де: $П$ – множина позицій; $П_р$ – множина переходів; $Р_б$ – множина вхідних та вихідних дуг; $М$ – множина маркерів. Отже, розроблена модель записана в математичній формі та дає змогу дослідити динаміку системи (у цьому випадку процес усунення ударів і вібрацій під час буріння). Для прикладу, на рис. 3 наведено схемну форму подання моделі (2) для алгоритму на рис. 2, а на рис. 4 показано граф досяжності станів [10], який дає змогу дослідити динаміку процесу використання параметрів режиму буріння – з бази знань.

Висновок. Розроблено метод автоматичного усунення ударів і вібрацій, що ґрунтується на знаннях експертів і основних методах усунення ударів і рішеннями, які застосовують на сьогодні інженери з буріння. Він охоплює варіації навантаження на долото та швидкості обертання бурової колони. Результат "успішності" заноситься в базу знань системи підтримки та прийняття рішень, завдяки чому при наступному усуненню ударів і вібрацій система може запропонувати більш швидке та ефективне рішення.

Література

1. Маляр А.В. Системи автоматизованого керування й моніторингу процесом видобування нафти : монографія / А.В. Маляр, Б.С. Калужний. – Львів : Вид-во НУ "Львівська політехніка", 2012. – 272 с.
2. Bommer P. A primer of oilwell drilling: a basic text of oil and gas drilling // 7-th ed. University of Texas, Austin, 2008. – Pp. 135-138.
3. Матвійків Т.М. Комп'ютерне моделювання промиву бурової колони / Т.М. Матвійків, В.М. Теслюк, А.Є. Струк, Р.В. Загарюк // Збірник наукових праць ППМЕ ім. Г.Є. Пухова НАН України. – 2012. – № 63. – С. 111-118.
4. Теслюк В.М. Формалізована інтегральна оцінка ресурсу роботи та ризику поломки бурових телеметричних систем / В.М. Теслюк, Т.М. Матвійків // Вісник Національного університету "Львівська політехніка". – Сер.: Сучасні досягнення геодезичної науки та виробництва. – Львів : Вид-во НУ "Львівська політехніка". – 2011. – № 705. – С. 19-21.
5. Matviykiv T.M. Use of influence diagrams for decision support in drilling automation / T.M. Matviykiv, V.M. Teslyuk // Journal of Global Research in Computer Science (JGRCS). – India, 2013. – Vol. 4, No. 4 (April). – Pp. 1-7.
6. Breyholtz O. Drilling Automation: Presenting a Framework for Automated Operations / O. Breyholtz, M. Nikolaou // SPE Drilling & Completion, March, 2012. – Vol. 27, Number 1. – Pp. 118-126.
7. Baik H.S. Decision support system for horizontal directional drilling / H.S. Baik, D.M. Abraham, S. Gokhale // Tunelling and Undrgraund Space technology, 2003. – Pp. 99-109.
8. Оре О. Теория графов / О. Оре. – Изд. 2-ое, [перераб. и доп.]. – М. : Изд-во "Наука", Гл. ред. физ.-мат. лит., 1990. – 384 с.
9. Теслюк В.М. Застосування мереж Петрі при проектуванні МЕМС на системному рівні / В.М. Теслюк // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи проектування: теорія і практика. – Львів : Вид-во НУ "Львівська політехніка". – 2006. – № 564. – С. 45-53.
10. Teslyuk V. Developing The Information Model Of The Reachability Graph / V. Teslyuk, P. Denysyuk, Hamza Ali Yousef Al Shawabkeh, A. Kernytskyy // Proc. of the XVth International Seminar / Workshop Of Direct And Inverse Problems Of Electromagnetic And Acoustic Wave Theory (DIPED – 2010). – Tbilisi, Georgia, 2010. – Pp. 210-214.

Матвийкив Т.М., Теслюк В.Н. **Метод автоматического устранения ударов и вибраций при бурении**

Разработан метод автоматического устранения ударов и вибраций в наклонно-управляемом бурении. Разработанный метод основывается на построенных алгоритмах, которые учитывают знания экспертов, существующие методы устранения ударов и вибраций, а также существующие решения подобных ситуаций, которые обеспечивают, при последующем устранении ударов и вибраций, получить решение быстрее и эффективнее. При этом построены модели исследования динамики процесса устранения ударов и вибраций. Разработанные модели базируются на теории сетей Петри и дают возможность исследовать динамику процесса автоматического устранения ударов и вибраций в наклонно-управляемом бурении.

Ключевые слова: метод, удары и вибрации, алгоритм, модель на основании сетей Петри, наклонно управляемое бурение.

Matviykiv T.M., Teslyuk V.M. **Decision Support System for Shocks and Vibrations Mitigation in Directional Drilling**

The development of decision-support system (DSS) for shocks and vibration mitigation in downhole directional drilling is described. System architecture, operation algorithm and schematic diagram design are focused on. The DSS incorporates real-time databases, rule-based and expert knowledge databases. During the design process, we use Bayesian Networks modeling for expert knowledge implementation. The proposed system works in an advisor mode. It can be used in downhole directional drilling of oilfield wells with modern MWD-, LWD-, RSS-systems.

Keywords: DSS, downhole directional drilling, shocks and vibrations, database, knowledge base.

УДК 004.[056+3.75]:061.68

Ст. викл. І.Р. Опірський, канд. техн. наук – НУ "Львівська політехніка"

КЛАСИФІКАЦІЯ МОДЕЛЕЙ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

Запропоновано і представлено ознаки для визначення об'єктів під час дослідження моделей захисту, такі як: способи реалізації моделей, характер процесів і явищ, які відбуваються у системі, характер підходу до моделювання об'єкта, призначення й специфіка об'єктів дослідження, ступінь узагальнення характеристик об'єктів дослідження, які узагальнюються. Представлено класифікацію моделей захисту інформації в інформаційних мережах держави. На основі класифікації моделей захисту наведено структурну модель моделей захисту за таким поділом: за способом реалізації, за характером процесів у системі, за характером підходу до моделювання об'єкта, за призначенням об'єктів дослідження, за характеристиками досліджуваного об'єкта.

Ключові слова: модель захисту інформації, інформаційні мережі держави, абстрактні моделі, захист інформації, математичні моделі, модель політики безпеки.

Вступ. Моделі захисту інформації є складовими частинами загального процесу моделювання. Моделювання системи полягає у побудові образу системи, адекватного з точністю до цілей моделювання системи, яка проектується, і в отриманні за допомогою побудованої моделі потрібних характеристик реальної системи. Отже, у загальному випадку весь процес моделювання можна поділити на дві складові частини: побудова моделі; реалізація моделі з метою отримання потрібних характеристик системи.

Основне призначення моделей – це створення умов для об'єктивної оцінки загального стану інформаційної системи з точки зору міри уразливості або рівня захищеності інформації в неї. Потреба в таких оцінках, зазвичай, виникає під час аналізу загальної ситуації, з метою відпрацювання стратегічних рішень під час організації захисту інформації.

Створення сучасних систем інформаційної безпеки, зокрема на рівні корпоративних мереж зв'язку, які є провідними у сучасній інфраструктурі фун-

кціонування суспільства, ґрунтується на комплексному підході, що охоплює принципи системного аналізу предметної сфери. Структура комплексного підходу орієнтована на створення захищеного середовища оброблення інформації на основі методів і засобів протидії відповідним загрозам. Методологічною основою комплексного підходу є: законодавчі, нормативно-правові, морально-етичні, організаційні, апаратно-програмні способи функціонального забезпечення інформаційної безпеки цифрових систем, каналів, мереж зв'язку.

Практичному створенню систем захисту інформації передує етап розроблення ряду моделей для оцінювання об'єктивних реальностей: загроз інформаційної безпеки, можливого порушника, моделі побудови й функціонування системи захисту. Відповідно до визначення наукової філософії, модель – деякий матеріальний або інший об'єкт, що є спрощеною версією об'єкта, що моделюється, або явища (прототипу) і в достатньому ступені повторює властивості, істотні для цілей конкретного моделювання.

Застосування моделей, як спрощених описів важливих компонентів системи, дає змогу спростити розв'язок завдання створення адекватної реальним загрозам системи захисту, розбити цей процес на ряд етапів, провести попереднє дослідження, зокрема із застосуванням комп'ютерної техніки, можливих варіантів побудови систем захисту, вивчити на моделі поведінки системи захисту в різних ситуаціях.

Аналіз моделей захисту та перенесення їх на конкретну структуру програмних засобів, операційних систем, системи управління базами даних та на автоматизовану систему загалом здійснюють на етапі проектування та техно-робочому етапі створення систем захисту.

Об'єкт дослідження – моделі захисту інформації в інформаційних мережах держави.

Предмет дослідження – аналіз та дослідження моделей захисту інформації.

Мета роботи – проведення аналітичного аналізу та дослідження моделей, що можуть бути використані або використовуються для захисту інформації в інформаційних мережах держави і на основі цього провести їхню структуризацію та класифікацію.

Виклад основного матеріалу. Системну класифікацію моделей в наступний час привести практично неможливо, оскільки з точки зору малого числа таких моделей для цього нема достатніх даних. Тому запропонуємо спрощену класифікацію моделей захисту інформації, яку зображено на рисунку. Але оскільки загальною ознакою будь-яких моделей є їх спроможність відображати головні для цілей дослідження признаки об'єктів, які досліджуються, то найбільш відомими ознаками будуть:

1. Способи реалізації моделей.
2. Характер процесів і явищ, які відбуваються у системі.
3. Характер підходу до моделювання об'єкта.
4. Призначення й специфіка об'єктів дослідження.
5. Ступінь узагальнення характеристик об'єктів дослідження, які узагальнюються.

Ці ознаки покладено в основу пропонованої класифікації. За способом реалізації моделі захисту інформації можуть бути абстрактними, матеріальними (предметними, реальними) або змішаними (матеріально-абстрактними). Побудова абстрактних моделей у кількох випадках є єдино можливим способом моделювання захисту інформації у складних системах. Такі моделі можуть бути реалізовані в математичній, словарній, зразковій і графічній формах.

Для абстрактних (моделей мислення) моделей природа матеріального не має принципового значення. Математичні моделі, в яких елементи, відношення та параметри систем, які моделюються, або явищ відображаються за допомогою різних математичних засобів, можуть бути представлені в аналітичній або алгоритмічній формах. Формули, рівняння, матриці, графи, алгоритми і програми – все це математичні моделі.

Аналітичну форму застосовують у ситуації, коли залежність між змінними, які характеризують модель, описується математичними виразами або сукупністю таких виразів. Дослідження з використанням аналітичної моделі можна проводити одним з таких способів:

- аналітично, коли отримують у загальному вигляді явні залежності вихідних змінних величин моделі від вхідних даних;
- чисельно, коли нема змоги отримати явні залежності в загальному вигляді, але можливо порахувати значення вихідних змінних даних за заданих параметрів моделі і конкретних значень вхідних величин;
- якісно, коли, не отримуючи рішення в явному вигляді, роблять висновок про параметри процесу, який моделюється, який описаний математичним виразом;
- рішення на основі аналітичних моделей може бути отримано внаслідок однократного розрахунку за формульними або логічними залежностями незалежно від конкретних значень характеристик (у загальному вигляді). Такий підхід зручний для виявлення закономірностей і при цьому має таку перевагу як наочність.
- алгоритмічна форма пропонує представлення моделі у вигляді алгоритму або програми. Алгоритмічні моделі (які потрібно відрізняти від алгоритмів розрахунку аналітичних моделей за їх чисельного дослідження), як правило, не можуть бути представлені еквівалентними формулами. Характерна особливість таких моделей полягає також у тому, що послідовність кроків їх розрахунку на комп'ютері відповідає поведінці системи, яка моделюється, тобто імітує її. Тому в літературі [3] набув поширення термін "Імітаційна модель".

Словесна модель – логічний об'єкт, який відображає властивості оригіналу за допомогою визначеної системи знаків або символів. Її різновидом є вербальна модель, яка надається у вигляді тексту на звичайній мові.

До образних відносять моделі, які конструюються з поглядово-чуттєвих елементів, що відображають визначені властивості у поведінці об'єкта. Різновидом таких моделей є гіпотетичні моделі та макети уяви. В основі перших лежить гіпотеза про процеси, які відбуваються у системі. Під час макетування на основі вивчення причинно-наслідкових зв'язків, які існують у системі, утворюється уявний образ – макет, функціонування якого тотожно відображає явища та процеси в оригіналі. Такі моделі використовуються на ранньому етапі проектування систем захисту інформації.

До графічних моделей відносять номограми, креслення, графіки і діаграми, які відображають співвідношення параметрів системи і дають змогу прог-

нозувати змінні останніх. Матеріальні моделі захисту інформації ґрунтуються на застосуванні моделей, які уявляють собою технічні конструкції. Вони можуть бути натурними або фізичними.

Натурні моделі припускають поведінку досліджень на реальному об'єкті, дозволяючи піддати його – відповідно до задуму дослідника – визначеним впливам. Результати експериментів подібного роду мають, як правило, високий ступінь достовірності і дають змогу виявляти закономірності та особливості перебігу реального процесу в системі, яка функціонує залежно від поставленої мети. До натурних моделей можна віднести стенди, на яких відповідні системи досліджуються в різних (зокрема, екстремальних) умовах, а також аналогічне обладнання для комплексних випробувань.

Рис. Класифікація моделей захисту інформації

Явища та процеси, які відбуваються у системі, можуть також досліджуватися на спеціально підібраних або утворених для цієї мети фізичних моделях – технічних пристроях, які відображають явища, наприклад, природи, і явища, які моделюються. Різновидом таких моделей є фізично подібні, які характеризуються однаковими фізичними процесами в об'єкті і моделі.

Змішані моделі – це з'єднання знакових форм виразу процесів і явищ з матеріальними моделями. Для тієї частини операції, яку неможливо описати за допомогою математичного апарату, використовують матеріальну модель, тоді як інше моделюється у знаковій формі. У цьому випадку йдеться про матеріально-знакову модель. До змішаних моделей відносять також напівнатурні моделі, сутність яких полягає в тому, що в загальну модель разом з математичними (аналітичними або алгоритмічними) моделями будь-яких систем, включається реальна апаратурна частина системи, яка моделюється.

Відповідно до характеру процесів, які відбуваються у системі, моделі можна поділити на детерміновані та стохастичні, статистичні та динамічні, а також дискретні, безперервні та дискретно-безперервні. Детерміновані моделі відображають процеси, в яких відсутні випадкові впливи, а стохастичні – ймовірнісні процеси. Статистичні моделі використовують для опису поведінки об'єкта в будь-який окремий момент, тоді як динамічні призначені для опису його поведінки за часом. Дискретні та безперервні моделі дають змогу описати процеси в системах, що відповідно не мають і мають такий параметр, як безперервність, а дискретно-безперервні моделі застосовують для дослідження систем, в яких відбуваються як безперервні, так і дискретні процеси.

За характером підходу до моделювання об'єкта розрізняють структурні та функціональні моделі. Під структурною моделлю розуміють опис структури об'єкта загалом. Функціональні моделі, які іноді мають назву кібернетичні, в жодному разі не претендують на фізичну або структурну подібність оригіналу: з погляду структури досліджуваний об'єкт розглядається як "чорний ящик". У спрощеному вигляді методику утворення кібернетичної моделі можна описати таким чином. Наглядаючи за реакціями системи на зовнішні впливи, підбирають математичну модель, яка подібним же чином "відкликається" на зовнішні впливи на оригінал, встановлюючи таким чином аналогію поведінки об'єкта та математичної моделі.

За призначенням і специфікою об'єкта дослідження розрізняють моделі загроз, моделі порушника, моделі політики інформаційної безпеки, моделі процесу захисту інформації, моделі систем захисту інформації, моделі систем розгородження доступу до ресурсів об'єкта.

Модель загроз – це формалізований або неформалізований опис методів і засобів здійснення загроз. Модель порушника – формалізований або неформалізований опис відповідних характеристик і поведінки порушника.

Модель політики інформаційної безпеки – формалізований або неформалізований опис відповідної політики, під якою розуміють сукупність законів, правил, обмежень, рекомендацій, інструкцій та інших нормативних актів, які регламентують порядок оброблення інформації.

Модель процесу захисту інформації відображає взаємодію між дестабілізаційними факторами, які впливають на інформацію, і протидіючими засобами захисту інформації, завершенням якого є визначений (більш або менш високий) рівень захищеності інформації. Модель системи захисту інформації повинна відображати основні процеси, які відбуваються в цій системі з метою оптимізації

процесів захисту інформації. Такі процеси в загальному вигляді можуть бути представлені як процеси розподілу і використання ресурсів, які виділяються на захист інформації.

Моделі систем розгородження доступу до ресурсів захищуваного об'єкта застосовують для розв'язку задач аналізу та синтезу систем (механізмів) розгородження доступу до різного виду ресурсів об'єкта, насамперед до масивів даних або полів пристроїв запам'ятовування комп'ютерних систем. Виділення цих моделей до самостійного класу моделей зумовлено тим, що механізми розгородження доступу відносять до найважливіших компонентів систем захисту інформації, від ефективності функціонування яких значною мірою залежить загальна ефективність захисту інформації.

За ступенем узагальнення характеристик об'єкта дослідження моделі поділяють на загальні, часткові та локальні. До категорії загальних відносять моделі, які дають змогу визначити (оцінити) загальні характеристики відповідних систем і процесів, на відміну від часткових і локальних моделей, які забезпечують визначення (оцінку) будь-яких часткових або локальних характеристик системи або процесів. Тут не треба путати загальні моделі зі структурними, а локальні і часткові – з функціональними.

Висновки. У роботі на основі представлених ознак для визначення об'єктів під час дослідження моделей захисту, таких як: способи реалізації моделей, характер процесів і явищ, які відбуваються у системі, характер підходу до моделювання об'єкта, призначення й специфіка об'єктів дослідження, ступінь узагальнення характеристик об'єктів дослідження, які узагальнюються, представлено класифікацію моделей захисту інформації в інформаційних мережах держави. На основі запропонованої класифікації моделей захисту наведено структурну модель моделей захисту за таким поділом: за способом реалізації, за характером процесів в системі, за характером підходу до моделювання об'єкта, за призначенням об'єктів дослідження, за характеристиками досліджуваного об'єкта. Отримані результати можуть застосовувати спеціалісти у сфері захисту інформації під час проектування та визначення моделей для захисту інформаційних мереж держави.

Література

1. Михайлов С.Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции / С.Ф. Михайлов, В.А. Петров, Ю.А. Тимофеев. – М. : Изд-во "Связь", 1995. – 56 с.

2. Голубенко О.Л. Політика інформаційної безпеки / О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань, Ю.Є. Яремчук. – Луганськ : Вид-во СНІ ім. В. Даля. – 2009. – 300 с.

3. Єжова Л.Ф. Управління інформаційною безпекою / Л.Ф. Єжова, І.О. Мачалін, Я.В. Невойт, В.О. Хорошко. – В 2-х т. – К. : Вид-во ДУІКТ, 2011. – 236 с.

4. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк. – М. : Изд-во "Высш. шк.", 2004. – 280 с.

5. Щеглов А.Ю. Защита компьютерной безопасности от несанкционированного доступа / А.Ю. Щеглов. – СПб. : Изд-во "Наука", 2004. – 384 с.

6. Згуровський М.З. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова – К. : Вид. дім ВНУ, 2007. – 544 с.

7. Козлова К.В. Кількісна оцінка захисту радіоелектронних об'єктів / К.В. Козлова, В.О. Хорошко // Захист інформації : зб. наук. праць. – 2007. – № 1. – С. 30-32.

Опирский И.Р. **Классификация моделей защиты информации в информационных сетях государства**

Предложены и представлены признаки для определения объектов при исследовании моделей защиты, такие как: способы реализации моделей, характер процессов и явлений, протекающих в системе, характер подхода к моделированию объекта, назначение и специфика объектов исследования, степень обобщения характеристик объектов исследования, что обобщаются. Представлена классификация моделей защиты информации в информационных сетях государства. На основе классификации моделей защиты приведена структурная модель моделей защиты по таким параметрам: по способу реализации, по характеру процессов в системе, по характеру подхода к моделированию объекта, по назначению объектов исследования, по характеристикам исследуемого объекта.

Ключевые слова: модель защиты информации, информационные сети государства, абстрактные модели, защита информации, математические модели, модель политики безопасности.

Opirsky I.R. **Classification Models of Information Security in Information Networks of the State**

Some signs to identify objects in the study of patterns of protection are proposed. They are the following: ways to implement the models, the nature of the processes and phenomena occurring in the system, the nature of the object modeling approach, purpose and specific objects of study, the degree of generalization of the characteristics of objects of study. The classification of models of information security in information networks of the state is provided. On the basis of the classification models of protection, a structural model of security models was given on such parameters as the method of implementation, the nature of the processes in the system, the nature of the object modeling approach, intended objects of study, the characteristics of the object under study.

Keywords: model of information security, information networks of the state, abstract models, data protection, mathematical models, model of security policy.

УДК 674.058.6 ***Ст. викл. І.З. Пилипів – НЛТУ України, м. Львів***

МАТЕМАТИЧНИЙ ОПИС ПРОЦЕСУ ГНУТТЯ КРИВОЛІНІЙНИХ ЕЛЕМЕНТІВ ІЗ ДЕРЕВОВОЛОКНИСТИХ ПЛИТ

Наведено приклади застосування криволінійних меблевих елементів із деревоволокнистих плит (ДВП). Внаслідок проведення теоретико-експериментальних досліджень встановлено зусилля для гнуття ДВП залежно від їх геометричних характеристик. Проведено математичний опис процесу гнуття на основі теоретичних положень напружено-деформованого та гранично рівноважного станів ДВП. Отримано математичну модель, яка дає змогу прогнозувати значення стискальної сили для виготовлення гнутих криволінійних елементів з мінімальною кількістю браку або відходів унаслідок руйнування.

Ключові слова: деревоволокниста плита, гнуття, криволінійний елемент критична сила, метод апроксимації.

Вступ. На сучасному етапі в багатьох меблевих виробах широко використовують криволінійні меблеві елементи. Для їх виготовлення застосовують деревину, шпон, різні композитні матеріали, а також деревоволокнисті плити (ДВП) (рис. 1). Якщо гнуті елементи у меблевих виробах із деревини виготовляли ще в далекі минулі часи, а із клеєних пакетів шпону, відколи людство навчилося стругати шпон, то процес виготовлення таких елементів на основі ДВП є новим і недостатньо вивченим [1-3]. Задачею дослідження є математичний