УДК 004.9

ОРГАНІЗАЦІЯ РОБОТИ СИСТЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНОГО КОМПЛЕКСУ УПРАВЛІННЯ ПОЛІГРАФІЧНИМ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ

Т. М. Майба

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

У загальній організації функціонування комплексу безпеки інформаційної системи управління необхідно передбачити компоненти для реалізації процесів захисту. Основними з них будуть система управління технологічним процесом, система безпеки та система оцінки ризику. Основою функціонування системи прийняття рішень (DSR) є система формування рекомендацій. Така система реалізується на різних рівнях відображення моделі, що описує процес функціонування. Найбільш загальною є структурна модель, яка являє собою граф, що описує різні можливі послідовності реалізації штатних режимів функціонування. Виникнення нештатної ситуації на цьому рівні полягає у тому, що система в цілому на деякому режимі штатного функціонування попадає у вершину графа, з якого немає вихідного ребра. Якщо на графі, що відображає структуру процесів функціонування, точка управління попадає на вершину, яка належить до іншого режиму функціонування, то це означає, що в системі управління виникла несправність, яка може бути діагностована. На рівні моделі система DSR реалізує побудову ланцюга, який забезпечував би вихід процесу з вершини e^t_i, і такий ланцюг повинен складатися з ребер, які належать до ланцюгів штатних режимів функціонування.

Ключові слова: *методи захисту, інформаційна система управління, система моніторингу, система прогнозування.*

Постановка проблеми. Загальна організація функціонування комплексу безпеки інформаційної системи управління *(ISU)* повинна передбачати всі компоненти, необхідні для реалізації процесів захисту, що ґрунтуються на використанні методів визначення величини ризику невиконання технологічним процесом виробництва заданої продукції. До таких компонент, зокрема, належать:

- система управління *TPP, (ISU)*;
- комплекс безпеки функціонування *ISU, (SUB)*;
- система оцінки ризику функціонування *ISU, (SOR)*;
- система моніторування поточного стану *ISU, (SM)*;
- система прогнозування поодиноких подій, що активізувалися негативними факторами *(PON)*;
- дорадча система для прийняття рішень у разі збільшення величини ризику функціонування *ISU, (DSR)*;

– система аналізу людських факторів і факторів зовнішнього середовища *(ALF)*.

До основних компонент засобів управління та засобів безпеки належать: *ISU, SUB* та *SOR*. Тому треба детальніше розглянути допоміжні складові загальної системи, до яких належать: *SM, PON, DSR* і *ALF*. Наведені системи є допоміжними, оскільки вони дають змогу ефективно в автоматизованому режимі використовувати дані, отримані завдяки застосуванню основних систем.

Мета статті — дослідження методів захисту процесу функціонування на основі уявлень про ризик що виникає у системі управління технологічним процесом.

Виклад основного матеріалу дослідження. Крім наведених вище компонент і систем для реалізації процесу загального управління, потрібно розглянути систему загального управління всіма наведеними компонентами, оскільки кожна з них повинна активізуватися відповідно до умов, що визначають потребу їх використання. Таку систему позначатимемо *(ZSU)*. Окремим завданням, яке має розв'язувати система *ZSU* є реалізація програми виробництва необхідного продукту. Коротко розглянемо таку систему. Очевидно, що система *ZSU*, крім основних функцій організації процесу виробництва, повинна керувати допоміжними технологічними процесами, які насамперед призначені для виконання процесів підготовки технологічних засобів до виробництва. Ці підготовчі процеси полягають у настроюванні технологічного обладнання на певні режими роботи устаткування. Прикладом може бути настроювання сили притискання друкуючого барабану під час кольорового друкування, такою настройкою може також бути регулювання кольоророзподілу та інші технологічні приготування, характерні для поліграфічного виробництва. Цей режим функціонування *ZSU* є специфічний, тому що він відображає особливості організації поліграфічного виробництва. В рамках цього режиму можуть використовуватися допоміжні прилади та установки, які не застосовуються в *TPP* [1].

До системи *ZSU* слід звертатися щоразу, коли вона бере участь у процесі функціонування основних компонент системи управління *TPP*.

Система моніторингу є засобом, який розв'язує такі завдання в рамках всього процесу виробництва:

– синхронізацію процесу функціонування всієї системи управління і, відповідно, всіх складових;
– початковий контроль основних параметрів усієї системи контролю;
– формування графіку використання окремих компонент або системи загальної сукупності засобів виробництва заданого продукту;
– реагування на критичні події, що виникають у всій системі або в кожній підсистемі.

Система моніторингу досить тісно пов'язана із системою управління, яка реалізує керування значною мірою неперервним технологічним процесом, прикладом якого є процес функціонування окремого накладу. Стосовно кожної системи, що входить до складу *ZSU*, система *SM* виконує різні функції. Головним способом співпраці *SM* з іншими системами є переривання процесу функціонування однієї

системи й активування іншої системи або призупинення функціонування деякої системи чи активізації іншої системи. Завдяки розподіленості *ZSU*, яка зумовлюється розподіленістю обладнання *TPP* (причому така розподіленість є функціональною та фізичною), існує можливість організувати паралельне функціонування окремих систем, що використовуються в *TPP*. Принцип паралельного функціонування реалізується не тільки на рівні системи управління *ZSU* але й на рівні функціонування окремих компонент технічного обладнання. Ці аспекти розглядатися не будуть, тому що вони пов'язані з технологічними процесами друкування. В основі співпраці *SM* з іншими системами, зокрема з *ISU*, є уявлення про пріоритети. Система пріоритетів, яка визначає можливість переривання одного процесу іншим, може бути стаціонарною або динамічною. Кожний з процесів будемо зіставляти із системою, яка відповідний процес реалізує. Тому замість процесів можна говорити про системи. У випадку *ZSU* встановлюється початкова система пріоритетів *PRI,* яка може в процесі функціонування змінюватися. Тому приймемо найвищі початкові пріоритети, які позначатимемо числами {1, 2, 3, ...}, що для системи *ISU* дорівнюватимуть 1, для системи *SUB* — 3 і для *SM* — 2. Інші системи будуть приймати нижчі пріоритети на початковому етапі їх призначення. Оскільки негативні зовнішні фактори діють на *ISU* переважно через канали доступу та інші канали, які можна зараховувати до загроз, якщо вони можуть бути використані зовнішніми небезпеками для реалізації вторгнення в ту чи іншу систему. Прикладом таких загроз є доступ до активізації системи переривання процесу. Цей доступ може існувати в рамках зовнішнього пристрою, що безпосередньо пов'язаний з процесом тої чи іншої системи, а також всі засоби введення інформації, починаючи зі спеціалізованих пультів управління, які можуть розміщуватися на технологічних установках, та закінчуючи засобами введення-виведення, що використовуються в рамках системи управління [2]. Особливість таких каналів доступу до системи полягає в тому, що вони можуть активізуватися нестандартними способами, що переважно не враховується під час проектування основних систем. У зв'язку з цим *SM* повинна із заданим періодом контролювати події, які можуть виникати в загальній системі:

- виникнення переривань процесів управління у всіх окремих апаратних засобах системи;
- запити на активізацію процесів функціонування окремих систем, які виставили відповідні запити;
- завершення функціонування окремих процесів;
- перепризначення пріоритетів окремим системам;
- зміна циклу моніторування та інші задачі, які є загальними для цілої системи.

Порядок розв'язання наведених задач також реалізується відповідно до пріоритетів, призначених цим задачам залежно від їх інтерпретації. Реакція на зміну пріоритету як процес має найвищий пріоритет, оскільки переривання певної категорії можуть активізуватися атаками на *ISU*. В цьому випадку інформація про відповідне переривання передається у *SUB,* яка залежно від характеру розпізнаної атаки може перейти на рівень найвищого пріоритету. Дії щодо зміни пріоритету реалізуються з використанням функції *ZSU*. Зміна пріоритету може бути тимчасовою,

для чого застосовується параметр часового інтервалу. Такий пріоритет позначається символом $Pr_i(\Delta t_i)$ де індекс «*i*» — номер пріоритету. Очевидно, що в разі зміни пріоритету в однієї компоненти в рамках *ZSU* реалізуються необхідні заміни пріоритетів у інших компонентах. Ще однією функцією *SM* є аналіз запитів на активізацію окремих компонент. Система *SM* самостійно реалізує запити на активізацію, якщо на поточний момент активізовано процес, у якого пріоритет є нижчий від пріоритету компоненти, яка виставила відповідний запит, то *SM* реалізує процес активізації. В іншому випадку *SM* передає в *ZSU* запит на активізацію наступного процесу. Всі процеси, що активізуються відповідними системами, функціонують циклічно. Це допомагає оптимізувати загальне управління, оскільки *ZSU* не потрібно аналізувати можливість переривання або закриття відповідного процесу. Крім того, більшість процесів після завершення циклу функціонування передають у *ZSU* дані, які є результатом функціонування і можуть бути необхідними або використаними іншими процесами, що їх передбачається активізувати. В цьому випадку *SM* передає відповідні дані системі, яка активізується після завершення функціонування попереднього процесу. Задача перепризначення пріоритетів, яка виконується на рівні *SM* реалізується в тому випадку, якщо в системі виникає критична ситуація, інформація про яку передається з *ZSU* у *SM*. Це зумовлено тим, що в кожний момент часу може бути активізована тільки та система, яка має найвищий пріоритет. Використання цієї умови дає змогу визначити систему, яка може бути активізована. Тому в системі не може бути компонент, які одночасно мають однакові пріоритети.

Система прогнозування є однією з ключових у рамках *ZSU,* адже потреба в прогнозуванні виникає в процесі функціонування різних компонент. Однією з основних компонент, що використовує механізми прогнозування, є компонента визначення ризику зменшення заданого рівня безпеки системи, або

$$R(t) = \mu(Be) - - \delta\mu(Be).$$

Іншою компонентою, що використовує засоби прогнозування, є система безпеки, яка повинна оновлювати параметри, що характеризують ймовірність виникнення атак At_i. Система *ALF* також потребує розв'язання задачі прогнозування, оскільки в її рамках існує достатньо ймовірнісних параметрів, характерних для випадків, які описують людські фактори. Отже, компонента *PON* повинна певною мірою бути адекватною, що дає змогу її підлаштувати до особливостей кожної із задач прогнозування. Тому розглянемо особливості її функціонування з різними системами.

Система оцінки ризику *SOR* прогнозує величину зменшення $\mu(Be)$ в результаті виникнення деякої події Po_i, яка є досить рідкісною. У цьому випадку рідкісною подією називається подія, що виникає один раз за період циклу роботи *TPP*. Така ситуація є природньою, оскільки нова подія вводиться або не вводиться у зв'язку з бажанням досягти кращих параметрів функціонування *TPP* наприклад, підвищення ефективності функціонування *TPP* під час підготовки відповідного циклу роботи *TPP*. Очевидно, що в такому разі за відсутності достовірних даних про те, що відповідні зміни приведуть до підвищення, наприклад, ефективності процесів

у *TPP* і не знизять рівень безпеки необхідно визначити ризик появи останньої події. При цьому результат обчислення $R(t)$ повинен полягати не тільки в тому, щоб забезпечувати достовірність виникнення негативного фактора, але в результаті обчислення $R(t)$ має бути можливо визначити або оцінити величину можливого зменшення рівня безпеки процесу функціонування *TPP*.

У випадку, коли *PON* використовується в межах реалізації одного циклу функціонування *TPP*, у зв'язку з потребою визначення можливості зміни ймовірності виникнення атаки на *ISU* зі сторони небезпек, що можуть активізувати At_i, для роботи *PON* застосовуються статистичні дані про виникнення атак у попередніх циклах та інші дані, які цих атак стосуються. Прикладом інших даних може бути кількість успішних атак, типи загроз, які використовувалися під час реалізації атак, та інша інформація, яка, по суті, розширює можливості системи прогнозування. Приклади використання *PON* в інших системах розглядати не будемо.

Важливою компонентою загальної системи *ZSU* є компонента, яка визначає вплив людських факторів і факторів зовнішнього середовища на технологічний процес. Природно, що в цьому випадку розглядатимемо лише ситуації негативного впливу цих факторів на *TPP,* бо всі позитивні ефекти такого впливу враховуються під час проектування *TPP* і всіх компонент *ZSU*. Аналізуючи людські фактори, спиратимемося на дві позиції, характерні для *TPP*:

– вплив людських факторів *TPP* на етапі підготовки технологічного процесу, зумовленого замовленням на виробництво;
– вплив людських факторів, що виникає в разі участі персоналу обслуги в процесі реалізації *TPP*.

З погляду реалізації процесу виробництва найнебезпечнішою є ситуація, яка виникає в другому випадку. Потреба аналізу другої ситуації зумовлена тим, що поява негативних подій в цих випадках може приводити до невідворотних негативних наслідків у функціонуванні *TPP*, оскільки останній в межах одного циклу функціонування є неперервним процесом [3]. Аналіз цих факторів доцільний ще й тому, що за умови досить точного прогнозування їх виникнення існує можливість реалізації заходів, які протидіють їх появі. Прикладом такої можливості є нормалізація процесів втручання персоналом обслуги в *TPP* або підвищення автоматизації процесів такого втручання, а в особливо критичних випадках можна виключити таке втручання за рахунок автоматичного керування відповідним фрагментом чи елементом *TPP*. При постійній експлуатації засобів технологічного процесу та певній незмінності асортименту продукції, що виробляється, вплив людського фактора можна звести до мінімуму, використовуючи автоматизацію. У цьому випадку процеси прогнозування застосовуються не тільки для виявлення поодиноких факторів негативного впливу, а й сукупності факторів, які в підсумку призводять до негативних змін. Особливість використання *PON* полягає у тому, що вхідні дані мають стохастичний характер, що дає змогу застосовувати простіші моделі прогнозування порівняно з попередніми.

Модель прогнозування використовується також загальною моделлю управління для визначення можливості виникнення критичних ситуацій. В цьому випадку

необхідно визначати не тільки факт виникнення критичних ситуацій, а і їхні параметри. Це зумовлено тим, що на критичні ситуації треба реагувати, в міру можливості, досить швидко. Для забезпечення такої можливості необхідно отримати інформацію про характер критичної ситуації, місце її виникнення, можливий час появи відповідної події. Очевидно, що в результаті прогнозування перераховані дані будуть неточними. Відповідна інформація передається в *SM* для того, щоб під час моніторингу можна було виявити критичну інформацію, після чого дані про критичну подію передає також у систему *SUB*, яка повинна протидіяти критичній події або її елімінувати на ранніх етапах розвитку, коли вона ще не встигла спричинити негативні зміни.

Оскільки *TPP* передбачає участь персоналу, то до його складу мають входити адміністратори системи, які повинні реагувати на ситуації, які є непередбачувані засобами автоматизації процесів виробництва та нормативними документами з втручання персоналу обслуги в технологічний процес. Така потреба зумовлена специфікою *TPP*, яка полягає в тому, що в рамках цього процесу використовуються фрагменти різної фізичної природи, які досить складно узгодити між собою засобами автоматизації [4]. Сьогодні здебільшого характерна відсутність у рамках систем прийняття рішень, які прийнято називати дорадчими або системами, що допомагають приймати рішення (*DSR*). Очевидно, що системи типу *DSR* необхідні в тому випадку, коли в *TPP* складаються нестандартні ситуації, які з різних причин було неможливо передбачити. Це означає, що в рамках самої системи DRS не існує правильного рішення, яке відповідало б нестандартній або нештатній ситуації. У цьому випадку обмежимося несправностями, що полягають у виявленні помилок у програмі. Для того щоб така ситуація в графі G могла виникнути, у ньому повинні існувати надмірні вершини і надмірні ребра. Ці вершини мають відображати стани системи, в які вона не повинна переходити, але фізично такий стан має бути можливим. Якщо деякий стан, що відповідає вершині e_i, є можливим, то до такої вершини щонайменше повинно входити хоча б одне ребро. Таке ребро є продовженням ланцюга, який належить до ланцюгів штатних режимів, оскільки в наступну ситуацію система може перейти тільки зі штатного режиму.

На логічному рівні вершина e_i приймає всі параметри з їх бінарною інтерпретацією, і логічна схема, яка описує логіку роботи фрагмента e_j, аналізує поточний стан логічної системи, що відповідає вершині [5]. Детальний опис функціонування цих рівнів моделей, що застосовуються в *ISU*, проводити не будемо, оскільки метою роботи є дослідження методів захисту процесу функціонування на основі уявлень про ризик $R(t)$, що виникають у системі управління *TPP*. Структурна схема загальної організації системи управління *TPP* зображена на рисунку. У ній використано оцінки ризиків, які виникають у системі управління.

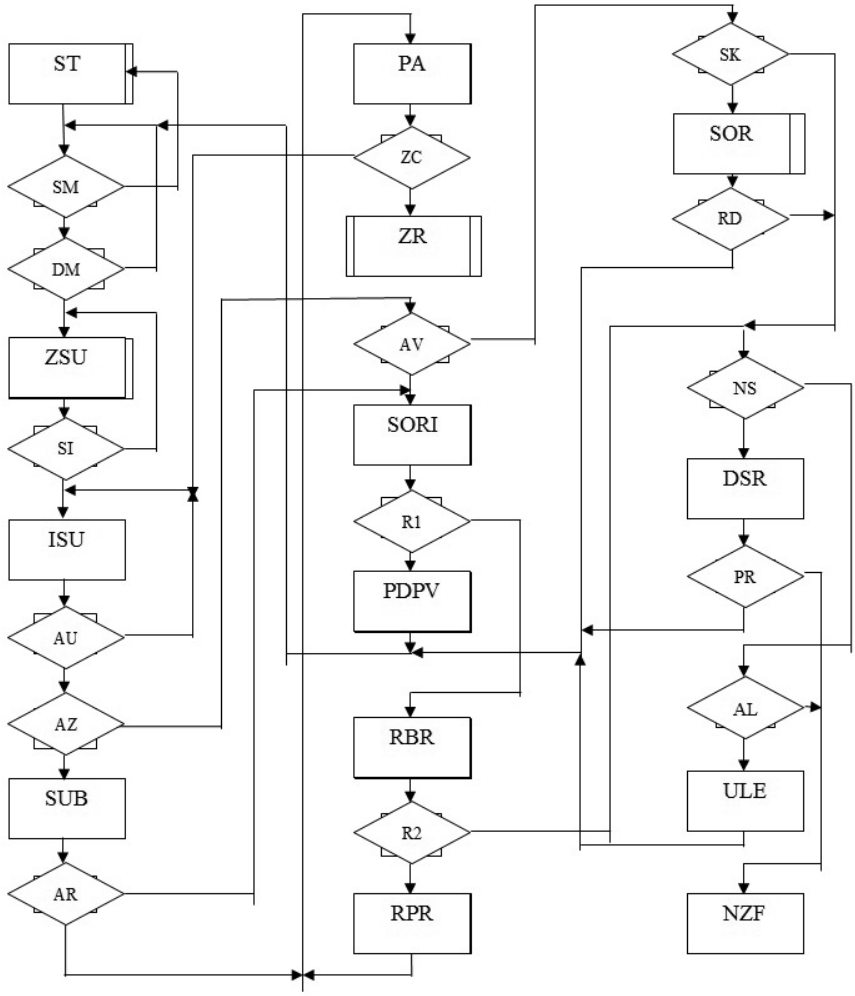

Рис. Структурна схема загальної організації системи управління *TPP* яка використовує оцінки ризику

У цій структурній схемі відображено окремі режими функціонування системи управління *TPP*. Схема відображає ті ситуації, які виникають у разі появи негативних факторів, що можуть зменшити рівень безпеки системи. На рисунку використано такі скорочення:

- *ST* — активізація загальної системи управління;
- *SM* — система моніторингу;
- *DM* — перевірка, чи встановлена дисципліна моніторингу;
- *ZSU* — загальна система управління;
- *SI* — перевірка, чи є система з найвищим пріоритетом;
- *ISU* — інформаційна система управління;
- *AU* — перевірка, чи в *ISU* є аномалії;

– *AZ* — перевірка, чи є атака зовнішньою;
– *SUB* — система управління безпекою;
– *AR* — перевірка, чи атака розпізнана;
– *PA* — активізація протидії атаці;
– *ZC* — перевірка, чи закінчився цикл *TPP*;
– *AV* — перевірка, чи атака внутрішня;
– *SOR1* — обчислення ризику виникнення внутрішніх подій;
– *R1* — ризик негативної дії, що відповідає одному параметру;
– *PDPV* — протидія внутрішній події, що зумовлює ризик;
– *RRP* — розширення розпізнаної події;
– *R2* — перевірка, чи ризик *R2* відрізняється від ризику *R1*;
– *RBR* — розширення модуля ризику *SOR*;
– *SK* — перевірка, чи ситуація є критична;
– *SOR* — система обчислення величини ризику;
– *RD* — перевірка, чи система *SOR* виявила ризиковану подію;
– *NS* — перевірка, чи виникла нестандартна ситуація;
– *DSK* — система, що допомагає прийняти рішення адміністратору системи;
– *PR* — перевірка, чи система прийняла рішення;
– *AL* — аналіз, чи негативний фактор є людським фактором;
– *ULF* — усунення дії на систему людського фактора;
– *ZR* — нормальне завершення роботи системи;
– *NZP* — некоректне завершення роботи системи.

Висновки. Побудована інформаційна модель загальної організації системи управління технологічним процесом з використанням оцінки ризику. Модель відображає окремі режими функціонування інформаційної системи, а також ситуації, що матимуть місце у разі появи негативних факторів, що зменшують рівень безпеки самої системи. В графових моделях ланцюг виходу системи з нештатного режиму повинен максимально складатися з ребер, які належать ланцюгам штатних режимів функціонування. Кожна вершина графу G структурної моделі відповідає окремій сукупності логічних функцій, що описують взаємозв'язки між параметрами деякого виділеного фрагмента системи. В рамках структурної моделі перехід з вершини e_i до вершини e_j зображає одне ребро v_{ij}, яке на логічному рівні відповідає передачі деякої сукупності параметрів, що є вихідними у фрагменті, зображеному вершиною e_i.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Проблемы полиграфии и издательского дела // Известия вузов. — 2002. — № 1/2. — С. 50–60.
2. Волкова Л. А. Издательско-полиграфическая техника и технология / Л. А. Волкова. — М. : МГУП «Мир Книги», 1999.
3. Техника флексографской печати : учеб. пособ. / пер. с нем. ; под ред. В. П. Митрофанова, Б. А. Сорокина. — М. : Изд-во МГУП, 2000.

4. Шаблій І. В. Стандартизація параметрів даних процесів поліграфічного виробництва / І. В. Шаблій, І. В. Піх // Квалілогія книги. — 2002. — Вип. 4. — С. 138–160.
5. Мендельсон Э. Введение в математическую логику / Э. Мендельсон. — М. : Наука, 1971.

REFERENCES

1. Problemy poligrafii i izdatelskogo dela. (2002). Izvestiya vuzov, 1/2, 50–60 (in Russian).
2. Volkova, L. A. (1999). Izdatelsko-poligraficheskaya tehnika i tehnologiya. Moscow: MGUP «Mir Knigi» (in Russian).
3. Mitrofanov, V. P., & Sorokin, B. A. (Eds.) (2000). Tehnika fleksograficheskoy pechati. Moscow: Izd-vo MGUP (in Russian).
4. Shablii, I. V., & Pikh, I. V. (2002). Standartyzatsiia parametriv danykh protsesiv polihrafichnoho vyrobnytstva // Kvalilohiia knyhy, vol. 4, 138–160 (in Ukrainian).
5. Mendelson, E. (1971). Vvedenie v matematicheskuyu logiku. Moscow: Nauka (in Russian).

ORGANISATION OF INFORMATION COMPLEX SECURITY SYSTEM OF PRINTING TECHNOLOGICAL PROCESS MANAGEMENT MANAGEMENT

T. M. Maiba

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

In general functioning of security complex of information management system it is necessary to provide components for the implementation of security process. The main ones are the management system of technological process, security system and risk assessment system. The basis of DRS decision making system is making the system recommendations. Such system is implemented at different levels of the model representation, describing the operation. The most common model is a structural one, which is a graph that describes different possible sequences of implementing the standard mode of the operation. The appearance of emergencies at this level is that the system as a whole on some standard operation mode enters into the top of the graph, from which there are no outgoing edges. If in the graph that displays the structure of the functioning, the management point gets to the top, which belongs to a different mode of operation, it means that there is a failure in the operation mode, which can be diagnosed. At the level of the model, DSR system realizes the construction of a chain, which would ensure the withdrawal process from the top e^t_i*, and this chain should consist of ribs belonging to the chains of the standard mode of the operation.*

Keywords: *methods of protection, information management system, monitoring system, forecasting system.*

Стаття надійшла до редакції 10.05.2016.
Received 10.05.2016.