УДК 004.056:004.7

С.В. СТАЙКУЦА
Одеська національна академія зв'язку ім.О.С.Попова

ДИНАМІЧНІ АСПЕКТИ ІНЦИДЕНТІВ ФІЗИЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ОХОРОНИ ОБ'ЄКТІВ

В статті розглядається динаміка інцидентів фізичної та інформаційної безпеки в конвергованих системах охорони об'єктів, підтверджено гіпотезу щодо її коливального характеру та розроблено модель «зловмисник-захисник» на основі моделі Лоткі – Волтерра. Отримані результати дозволяють підвищити ефективність роботи конвергованих систем інформаційної та фізичної безпеки та формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем інформаційної та фізичної безпеки конвергованих систем охорони об'єктів з використанням методів нелінійної динаміки.

Ключові слова: *інформаційна безпека, фізична безпека, система охорони об'єктів, конвергенція, нелінійна динаміка, інциденти.*

S.V. STAIKUCA
O.S. Popov Odessa national academy of telecommunications

DYNAMIC ASPECTS OF THE INCIDENT PHYSICAL AND INFORMATION SECURITY SYSTEMS OF OBJECTS

In the article the dynamics of incidents of physical and information security in convergent systems of objects, confirmed the hypothesis about its oscillatory nature of the model and the "attacker-defender" model-based Lotki – Volterra. The results allow to increase the efficiency of convergent information systems and physical security and formalize directions for further research to develop new effective information systems and physical security of convergent systems of objects using methods of nonlinear dynamics.

Keywords: information security, physical security, security systems of objects, convergence, nonlinear dynamics, incidents.

Вступ

Інформаційна та фізична безпека критично важливих інфраструктур держави, зокрема, систем охорони об'єктів, увійшла в число найбільш значимих задач науки і практики. Системи охорони об'єктів стали складними, автоматизованими та такими, що постійно вдосконалюються. Спостерігається процес уніфікації та конвергенції систем інформаційної безпеки та систем охорони об'єктів (технічних засобів охорони). Динамічний характер об'єктів захисту приводить до труднощів аналітичного описання систем інформаційної та фізичної безпеки. Методичною основою створення моделей динаміки кількості інцидентів безпеки можуть стати нелінійна динаміка та комп'ютерне моделювання. Основними математичними моделями в теорії захисту інформації, які з 90-х років минулого століття є «доказовою теоретичною базою для побудови сучасних систем захисту інформації» і класифікація яких дана в [1; § 4.4] на основі дискреційної політики безпеки, мандатної політики та моделей безпеки інформаційних потоків [2; § 3.3-3.5], ймовірнісних моделей. Популяризуються моделі, що внесені Юдіним О.К., Корченко О.Г. та Конаховичем Г.Ф. в узагальнені концепції побудови та структурні моделі організації систем безпеки [3; § 7.2-7.5].

В цілому моделі охоплюють функціональні аспекти, детермінований та, частково, стохастичний характер функціонування систем безпеки. Динамічні аспекти процесів, характерні для процесів різних видів безпеки та катастроф, розглядаються із застосуванням методів нелінійної динаміки у роботі колективу вчених за редакцією Малінецького Г.Г. [4].

Після робіт основоположників нелінійної динаміки (синергетики) Г. Хакена та І. Пригожина перелік літератури з цих питань став неоглядним. Багато дослідників відзначають застосовність методів нелінійної динаміки до вирішення задач у багатьох галузях на стику фізики й хімії, біології й екології, соціології й економіки, психології й управління. Що стосується досліджень загальної динаміки процесів забезпечення інформаційної та фізичної безпеки у складних конвергованих системах охорони об'єктів (КСОО), то таких досліджень поки що не достатньо.

Цілі та задачі дослідження

Метою даної роботи є підвищення ефективності розробки систем інформаційної та фізичної безпеки системи охорони об'єктів в умовах їх конвергенції за рахунок створення та аналізу моделей нелінійної динаміки інцидентів інформаційної та фізичної безпеки, застосовуючи методи моделей систем інформаційної безпеки.

Основна частина

Проведемо обґрунтування методики досліджень. Застосування методів нелінійної динаміки для моделювання процесів забезпечення інформаційної та фізичної безпеки надає ряд можливостей. Вдається звести змістовне описання об'єкта до двох – трьох диференційних рівнянь. «Хорошою рисою таких моделей ... являється наявність невеликого числа базових моделей, дослідження яких дозволяє ефективно будувати та вивчати великі класи моделей різноманітних явищ. ... Можна будувати вкрай прості нелінійні

математичні моделі, які являються глибокими і змістовними [5, с. 19; 6]». Система інформаційної та фізичної безпеки КСОО є відкритою не рівноважною системою тому, що вона активно обмінюється із своїм оточенням інформацією. Основним математичним апаратом є якісна теорія диференційних рівнянь. Синергетичний підхід та відповідні моделі можуть стати важливим елементом досліджень масштабних систем інформаційної та фізичної безпеки.

Слідуючи методики, яка викладена у [7], розглянемо однорідну мережу із K об'єктів. Нехай на кожному з об'єктів є L уразливостей. Так що у мережі, далі – системі, сумарно є

$$z = K \times L \tag{1}$$

уразливостей. «Візьмемо систему , яка складається із множини об'єктів захисту, які мають вразливості, із множини зловмисників, які створюють потік атак на систему, із множини працівників служби безпеки, які виявляють і протидіють атакам та ліквідують виявлені вразливості. Атака закінчується зломом системи, якщо у системі знаходиться хоча б одна із вразливостей, відповідно. Інтерес одного працівника служби безпеки полягає у відсутності зловмисників. Інтерес колективу працівників служби безпеки вимагає деякої малої кількості зловмисників для підтримки професійного рівня працівників. Повна відсутність зловмисників приводить до "віртуалізації" ролі служби безпеки на підприємстві та/або відсутності динаміки в рівні кваліфікації її співробітників. Інтерес "успішних" зловмисників полягає у тому, щоб було багато вразливостей (і працівників служби безпеки, бо число останніх свідчить про цінність інформаційних ресурсів, які захищаються). Задача працівників служби безпеки полягає у ліквідації вразливостей. Інтерес усієї системи вимагає підтримання мінімальної чисельності зловмисників, працівників служби безпеки і вразливостей. У такій постановці наша задача схожа на задачі, які вирішуються у класичній моделі «хижак - жертва». У біології ця модель вивчається з метою визначення умов, за яких підтримується екологічно рівноважна кількість взаємозалежних популяцій при заданих природних ресурсах та екологічної рівноваги. Представляє інтерес аналіз умов за яких мінімізується кількість уразливостей і, відповідно, атак [7]».

Проведемо конструювання моделі динамічних процесів інформаційної та фізичної безпеки. У сучасних версіях КСОО помилок, які призводять до вразливостей від атак, багато за об'єктивних причин. Розміри програмного коду стали настільки гігантськими, що повне тестування КСОО стало фактично неможливим за показниками часу і вартості. З моменту початку експлуатації КСОО число помилок у системі поступово зменшується. Помилки знаходять та виправляють проектувальники, розробники, вендори, служби підтримки, а також добросовісні користувачі. За помилками полюють зловмисники.

У моделі динамічних процесів інформаційної безпеки ресурсом будемо вважати вразливості системи інформаційної та фізичної безпеки, характеристикою яких буде загальне число вразливостей (незалежно від їх типу). Початкову кількість уразливостей можемо обчислювати за формулою $z = n \times N$, де n – кількість уразливостей в системі; N – кількість інсталяцій даної системи. Між зловмисниками та персоналом служби безпеки йде боротьба за кінчений ресурс. Зловмисники споживають ресурс-вразливості для здійснення атак. Служби безпеки виявляють атаки, аналізують вразливості й закривають або ліквідують ресурс-вразливості.

Система, що розглядається, є системою із запізнюванням. Запізнювання виникає внаслідок проведення роботи по аналізу атак: виділення характерних ознак атаки, виявлення та ліквідація вразливості тощо. Запізнювання виникає і як соціально-психологічне явище, наприклад, за необхідності навчання користувачів, фахівців та осіб, що приймають рішення. «Тут ми стикаємося з ефектом Касандри, про який майже завжди згадують очевидці найбільших лих – багато, а інколи й більшість людей на слідують застереженням, ігнорують попередження щодо небезпеки і завчасно не розпочинають ніяких заходів, які б допомогли їм врятуватись, див. [4, вступ, § 3; 7]». Тут мало знати закономірності, передбачати інциденти з безпекою, створювати механізми захисту. Треба домогтись, щоб це було зрозуміло людям і ними використано. Ще однією причиною запізнювання є прискорення зміни технологій і звикання до них.

У даному разі може постати питання, чи правомірний перехід до розгляду системи, а точніше до «колективу» об'єктів захисту, замість того, щоб надійно захистити кожен об'єкт окремо. Тоді, так здавалося б, що й загальна безпека буде забезпечена. Але стан інформаційної та фізичної безпеки сьогодні не дозволяє самостійно забезпечити надійний захист. Виявлення та протидія атакам на складну систему не під силу окремим її вузлам.

Оскільки загрози стали надходити від багатоелементної системи, то для аналізу систем протидії природним є використати методи синергетики або нелінійної динаміки. Саме синергетика як теорія сумісних дій, вивчає виникнення у складної системи, що складається із взаємодіючих елементів, нових властивостей, якими окремі елементи не володіють.

Історично першою найпростішою лінійною моделлю у цій області була модель народонаселення, запропонована у 1798 р. Т. Мальтусом,

$$\frac{dN}{dt} = \alpha N, \qquad N(0) = N_0, \qquad \alpha = const > 0. \tag{2}$$

Фізичний смисл моделі у тому, що швидкість росту населення, за відсутності стримуючих факторів або протидії, пропорційна чисельності населення N. Вирішенням цього рівняння є $N(t) = N_0 e^{\alpha t}$. Вирішення має сингулярність: $N(t) \to \infty$ при $t \to \infty$. Модель можна застосувати для описування росту

населення, біологічних вірусів, а також росту числа комп'ютерних вірусів в умовах, коли нема ніякого антивірусного захисту й віруси мають необмежений доступ до потрібних їм ресурсів середовища.

В реальних умовах є обмеження росту – або закінчуються ресурси, або вразливості знищуються, коли проти них ведеться боротьба. «У 1835 р. Л.А. Кетле і П.Ф. Ферхюльст, а в 1920 р. повторно Р. Пірл і Л.Д. Рід, відкрили, що чисельність виду N змінюється у відповідності з законом, який задається *логістичним рівнянням*

$$\dot{N} = r\left(1-\frac{N}{K}\right)N, \tag{3}$$

де K – середній розмір популяції;

N – чисельність популяції;

r – мальтузіанський коефіцієнт лінійного росту.

Середній розмір популяції – K залежить від ємності середовища, тобто від кількості їжі, розміру ареалу заселення. Логістичний закон добре описує динаміку росту простих біологічних і комп'ютерних вірусів, див. [4; глава 9, § 1.1]». Але логістичний закон не застосовний для моделювання більшості інших видів атак на КСОО, бо не враховує фактор запізнення.

Результати, отримані в нелінійній динаміці, дозволили сформулювати наступну гіпотезу. «*Довгострокові процеси забезпечення інформаційної безпеки, як і процеси у численних складних природних системах, можуть мати коливальний, циклічний характер і мають періоди зростання і спадання* [7]». Одним із механізмів коливальності пов'язаний з тим, що система забезпечення інформаційної та фізичної безпеки являється *системою із запізненням*. В них результат впливу позначається не відразу, а через певний час h – час запізнення. На вироблення заходів протидії та їх впровадження витрачається певний час. Для описування систем, що схильні до різких циклічних коливань «у 1948 р. Г.Хатчинсон запропонував наступне узагальнення рівняння (3):

$$\dot{N} = r\left(1-\frac{N(t-h)}{K}\right)N(t), \tag{4}$$

де h – час запізнення.

Введення додаткової постійної h — це спроба врахувати фактор запізнення. Рівняння описує наступну ситуацію: вид заселений у однорідному середовищі, міграційні фактори не суттєві, мається задана кількість їжі, яка відновлюється при зменшенні численності популяції, див. [4; гл.9, § 1.1, формула (3)]». Період коливальних процесів у системах із запізненням може бути значно більшим, ніж час запізнення. Для випадку, що розглядається у цій роботі, більш придатна модель «хижак - жертва». Існують численні добре вивчені модифікації цієї моделі. Задача зводиться до вибору модифікації моделі, удосконалення її та адекватної інтерпретації у термінах систем інформаційної та фізичної безпеки.

Із декількох різновидів моделі «хижак-жертва» оберемо як зразок модель Лоткі – Волтерра, удосконалений варіант якої описано та проаналізовано аналітично у [4, ; глава 9, § 5.1, а також використано у [7]. Покажемо, що цю модель можна удосконалити, перетворивши її у модель «зловмисник - захисник» в КСОО. Позначимо за x – кількість атак на систему, що виконуються зловмисниками, це аналог «жертв»; за y – кількість операцій, що виконуються захисниками КСОО, це аналог «хижаків»; за z – кількість уразливостей у системі, ця змінна характеризує «ресурси». Кількість вразливостей у комп'ютерах, які можуть бути атаковані, враховується у «ресурсах» за формулою (1). Середнє значення цих величин позначимо великими буквами, відповідно – X_c, Y_c, Z_c. Динаміка чисельності взаємодіючих популяцій захисника $x(t)$ та хижака $y(t)$ будемо моделювати системою рівнянь

$$\begin{cases} \dot{x}(t) = r_x\left[1+a\left(1-\dfrac{y(t)}{Y_c}\right)-\dfrac{x(t-h_x)}{X_c}\right]x(t) \\ \dot{y}(t) = r_y\left[\dfrac{x(t)}{X_c}-\dfrac{y(t-h_y)}{Y_c}\right]y(t) \end{cases}, \tag{5}$$

де r_x та r_y – мальтузіанські коефіцієнти росту;

h_x та h_y – середній час затримки, відповідно, аналізу (планування) атаки зловмисником й впровадження засобів протидії та пошуку вразливості захисником;

X_c та Y_c – середні кількості операцій для атак та з ліквідації атак, відповідно;

a – коефіцієнт тиску захисників на зловмисників, який визначає ефективне зменшення середньої кількості дій зловмисників за умови збільшення активності захисників (хижаків). Коефіцієнт тиску захисників на зловмисників – a визначає ефективне зменшення кількості операцій зловмисників по плануванню, підготовці та здійсненню атак. Його можна визначити неявним чином

$$X_c(a) = \frac{X_c(0)}{1+a}. \tag{6}$$

На практиці кількість вразливостей системи поступово зменшується внаслідок діяльності служби безпеки та вдосконалення теорії безпеки. Але часта зміна технологій і потік нових версій підвищують стрибкоподібно число вразливостей. Кількість вразливостей доводиться вважати поновлюваним ресурсом.

Проведемо аналіз цієї моделі при початкових умовах на інтервалі часу $\{-h_x...0\}$ від: $x(0)=1$, $y(0)=1$. Фізичний смисл моделі, яка представлена системою рівнянь (5), можна зрозуміти порівнявши її з іншими моделями. Так, якщо виключити члени, які описують взаємні зв'язки, система рівнянь розпадається. При цьому, якщо нема захисників $(a=0)$, то перше рівняння перетворюється на рівняння Хатчинсона (4). Якщо, крім того, виключити запізнення $(h_x=0)$, то маємо логістичне рівняння. А якщо, крім того, далі зняти самообмеження на ріст кількості атак $(X_c\to\infty)$, то перше рівняння стає рівнянням мальтузіанського росту. Якщо нема зловмисників $(x(t)=0)$, що важко собі уявити, та виключити фактор запізнювання, то із другого рівняння (5) отримаємо, що захисники поступово "вимирають", тобто їх кількість поступово зменшується. Якщо у моделі, тобто системі рівнянь (5), виключити запізнення з обох рівнянь $(h_x=0;h_y=0)$, то модель стає канонічною, яка ретельно проаналізована аналітично та чисельно, див. [5; глава 8, пример 1]. Модель із запізненням (5) досліджена значно менше. У [6; глава 4 та вправа 4.9] розроблена методика розрішення диференційних рівнянь із запізненням та надано приклад розрахунку для простої моделі «хижак-жертва», що схожа на модель (5).

Для спрощення моделі (5) при чисельному розрахунку зменшують кількість параметрів за допомогою заміни. Слідуючи [6; формули (3), (4)], робимо заміни: $t=h_x\tau$, $x(h_x\tau)=X_cN_1(\tau)$, $y(h_y\tau)=Y_cN_2(\tau)$ і далі, позначивши $\lambda_1=r_xh_x$, $\lambda_2=r_yh_y$, $h=h_y/h_x$, та перепозначивши τ через t, отримуємо

$$\begin{cases}\dot N_1(t)=\dfrac{\lambda_1}{1+a}\left[1+a\left(1-N_2(t)\right)-N_1(t-1)\right]N_1(t),\\ \dot N_2(t)=\lambda_2\left[N_1(t)-N_2(t-h)\right]N_2(t).\end{cases} \tag{7}$$

Для моделювання нами була використана програма проведення розрахунків за формулою (5), люб'язно наданою автором роботи [7]. Результати одного з відпрацювань моделі при $r_x=1.28$, $r_y=0.99$, $a=0.9$, $h_x=1$, $h_y=0.4$, $X_c=35$, $Y_c=25$, представлено на рис. 1.

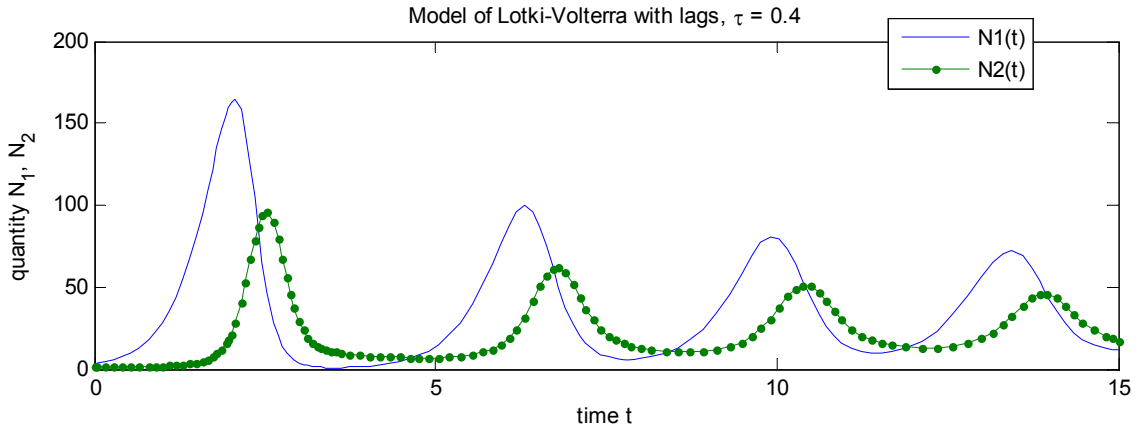

Рис. 1. Розрахунки моделі в середовищі MATLAB (Рисунок наведено з дозволу автора роботи [7])

До недоліків розглянутої моделі динаміки кількості інцидентів інформаційної та фізичної безпеки можна віднести її якісний характер.

Висновки

Запропонована у даній статті модель «зловмисник-захисник» на основі моделі Лоткі-Волтерра підтвердила гіпотезу щодо коливального характеру динаміки інцидентів інформаційної та фізичної безпеки у КСОО та дозволяє визначити напрямки подальших досліджень щодо розробки методів та побудови систем охорони об'єктів, а також створити концептуальні моделі попередження атак та формалізувати, на основі методів нелінійної динаміки, можливості превентивних систем для підвищення ефективності їх вибору й формулюванню вимог при їх проектуванні та розробки. Розроблена модель взаємовпливу порушника і захисника в КСОО дозволяє визначити сукупність заходів різного характеру для організації комплексної системи інформаційної та фізичної безпеки в КСОО. Вибір адекватної моделі та розрахунок її кількісних характеристик на основі експериментальної статистики й розробка прогнозу є метою подальшої роботи.

Література

1. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група ВНУ, 2009. – 608 с.
2. Богуш В.М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.
3. Юдін О.К. Захист інформації в мережах передачі даних / Юдін О.К., Корченко О.Г., Конахович Г.Ф. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.
4. Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. – М.: РАН, 2000. – 249 с. – Режим доступа: http://risk.keldysh.ru/risk/risk.htm.
5. Малинецкий Г.Г. Математические основы синергетики. Хаос, структура, вычислительный експеримент. – М.: КомКнига, 2005. – 312 с. (Синергетика : от прошлого к будущему).
6. Шампайн Л.Ф. Решение обыкновенных дифференциальных уравнений с использованием МАТЛАБ: Учебное пособие / Л.Ф. Шампайн, И. Гладвел, С. Томпсон. Пер. с англ. – СПб.: Издательство «Лань», 2009. – 304 с. (Учебники для вузов. Специальная литература).
7. Кононович І. В. Динаміка кількості інцидентів інформаційної безпеки / І.В. Кононович // Інформатика та математичні методи в моделюванні. – Одеса, 2014, Т. 3, № 3. – С. 35-43.

References

1. Hayvoronskyy M. V. Bezpeka informatsiyno-komunikatsiynykh system / M.V. Hayvorons□kyy, O.M. Novikov. – K.: Vydavnycha hrupa VNU, 2009. – 608 s.
2. Bohush V.M. Teoretychni osnovy zakhyshchenykh informatsiynykh tekhnolohiy: navch. posib. / V.M. Bohush, O.A. Dovyd□kov, V.H. Kryvutsa. – K.: DUIKT, 2010. – 454 s.
3. Yudin O.K. Zakhyst informatsiyi v merezhakh peredachi danykh / Yudin O.K., Korchenko O.H., Konakhovych H.F. – K.: Vyd-vo TOV «NVP»INTERSERVIS», 2009. – 716 s.
4. Upravleniye riskom / [Elektronnyy resurs] pod red. G.G. Malinetskogo. – M.: RAN, 2000. – 249 s. – Rezhim dostupa: http://risk.keldysh.ru/risk/risk.htm
5. Malinetskiy G.G. Matematicheskiye osnovy sinergetiki. Khaos, struktura, vychislitel'nyy yeksperiment. – M.: KomKniga, 2005. – 312 s. (Sinergetika : ot proshlogo k budushchemu)
6. Shampayn L.F. Resheniye obyknovennykh differentsial'nykh uravneniy s ispol'zovaniyem MATLAB: Uchebnoye posobiye / L.F. Shampayn, I. Gladvel, S. Tompson. Per. s angl. – SPb.: Izdatel'stvo «Lan'», 2009. – 304 s. (Uchebniki dlya vuzov. Spetsial'naya literatura).
7. Kononovych I. V. Dynamika kil□kosti intsydentiv informatsiynoyi bezpeky / I.V. Kononovych // Informatyka ta matematychni metody v modelyuvanni. – Odesa, 2014, T. 3, № 3. – S. 35-43.

Рецензія/Peer review : 15.1.2015 р. Надрукована/Printed :24.1.2015 р.
Стаття рецензована редакційною колегією

УДК 681.518:667.6

О.О. КОВАЛЮК
Вінницький національний технічний університет
Д.О. КОВАЛЮК, П.М. ЧУБАРОВ
Національний технічний університет Україна «Київський політехнічний інститут»

КЕРУВАННЯ ПОЛІМЕРИЗАЦІЙНОЮ КОЛОНОЮ ПРИ ВИРОБНИЦТВІ РІЗНИХ МАРОК ПРОДУКТУ

У статті розглядається керування полімеризаційною колоною для отримання заданої марки продукції. Проаналізовано полімеризаційну колону як об'єкт автоматизації. Запропоновано структурну схему системи керування та описано алгоритм її роботи. Наведено постановку задач для реалізації системи керування.

Ключові слова:система керування, алгоритм керування, полімеризаційна колона, прогнозування, клас якості.

O.O. KOVALIUK
Vinnytsia National Technical University
D.O. KOVALIUK, P.M. CHUBAROV
National Technical University of Ukraine "Kyiv Polytechnic Institute"

CONTROL OF POLYMERIZATION COLUMN OF THE VARIOUS PRODUCT BRANDS PRODUCTION

The paper presents the control of polymerization column of the various product brands production. The polymerization column is analyzed. A block diagram of the control system is proposed and the algorithm of its work is described. List of tasks for the implementation of the control system is shown.

Key words: control system, control algorithm, polymerization column, forecasting, quality class.

Вступ

Полістирол є важливою складовою промислового виробництва. З полістиролів виробляють широку гаму виробів, які в першу чергу застосовуються в побутовій сфері (одноразовий посуд, упаковка, дитячі