуку в кращому напрямку.

Висновки й перспективи подальших досліджень

Таким чином, ефективність зазначених вище алгоритмів в значній мірі визначаться числом переглянутих рішень за виділений для розрахунку час, тобто їх швидкодією. Актуальність підвищення швидкодії зростає для адаптивних процедур, які потребують додаткових рішень для накопичення досвіду і адаптації. Існуючі способи підвищення швидкодії алгоритмів (вибір способу обчислення оцінки, розгалуження, ступеня і довірливість адаптивних процедур) зазвичай пов'язані зі специфікою конкретних задач. Подальші дослідження сприятимуть вирішенню нових прикладних задач, пов'язаних з оцінкою і вибором варіантів побудови систем захисту інформації.

Література

1. Нашинець-Наумова А. Організація системи захисту інформації суб'єктів господарювання /А. Нашинець-Наумова// Підприємство, господарювання і право К.: КУ ім. Бориса Грінченка, 2016. – С.110-116. **2. Благодарний А.М.** Адміністративно-правові заходи охорони інформації в автоматизованих системах /А.М. Благодарний// Інформаційна безпека людини, суспільства, держави №1(14) К.: 2014 С.70-75. **3. Пількевич І.А.** Захист інформації в автоматизованих системах управління /І.А.Пількевич, Н.М.Лобанчикова, К.В.Молодецька// Навчальний посібник Ж.: ЖВІ ім. С.П.Корольова, 2015 С. 57-102. **4. Клеха О.В.** Основні проблеми при побудові моделей захисту інформації в комп'ютерній мережі автоматизованих системах /О.В.Клеха// збірник Компютерно-інтегровані технології: освіта, наука, виробництво №8 Л.: Луцький НТУ, 2012. – С.42-46. **5. Гавловський В.** Інформаційна безпека захист інформації в автоматизованих системах (організаційно-правові аспекти) /[Электронный ресурс]// Режим доступу http://pnzzi.kpi.ua – Назва з екрану. **6. Росс Г., Табаков А**. Проблемы безопасности автоматизированных информационных систем на предприятиях /[Электронный ресурс]// Режим доступу http://www.okbsapr.ru – Назва з екрану.

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СУБЪЕКТОВ ОХРАННОЙ ДЕЯТЕЛЬНОСТИ

***Олег Александрович Шкарлат*[1]**
***Роман Михайлович Штонда*[2]**
***Юлия Александровна Черныш*[2]**
***Мария Владимировна Сулимовская*[3]**

[1]Асоциация охранно-юридических фирм "Паладин", Киев, Украина
[2]Военний институт телекоммуникаций и информатизации имени Героев Крут, Киев, Украина
[3]Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Информационная безопасность субъекта охранной деятельности, состоит в защищенности интересов субъекта охранной деятельности, связанных с защитой от несанкционированного доступа к тем ведомостям, которые являются важными в работе субъекта охранной деятельности. Критические ведомости могут быть представлены совокупностью информации, которая способна удовлетворять интерес владельца, и его действия, направленные на овладение информацией или скрытие информации. Эти ведомости и защищаются от внешних и внутренних угроз. В случае, когда субъект охранной деятельности не видит необходимости в защите своих действий, например, в связи с тем, что это не окупается, содержание информационной безопасности может быть сведено к защищенности конкретной информации, раскрытие которой может нанести заметный убыток деятельности. Конфиденциальная для субъекта охранной деятельности информация входит в сферу повышенного интереса конкурирующих компаний. Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес имеет информация о составе менеджмента организации, ее статусе и деятельности. Подобная информация обычно относится к коммерческой тайне. В некоторых случаях также обеспечение похищения 1/5 конфиденциальной информации может иметь критические последствия для финансовой безопасности.

Ключевые слова: *автоматизированная система, информационная безопасность, средства защиты информации, система информационной безопасности, субъект охранной деятельности.*

PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS OF SECURITY ACTIVITY SUBJECTS

***Oleg O. Shkarlat*[1]**
***Roman M. Shtonda*[2]**
***Yulia A. Chernish*[2]**
***Maria M. Sulimovska*[2]**

[1]***Association of Security Law Firms "Paladin", Kyiv, Ukraine***
[2]***Military Institute of Telecommunications and Information named after Heroiv Krut, Kyiv, Ukraine***
[3]***National Defense University of Ukraine named after Ivan Chernyhovski, Kyiv, Ukraine***

The information security of the subject of the security activity, is in the protection of the interests of the security activity subject, connected with protection from unauthorized access to those data that are important in the work of the security activity subject. Critical data can be presented by a combination of information that is able to satisfy the owner's interest, and his actions aimed at mastering information or a screen of information. These data are protected against external and internal threats. In the case when the subject of the hunting activity does not see the need to protect its actions, for example, due to the fact that this does not pay off, the content of information security can be reduced to the protection of specific information, the disclosure of which may cause a noticeable loss of activity. Confidential for the subject of security activities information is in the sphere of increased interest of competing companies. For unscrupulous competitors, corrupt officials and other intruders, information about the composition of the organization's management, its status and activities is of particular interest. Such information usually refers to trade secrets. In some cases, also ensuring the kidnapping of 1/5 of confidential information can have a critical impact on financial security.

Key words: *automated system, information security, information security means, information security system, security activity subject.*

References

1. Nashinets-Naumova A. (2016) Organization of the system of protection of information of business entities [Orghanizacija systemy zakhystu informaciji sub'jektiv ghospodarjuvannja] Kyiv, KU them. Boris Grinchenko Enterprise, management and law of, pp.110-116. **2. Grateful A.M.** (2014) Administrative-legal measures of protection of information in automated systems. [Administratyvno-pravovi zakhody okhorony informaciji v avtomatyzovanykh systemakh] Kyiv, Information security of a person, a society, a state №1(14) pp.70-75. **3. Pilkevich I.A.**, Lobanchikova N. M., Molodetska K. V.(2015) Information protection in automated control systems [Zakhyst informaciji v avtomatyzovanykh systemakh upravlinnja] Zhytomyr, ZhVI im . S.P.Korolova Educational manual for pp. 57-102. **4. Klekha O.V.** (2012) The main problems in the construction of data protection models in a computer network of automated systems [Osnovni problemy pry pobudovi modelej zakhystu informaciji v komp'juternij merezhi avtomatyzovanykh systemakh] Lutsk Lutsk NTU Collection Computer-integrated technologies: education, science, production No. 8 pp.42-46. **5. Gavlovsky V.** Information security information protection in automated systems (organizational and legal aspects) [Informacijna bezpeka zakhyst informaciji v avtomatyzovanykh systemakh (orghanizacijno-pravovi aspekty)] Electronic resource Access mode http://pnzzi.kpi.ua - Title from the screen. **6. Ross G**. Tabakov A. Security problems of automated information systems at enterprises [Problemyi bezopasnosti avtomatizirovannyih informatsionnyih sistem na predpriyatiyah] Electronic resource Access mode http://www.okbsapr.ru- Screen name.