УДК 004.056.2

ОРГАНІЗАЦІЯ ПРОЦЕСУ ФУНКЦІОНУВАННЯ ЗАСОБІВ ЗАХИСТУ СОЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Б. В. Дурняк, Т. М. Хомета

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Розроблено загальну організацію соціальної інформаційної системи. В рамках такої організації відображено переходи з одного стану безпеки в інший стан. Проаналізовано умови цього переходу.

Ключові слова: *система доступу, безпека, рівень безпеки, стан безпеки, соціальна система.*

Постановка проблеми. Метод реалізації кожного окремого засобу захисту може передбачити різні рівні вимог до способу їх функціонування. Ці рівні визначають повноту виконання функцій щодо виявлення та протидії атакам. Необхідність введення таких рівнів зумовлена тим, що не завжди зовнішні небезпеки реалізують свої максимальні можливості. Тому і протидія повинна реалізуватися адекватною мірою.

Аналіз останніх досліджень та публікацій. Над процесами функціонування інформаційних систем працюють фахівці, які розробляють бази даних різного призначення. У межах таких систем переважно створюють інтерфейси користувачів, в рамках яких розв'язують задачі доступу. Бази даних створює більшість фахівців у галузі інформатики, використовуючи відповідні мови програмування, що орієнтовані на створення баз даних, тому не має сенсу називати прізвища окремих фахівців.

Мета статті — дослідження та аналіз процесу функціонування засобів захисту соціальної інформаційної системи.

Виклад основного матеріалу дослідження. Системи, які обслуговують розв'язування соціальних задач, переважно переходять на використання інформаційних електронних засобів, що становлять основу технології функціонування таких систем. Організовуючи процес функціонування цих систем, треба визначити умови або стан системи, який умовно можна вважати початком функціонування. Здебільшого вводиться уявлення про псевдоцикл функціонування системи, що дозволяє прийняти, що система хоч і функціонує неперервно, але технологія її використання може розглядатися в рамках деякого циклу. Переважно такі псевдоцикли визначаються періодом проведення аудиту відповідної системи [1]. У нашому випадку приймемо деякі початкові умови системи CS_i та розглянемо алгоритм реалізації в системі функцій, що передбачаються в рамках цього дослідження, включно з функціями захисту системи від атак різних типів. Алгоритм загальної організації

процесу функціонування системи CS_i потрібно розглядати на різних рівнях узагальнення його представлення, оскільки в рамках вибраного псевдоциклу в системі розв'язується досить широкий клас задач, пов'язаних з обслуговуванням користувачів, виявленням та протидією атакам зі сторони зовнішніх факторів, які називаються небезпеками, визначенням рівня безпеки системи як деякої оцінки, яка дозволяє визначити доцільність або допустимість зберігання персональних даних в інформаційній системі, орієнтованій на розв'язування соціальних задач.

На найзагальнішому рівні алгоритм функціонування системи CS_i описується стратегією, яка визначає переходи системи загалом з одного рівня безпеки на інший, визначає моменти активізації різних систем, що є компонентами всього комплексу CS_i, та реалізує синхронізацію роботи цілої системи. Стратегія функціонування комплексу CS_i охоплює один псевдоцикл, який визначається двома послідовними в часі аудитами. Загальна часова послідовність функціонування стратегії $St(CS_i)$ може бути описана послідовністю задач, розв'язання яких ця стратегія ініціює:

- визначення загального рівня безпеки CS_i, $RB(CS_i)$;
- активізацію засобів доступу для користувачів типів h_i^c і h_i^φ;
- базове фонове тестування основних компонент системи $T_s(CS_i)$;
- перевірку інтегральних параметрів комплексу CS_i;
- перевірку запитів підсистем на позачергове обслуговування останніх;
- переведення системи з одного рівня стану безпеки на інший рівень стану безпеки, що здійснюється на основі аналізу системи безпеки;
- активізацію засобів захисту та протидії атакам.

Загальний рівень безпеки системи є її інтегральним параметром, який насамперед визначає, чи необхідно вживати невідкладних заходів щодо забезпечення безпеки персональних даних, які містяться в CS_i. Оскільки $RB(CS_i)$ є загальним параметром, то його обчислення доцільно реалізовувати в рамках $St(CS_i)$. На основі даних про величину цього параметра в рамках $St(CS_i)$ приймаються рішення про активізацію таких екстремальних дій, як:

- копіювання персональних даних, які виявились найбільш завантаженими на зовнішні носії даних;
- обмеження або блокування доступу користувачів, які визначаються за наперед визначеними параметрами, пов'язаними з засобами захисту та системою безпеки $SB(CS_i)$ загалом;
- встановлення вимог до засобів, які розв'язують задачі виявлення атак і загроз;
- введення підвищеного рівня пріоритету засобам, що забезпечують безпеку системи CS_i загалом;
- моніторування активізованих засобів захисту та аналіз результатів їх функціонування.

Копіювання найвразливіших персональних даних користувачів є стандартною процедурою у випадку виникнення небезпеки, яка може здійснити успішну атаку на дані. Завдяки копіюванню дані захищені від знищення внаслідок дії відповідних атак, від порушення цілісності або несанкціонованої модифікації. Копіювання реалізується у випадках, якщо існує високий рівень загрози їх пошкодження, що

відповідає стану аварійного рівня безпеки, коли використовуються всі засоби захисту, якими володіє система безпеки $SB(CS_i)$.

Обмеження доступу для окремих користувачів на вибраний інтервал часу є ефективним засобом для виявлення джерела несанкціонованих спроб отримати персональні дані. Оскільки рішення про видавання, чи невидавання даних приймається не тільки на рівні автентифікації користувача, а й на рівні аналізу профілю користувача й на основі аналізу даних, за наданням яких звернувся користувач, то останнє дає змогу глибше аналізувати можливі атаки загалом. Наприклад, якщо користувач відповідає профілю, то проводиться аналіз, чи черговий запит не суперечить іншим параметрам захисту. Аналогічно аналізуються дані, які позначаються маркерами заборони їх видавання (наприклад, їхньому власнику) чи маркерами необхідності проведення консультацій із відповідними користувачами класу h_i^{φ}. Якщо при обмеженні доступу користувача до системи виявиться, що атака зникає, то це може означати, що відповідний вхідний термінал становить загрозу для певного типу атак [2].

Встановлюється, що вимоги до процесу виявлення та протидії атакам можуть мати різний рівень функціональної повноти процесу виявлення. Наприклад, засіб, що реалізує моніторинг можливих загроз, може працювати в режимі вибіркового аналізу чи в режимі повного аналізу загроз, який інтерпретується як максимальна вимога до функціонування засобу захисту. Залежно від способу реалізації кожного окремого засобу захисту в ньому можна передбачити різні рівні вимог до способу їх функціонування. Такі рівні визначають повноту виконання тих чи інших функцій щодо виявлення та протидії атакам. Необхідність введення таких рівнів зумовлена тим, що не завжди зовнішні небезпеки реалізують свої максимальні можливості, тому і протидія повинна реалізуватися адекватною мірою. Прикладом визначення таких мір повноти реалізації функцій засобами захисту, з одного боку, та дії зовнішніх небезпек, з іншого, є введені рівні безпеки системи, що позначається як *BZS*, *PZS*, *RZS*, *SZS*, *NZS* та *AZS*. У рамках наведеної інтерпретації відповідних мір міра, що відповідає небезпечному рівню безпеки *NZS*, означає таке. У межах системи час від часу виникають несправності, які спричиняють відмови в обслуговуванні. Система безпеки $SB(CS_i)$ активізує окремі засоби захисту, що вибирають залежно від типу відмов, для виявлення причин таких відмов і на основі даних, отриманих від цих засобів захисту, активізує засоби протидії причинам виникнення відмов, які, відповідно до прийнятої термінології являють собою атаки на відповідну інформаційну систему CS_i. Якщо частота таких атак збільшується і перевищує деяку прийняту величину, то система переходить на аварійний рівень безпеки. Цей рівень характеризується тим, що $SB(CS_i)$ активізує всі наявні засоби захисту, що здійснюють виявлення атак, і засоби, які протидіють таким атакам. У стані *AZS* система аналізує результати роботи всіх засобів захисту. Якщо певна кількість засобів захисту не виявляє атак протягом заданого інтервалу, то система переходить на небезпечний рівень безпеки *NZS*.

У разі, коли частота відмов, яка була в *NZS*, зменшується до визначеного рівня, то система переходить на рівень стратегічної безпеки *SZB*. Це означає, що стратегія

функціонування системи безпеки *St*(*SB*) визначає певний порядок моніторування системи, щоб виявити причини можливого виникнення атак на систему. Стратегія St_i, яка, по суті, на цьому рівні безпеки *SZB* здійснює керування засобами безпеки, насамперед визначає поточні значення рівня безпеки системи $RB(CS_i)$ як базового інтегрального параметра, поточні значення інших інтегральних параметрів, які можуть стосуватися процесу функціонування системи, наприклад, частоту звертань до системи користувачів типу h_i^c чи h_i^φ, і на основі даних про значення вибраних інтегральних параметрів реалізує управління системою $SB(CS_i)$.

Якщо виникнення атак на CS_i зменшується, коли система перебуває на рівні *SZB*, то система може перейти на рівень стану безпеки *RZB*, який відповідає ситуації, коли засоби безпеки активізуються відповідно до вибраної дисципліни, що не змінюється протягом інтервалу часу перебування системи на рівні *RZS*. Цей рівень безпеки зберігається доти, доки в системі інтегральні параметри безпеки та процесу функціонування не зміняться таким чином, що кількість відмов наблизиться до нуля. В цьому випадку система переходить на рівень безпеки *PZS*, на якому активізуються процеси діагностики вибраних компонент, які визначаються як ключові. Якщо в результаті процесів діагностики протягом заданого інтервалу часу не буде виявлено недопустимих відхилень у роботі системи, то система переходить на безпечний рівень безпеки системи *BZS*.

Переходи системи з одного рівня безпеки на інший рівень безпеки можуть здійснюватися в довільному порядку, який визначається системою управління засобами захисту або адміністратором чи задачею адміністрування. Такі способи переходів та керування ними являють собою загальну стратегію системи функціонування комплексу, який складається з системи безпеки $SB(CS_i)$ та соціальної інформаційної системи CS_i. У наведеному вище описі переходів системи з одного рівня безпеки на інший рівень використовувався інтегральний параметр, який визначався частотою відмов в обслуговуванні, які виникали в системі *Z*.

Прикладом іншого інтегрального параметра може бути параметр, що характеризує вибрані властивості даних, які містяться в CS_i. Однією з таких властивостей даних може бути міра їх таємності. Ця міра в процесі функціонування системи, незалежно від того, чи виникали відмови, чи ні, може змінюватися. Кількість таких таємних даних також може змінюватися. У цьому випадку інтегральним параметром, який може використовуватися для керування рівнем безпеки системи, є параметр середнього рівня таємності даних. Такий параметр може являти собою деяку функцію від кількості даних $x_i \in CS_i$, які мають певний рівень таємності η_i або $x_i(\eta_i)$ та сам рівень таємності, що формально описується співвідношенням $x = f\left\{n, \left[x_i\left(\eta_j\right)\right], \eta_j\right\}$, де n — кількість параметрів x_i, які мають рівень таємності η_i; η_j — виділений рівень таємності. Можна ввести параметр x^*, який буде залежати від $n\left[x_i\left(\eta_i\right)\right]$, а рівень таємності η_i може залежати від інших параметрів, наприклад, від частоти запитів даних, що мають рівень таємності η_i, та від часу, протягом якого відповідні дані перебувають у CS_i. Тоді співвідношення для x_i запишемо у вигляді:

$$x^* = F\left\{n\left[x_i\left(\eta_i\right)\right], \eta_i\left(t\right), t_i\right\}.$$

Форма наведеної залежності будується на основі прийнятої інтерпретації кожної з компонент. Сама залежність x^* ґрунтується на гіпотезі, яка пов'язує $RB(CS_i)$ з рівнем таємності даних.

Гіпотеза 1. Що вищий рівень таємності даних, які містяться в CS_i, то вища загроза того, що зовнішні небезпеки будуть атакувати систему.

Гіпотеза 2. Що більше даних $x_i \in CS_i$ з високим рівнем таємності η_k, то вищий рівень безпеки RB_i, яку повинна забезпечувати для CS_i відповідна система захисту, яка реалізується у вигляді $SB(CS_i)$.

Окрім міри таємності, як інтегральний параметр може використовуватися параметр ризику незабезпечення безпеки, який уже був застосований для загальної оцінки. Ризик зниження необхідного рівня безпеки є параметром, значення якого прогнозується [3]. Цей параметр обчислюється здебільшого на основі статистичних даних, що стосуються змін величини безпеки, які відбувалися на минулих інтервалах часу функціонування системи. Хоча значення цього параметра являє собою величину, яка обчислюється на основі статистичних даних, але загальноприйнята інтерпретація величини ризику зіставляє цю оцінку з поточним моментом процесу функціонування системи [4]. Завдяки цьому величина ризику зменшення рівня безпеки системи може використовуватися для прийняття рішення системою управління безпекою CS_i щодо реалізації тих чи інших дій, спрямованих на забезпечення підтримки заданого рівня безпеки системи. Оскільки ризик визначає можливість зниження рівня безпеки, то дії $SB(CS_i)$ мають полягати в реалізації таких функцій:

– активізації додаткових засобів захисту;
– виявленні можливих загроз, які існують у системі;
– зміні параметрів функціонування наявних засобів захисту з ціллю підвищення їх ефективності.

Упроваджена послідовність рівнів безпеки, на яких може перебувати система, з погляду фізичної інтерпретації процесів функціонування інформаційної системи не може закінчуватися аварійним рівнем безпеки, адже не існує практичної можливості забезпечити повну безпеку системи, особливо, коли йдеться про інформаційну систему. Отже, потрібно передбачити можливість існування одного стану рівня безпеки, якого необхідно уникати. Цей рівень безпеки будемо називати критичним (*KZS*). Він означає, що в системі можуть розвиватися процеси, які можуть призвести до катастрофічних ситуацій. У цьому випадку, крім активізації всіх наявних засобів захисту, активізуються критичні процеси безпеки, про які йшлося і прикладом яких є копіювання персональних даних на аварійні зовнішні носії інформації, підключення резервних блоків до інформаційної системи та інші дії, що реалізуються на основі особливостей функціонування кожної окремої системи. Прикладом такої особливості може бути використання резервних джерел живлення та інші фактори. Оскільки *KZS* є рівнем безпеки, в який може перейти система з рівня безпеки *AZS*, що відповідає аварійному рівню, то в рамках функціонування процесів безпеки на цьому рівні, крім засобів захисту, що долучаються до роботи *SB*, повинні виконуватися функції, які були б орієнтовані на виведення системи

CS_i зі стану *AZS* щонайменше у стан *NZS*. У стані безпеки *AZS* система $SB(CS_i)$ активізує всі наявні засоби захисту, які існують у режимі максимальної ефективності, для забезпечення переходу на вищий рівень безпеки, тому *SB* повинна реалізувати процедури протидії зовнішнім небезпекам, що генерують атаки. Тільки в цьому випадку виникає можливість перейти з рівня *AZS* до вищого рівня безпеки. Відомі методи, які мають характер нейтралізації цілої небезпеки, полягають у створенні латентних хостів, що імітують реальні системи [5]. Крім методів імітації реальних хостів, використовуються методи виявлення небезпек в інформаційній мережі та блокування їх роботи на основі збігів із мережевим оточенням джерела атак.

У ситуації, яка виникла на рівні безпеки *BZS*, що відповідає безпечному функціонуванню системи, також треба ввести деякий початковий стан, який був би гарантом того, що система функціонуватиме безпечно. Такий рівень безпеки будемо називати рівнем контрольної перевірки системи *TZS*. Цей рівень завжди використовується перед початком експлуатації системи. Незважаючи на те, що система типу CS_i функціонує неперервно, на ній проводиться аудит, і після кожного аудиту система проходить через стан безпеки *TZS*. У стані безпеки *TZS* реалізуються тестові перевірки процесів функціонування системи. Принципова відмінність рівня безпеки *TZS* від рівня безпеки *PZS* полягає ось у чому:

- на рівні *TZS* здійснюється тестування процесів функціонування системи з використанням терміналів доступу, якими послуговуються користувачі типу h_i^c і h_i^φ;
- на рівні *TZS* не реалізуються процеси розв'язування соціальних задач;
- на рівні *PZS* здійснюється тестування системи, яке полягає у перевірці тестових параметрів;
- на рівні *PZS* функціонують процеси розв'язування соціальних задач, які активізуються користувачами.

Отже, перевірка працездатності системи реалізується на рівнях безпеки *TZS* та *PZS*. Враховуючи введені рівні безпеки, загальна схема взаємозв'язків окремих рівнів безпеки може бути описана у вигляді такого співвідношення:

$$TZS \rightarrow BZS \rightarrow PZS \rightarrow SZS \rightarrow NZS \rightarrow AZS \rightarrow KZS. \quad (1)$$

Для повного відображення процесів функціонування системи безпеки співвідношення (1) можна записати у вигляді:

$$TZS \rightarrow BZS \rightarrow PZS \rightarrow RZS \rightarrow SZS \rightarrow NZS \rightarrow AZS \rightarrow KZS$$
$$AZS \rightarrow NZS \rightarrow SZS \rightarrow RZS \rightarrow PZS \rightarrow BZS. \quad (2)$$

На рисунку використовуються такі позначення:

- *TZS* — початкове тестування системи;
- *IA* — ідентифікація користувача h_i^c;
- *VPD* — вибір персональних даних;
- *MV* — перевірка, чи дані можна видавати користувачеві;
- *AK* — визначення, чи відбувається атака на користувача;
- *ZP* — зміна пароля;
- *DF* — перевірка, чи користувач типу h_i^φ вводив відповідні дані в систему;
- *MDK* — модифікація даних для користувача типу h_i^c;

– *DKA* — діалог з користувачем h_i^c стосовно ідентифікації;
– *DKD* — діалог з користувачем відносно атаки на дані;

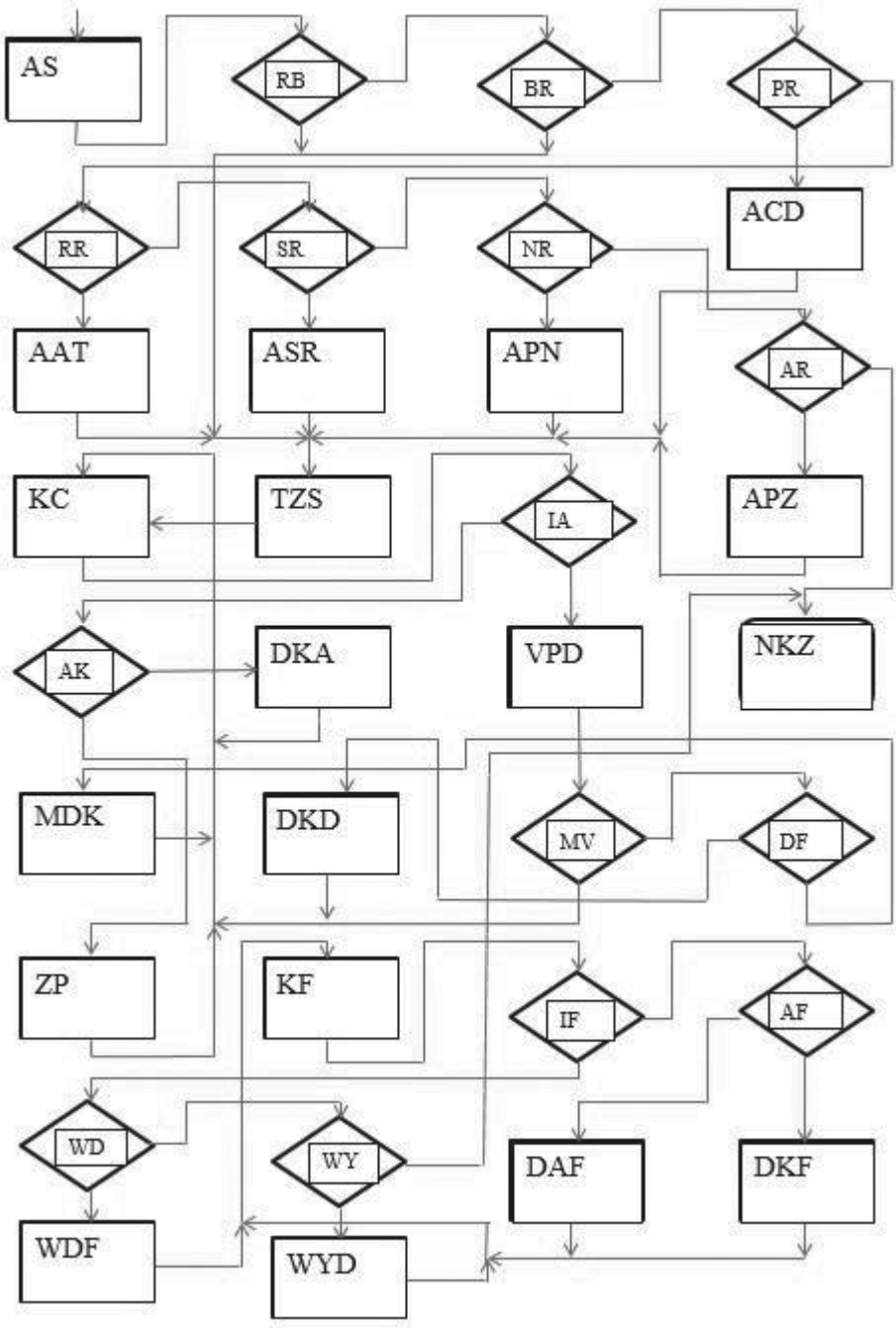

Рис. Блок-схема загальної організації соціальної інформаційної системи

– *IF* — ідентифікація користувачів h_i^{φ};
– *WDF* — введення даних;
– *AF* — визначення, чи здійснюється атака на фахівця;
– *WD* — перевірка, чи вводяться дані;
– *WY* — перевірка, чи виводяться дані;
– *IF* — ідентифікація користувачів h_i^{φ};
– *WDF* — введення даних фахівцем;
– *AF* — визначення, чи здійснюється атака на фахівця;
– *WD* — перевірка, чи вводяться дані;
– *WY* — перевірка, чи виводяться дані;
– *DKF* — діалог з користувачем стосовно атаки;
– *WYD* — виведення даних фахівцю;
– *DAF* — діалог стосовно атаки на фахівця;
– *RB* — визначення, чи є заданий рівень безпеки системи;
– *RB* — перевірка, чи система перебуває на безпечному рівні;
– *PR* — перевірка, чи система перебуває на профілактичному рівні безпеки;
– *RR* — перевірка, чи система є на активному рівні безпеки;
– *SR* — перевірка, чи система перебуває на стратегічному рівні безпеки;
– *NR* — перевірка, чи система перебуває на небезпечному рівні безпеки;
– *ACD* — активізація фонової діагностики системи;
– *AAT* — виявлення атак;
– *ASR* — активізація стратегічного рівня роботи інформаційної системи;
– *APN* — активізація протидії небезпекам;
– *APZ* — активізація повного захисту;
– *NKZ* — некоректне завершення задачі;
– *AS* — адміністрування системи;
– *AR* — перевірка, чи система перебуває на аварійному рівні безпеки функціонування;
– *KC* — хост користувача типу h_i^{c};
– *KF* — хост користувача типу h_i^{φ}.

Загальна організація системи CS_i відображає її функціонування в основних режимах, які відповідають розв'язуванню таких задач:
– обслуговування користувача типу h_i^{c};
– обслуговування користувача типу h_i^{φ};
– виявлення атак на користувачів і дані;
– керування рівнями безпеки системи;
– керування комплексом, який включає *SB*.

Висновки. Розроблений алгоритм функціонування інформаційної соціальної системи ілюструє можливості контролю рівнів безпеки, що змінюються в межах усієї системи через модифікації і зміни, які відбуваються з даними. Це дає змогу забезпечувати різні рівні захисту для окремих фрагментів даних, використовуваних системою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. — М. : Электро-информ. — 1997.
2. Materialy Bundesamt fur Sichercheit in der Jnformationstechinik. — Grund-sehutrhand buch, Niemcy 2002.
3. Шурыгин А. М. Прикладная стохастика: робастость, оценивание, прогноз / А. М. Шурыгин. — М. : Финансы и статистика. — 2005.
4. Лукач Е. Математика рискового страхования / Е. Лукач. — М. : Олимп-Бизнес, 2005.
5. Swanson M., Fabius J.,Stevens M., Mc Larnon M. Automated Security Self-Evaluation Tooln User Manual, National Jnstitute of Standards and Technology, Publication NISTIR 6885 2003 ED, 2003.

ORGANIZATION OF FUNCTIONING PROCESS OF PROTECTION FACILITIES OF SOCIAL INFORMATIVE SYSTEM

B. V. Durnyak, T. M. Khometa

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine

The general organization of the social informative system has been developed in the article. Within the framework of such organization, the transitions from one security status to another have been represented. The analysis of transition terms from one security status to another has been conducted.

Keywords: *access system, safety, security level, security status, social system.*

Стаття надійшла до редакції 16.06.2016.