Ключові слова: автентифікація, криптографічний протокол, криптосистема з відкритим ключем, шифрування, шифртекст.
Ключевые слова: аутентификация, криптографический протокол, криптосистема с открытым ключом, шифрования, шифртекст.
Keywords: authentication, cryptographic protocol, public key cryptosystem, encryption, ciphertext.

Баландіна Наталія Миколаївна
Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки

Василенко Микола Дмитрович
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

ДЕЯКІ НОТАТКИ ЩОДО МАТЕМАТИЧНИХ МОЖЛИВОСТЕЙ В МОДЕЛЮВАННІ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасний стан захисту інформації посприяв розвитку досліджень, які пов'язані з інтелектуалізацією обчислень в галузі підтримки прийняття рішень в кібербезпеці та в захисті інформації в цілому для різних інформаційних систем і технологій. Сьогодні продовжують розроблятися нові методи та моделі для підтримки прийняття рішень щодо вибору і реалізації стратегії захисту інформаційних процесів. В роботі наведено спробу встановлення деяких реальних дій обмежень в питанні математичних можливостей при моделюванні захисту інформації. Очевидно, що моделі захисту інформації являють собою складову частину загального процесу моделювання. І тут моделювання системи полягає у побудові образу системи, адекватного з точністю до цілей моделювання системи, яка проєктується, і в отриманні за допомогою побудованої моделі потрібних характеристик реальної системи з метою побудови захисту. Оскільки інформаційні системи змінюються

в часі та мають зміни в середовищі, наприклад в умовах КОВІД-19, треба користуватися динамічними моделями для нелінійних систем, а як добре відомо, що модель представляє собою теж систему, то, безумовно, модель може бути також нелінійною. Формально нелінійність моделі може бути виражена у структурі рівнянь, що використовуються, а знаходження їхніх розв'язків, щонайменше, у чисельному вигляді, в деяких випадках може бути цілком здійсненною задачею. Основну увагу при побудові нелінійних конкурентних моделей нині приділяють аналізові принципових внутрішніх взаємодій динамічних систем на основі логістичних моделей. Моделювання динаміки розвитку на основі диференціальних логістичних рівнянь широко використовується для моделювання найрізноманітніших як природних, так і соціальних процесів. Відзначимо, що при цьому в загальному випадку весь процес моделювання можна поділити на дві складові частини: побудова моделі та реалізація моделі з метою отримання потрібних характеристик системи.

В загальному вигляді основне призначення моделей визначається як 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, яка відносить ще й до складних систем. Найчастіше для моделювання складних систем застосовують диференціальні рівняння, які описують динаміку зміни станів таких систем. Як правило, це система рівнянь першого порядку, що має вигляд, представлений в [1].

Створення сучасних систем інформаційної безпеки на практиці може задовольнятися трьома формальними методами побудови моделей: кібернетичним підходом, системною динамікою та теоретично-множинним підходом. Сучасні технології роботи з великими даними майже завжди потребують створення математичних можливостей, що визначають

процес пошуку та оброблення інформації. Навіть при дотриманні усіх основних принципів побудови моделей (інформаційної достатності, доцільності, здійсненності, множинності моделей, агрегації, параметризації, із застосуванням методології інтеграційного (багаторівневого) моделювання важко досягти бажаних результатів. В результаті розробники практично завжди пропонують програмні продукти, які мають велику кількість уразливостей. Це дозволяє зловмисникам будувати складні алгоритми атак, що можуть досягати своєї мети різними способами, в залежності від ситуації в кіберпросторі. На практиці для реалізації атак у мережному середовищі зазвичай використовуються троянські програми, кінцевою метою яких є впровадження у програмний код атакованої системи додаткових прихованих функцій. Негараздом є те, що зазвичай факт втручання може бути виявлений вже після здійснення атаки. При цьому такі несанкціоновані втручання до інформаційної системи не мають чітко визначеної часової закономірності, а їх тривалість є недостатньою для належного реагування. Таким чином, задача полягає у створенні такої стратегії боротьби, яка б дозволяла визначати зловмисні дії вже на перших кроках реалізації кібератак. Однією з умов створення ефективної системи захисту стає володіння інформацією про всі слабкі місця кібератаки, а також розуміння формальних моделей організації сучасних атак у середовищі експлуатації інформаційних систем. І самі моделі, і визначення переліку уразливостей ґрунтується на постійному моніторингу можливих джерел загроз, з точки зору їх мотивів та наявності ресурсів для реалізації цих загроз, а також аудиту системи захисту на наявність у ній уразливостей. Відповіді на ці питання дає використання «ромбоподібної» моделі, яка наведена у [2]. Саме вона породжує ланцюжок «кібервбивств». Відповідно до результатів [2] зловмисник атакує інформаційний ресурс, керуючись своїми мотивами, а не планом вторгнення. Ця модель враховує чотири основних елементи: супротивника і його ресурси, інфраструктуру,

здатність до нападу і ціль. Для прогнозування дій порушника найчастіше використовується модель послідовних вторгнень [3]. Порушник крок за кроком виконує спроби подолання системи захисту, намагаючись подолати механізми захисту через уразливості там, де він їх знаходить. Основними елементами моделі послідовних вторгнень є індикатори, під якими розуміється будь-яка інформація, що об'єктивно описує кожний етап вторгнення. Отже, послідовність вторгнення включає сім етапів: розвідку, озброєння, доставлення, виконання, створення «чорного входу», установка таємного каналу і зловмисні дії щодо об'єкта атаки. Попри тип обраної моделі атак, автоматизація процесів протидії нападу на інформаційну систему з боку зовнішнього кібернетичного середовища передбачає створення досить складного програмного коду. Ця робота зазвичай розпочинається із розроблення великої кількості формальних алгоритмів, що потребує використання усталеного математичного апарату. Саме через це, ще на початку розвитку мережного середовища, коли атаки на інформацію були досить простими, для визначення їх архітектури використовували графові моделі [4]. Графи атак являють собою концептуальні діаграми і використовуються для аналізу можливих шляхів реалізації конкретної загрози, які структурно вони представляють собою багаторівневі деревоподібні структури, що мають дочірні елементи з одним коренем. У випадку опису сучасної атаки вони мають тисячі вузлів і шляхів подолання механізмів захисту. Тому генерація графів для атак у складних мережах є дуже складною в обчислювальному сенсі. На основі проведеного аналізу наявних моделей реалізації мережних атак можна зазначити, що перевага має надаватись таким, які дозволяють, по-перше, оцінити вірогідність нападу з боку можливих джерел загроз, по-друге, визначити стратегію розпізнавання атаки на початку спроби її реалізації порушником безпеки. Модель повинна легко піддаватись формальному опису для подальшого її використання у процедурах автоматизації управління захистом.

Список використаних джерел:

1. Малков С.Ю. Математическое моделирование исторической динамики: подходы и модели. М.: РГСУ. 2004. 188 с.

2. Caltagirone S., Pendergast A., Betz C. The diamond model of intrusion analysis. DTIC Document, Tech. Rep. 2013. 21 P.

3. Hutchins E. M., Cloppert M. J., and Amin R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research. 2011. Vol. 1. P. 80-82.

4. Schneier B. Attack trees. Dr. Dobbs journal. 1999. Vol.24. No. 12. P. 21-29.

Ключові слова: інформаційна безпека, кібербезпека, модель, динамічні системи, нелінійність, методи, кібератаки.

Ключевые слова: информационная безопасность, кибербезопасность, модель, динамичные системы, нелинейность, методы, кибератаки.

Keywords: information security, cybersecurity, model, dynamic systems, nonlinearity, methods, cyber attacks.

Орлов Сергей Вячеславович

Національний університет «Одеська юридична академія»,
старший преподаватель кафедры информационных технологий

ПРОБЛЕМА УДЛИНЕНИЯ ТЕКСТА В СИСТЕМАХ ШИФРОВАНИЯ НА ОСНОВЕ КОНЕЧНОГО АВТОМАТА И АВТОМАТА С МАГАЗИННОЙ ПАМЯТЬЮ

Удлинение текстов при шифровании является одной из важных характеристик любой системы шифрования. Шифрование контента все большего объема характерно для современных технологий. Это не только обмен видео, в том числе потокового, но и реализация блок чейн технологий и многое другое. В связи с этим все более важной характеристикой систем шифрования становиться ее способность не очень сильно увеличивать объем информации при шифровании.

Рассмотрим систему шифрования построенной на основе контекстно свободной и регулярной грамматик предложен-