11. Кирилычев, А. А. Решение задачи нормирования ходового времени и расхода топлива морского судна [Текст] / А. А. Кирилычев, Н. В. Ивановский, С. П. Голиков, Д. Г. Куценко, В. А. Зеленцов // Восточно-Европейский журнал передовых технологий. — 2012. — № 6/3(60). — С. 28—32.

ОПТИМАЛЬНЕ УПРАВЛІННЯ ЕЛЕКТРОПРИВОДОМ ТРАЛОВОЇ ЛЕБІДКИ

У статті розглядається задача пошуку оптимального керування електроприводом траловой лебідки. Критерієм оптимізації є мінімум затрачуваної енергії. Основним результатом дослідження є методика розрахунку коефіцієнта посилення електроприводу траловой лебідки при намотуванні ваєра на барабан при врахуванні зміни радіуса намотування і моменту інерції барабана.

Ключові слова: тралова лебідка, електропривод, коефіцієнт підсилення.

***Голиков Сергей Павлович**, кандидат технических наук, доцент, декан морского факультету, Керченский государственный морской технологический университет, Украина.*

***Голіков Сергій Павлович**, кандидат технічних наук, доцент, декан морського факультету, Керченський державний морський технологічний університет, Україна, **e-mail: golosaa@mail.ru**.*

Golikov Sergej**, Kerch State Maritime Technical University, Ukraine, **e-mail: golosaa@mail.ru

УДК 004.9:517.978.2

Грищук Р. В.

МЕТОДОЛОГІЯ ПОБУДОВИ БАГАТОКРИТЕРІЙНИХ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ ТА МЕТОДІВ

У роботі запропоновано методологію синтезу та аналізу багатокритерійних диференціально-ігрових моделей та методів моделювання процесів кібернападу. Результати методології відображаються як у кількісній, так і якісній формі, що не суперечить основним положенням теорії складних систем. Застосування методології сприяє процесу інтеграції прогресивних систем інформаційної безпеки в новостворювані інформаційні технології.

Ключові слова: *процес кібернападу, рівень захищеності, багатокритерійна диференціально-ігрова модель, інформаційний ресурс.*

1. Вступ

Питання, що розглядаються в роботі, відносяться до галузі інформаційної безпеки. Стрімкий розвиток науково-технічного прогресу на початку XXI сторіччя в галузі інформаційних технологій (ІТ) пов'язаний з повсюдним впровадженням їх у всі сфери діяльності сучасного суспільства будь-якої розвиненої держави світу. Високі темпи інформатизації українського суспільства та державних інститутів сприяють подальшому зростанню ролі й місця кіберпростору в питаннях забезпечення національної безпеки в інформаційній сфері.

2. Постановка проблеми

Кіберпростір на сьогодні виступає системоутворюючим чинником, безпека якого не в останню чергу визначає рівень інформаційної безпеки (ІБ) держави. Масова доступність ІТ відкриває широкі можливості щодо здійснення несанкціонованого доступу (НСД) до державних інформаційних ресурсів (ІР) як неавторизованим користувачам, так і злочинним угрупованням, чим створює передумови для виникнення загроз безпеці інформації у національному сегменті кіберпростору в інформаційній сфері [1]. Протидія таким загрозам є принциповим аспектом укріплення стратегічної стабільності держави та її ІБ [2]. Саме тому потребують перегляду діючі концепції побудови систем ІБ (СІБ) та стратегій їх ефективного застосування.

3. Аналіз досліджень і публікацій

Аналіз останніх досліджень і публікацій [1—7] дозволив встановити один з пріоритетних напрямків підвищення рівня захищеності (РЗ) ІР зокрема, та подальшої стабілізації ІБ держави в цілому. Він полягає в якісно новому вирішенні проблеми ІБ держави шляхом створення сучасних методів та засобів захисту інформації (ЗІ) від кібернападу (КБн), що реалізують НСД до ІР інформаційно-телекомунікаційних систем. Так, вагомі наукові результати при вирішенні проблеми ІБ держави та розкритті окремих її складових одержано в наукових працях [1, 2, 8, 9] та ін., але незважаючи на це проблема залишається актуальною не тільки для України, а й для усієї світової спільноти.

Виходячи з єдиних системних позицій [10] та потреби реалізації комплексного підходу до побудови прогресивних СІБ на сучасному етапі розвитку науки і техніки існує об'єктивне протиріччя між високими вимогами, що висуваються до забезпечення захищеності ІР в умовах інформаційного конфлікту (ІК) під час реалізації процесів КБн, та принциповою неможливістю їх виконання на базі сучасної практики ЗІ, яка ґрунтується на застарілих моделях і методах, більшість з яких є однокритерійними. Однокритерійність, як наслідок, породжує проблему підвищення достовірності отримуваних результатів та адекватності розроблюваних моделей. У зв'язку з цим, у статті переслідується мета щодо розробки відповідної методології синтезу та аналізу багатокритерійних моделей та методів моделювання

процесів КБн, необхідної і достатньої для розв'язання ряду практичних задач ЗІ.

4. Методологія синтезу та аналізу

У [8] розроблено методологію синтезу диференціально-ігрових моделей та методів моделювання, а в [11] викладено основи багатокритерійного синтезу систем інформаційної безпеки. На основі досліджень [11, 12] в статті пропонується відповідна методологія. Вона містить три етапи: 1) визначення множини станів СІБ; 2) оптимізація ресурсів КБз та оцінювання РЗ; 3) оцінювання ефективності СІБ.

Визначення множини станів СІБ. На першому етапі, виходячи з того, які характеристики безпеки ІР повинні бути забезпечені (конфіденційність, цілісність, доступність) та множини параметрів, що визначають інтенсивності реалізації кібератак (КБа) $\mu_i(t)$ ($i=\overline{1,n}$, де n — кількість КБа), відмов СІБ $\beta_i(t)$, знаходження вразливостей $\gamma_i(t)$ тощо, експертом з ІБ вирішується концептуальне завдання щодо визначення множини можливих станів $\{P_z(t)\}$, у яких може перебувати новостворювана СІБ ($P_z(t)$ — ймовірності перебування СІБ під впливом відповідних методів, $z=\overline{0,c}$, c — кількість станів СІБ). Наприклад, якщо $z=0$, то СІБ у момент часу t перебуває під впливом методів НСД, якщо $z=1$ — під впливом МЗІ тощо.

Оптимізація ресурсів КБз та оцінювання РЗ. На цьому етапі вирішуються ряд задач. Основна задача — це задача оптимізації обмеженого ресурсу КБз $\lambda_{z\min}^{opt}(t)$ за умови відповідності поточного РЗ прогнозованому, який не гірше за ціну гри I_0^{VR}. Другорядна задача — задача підвищення достовірності одержуваних оцінок прогнозованого РЗ та адекватності відповідних багатокритерійних диференціально-ігрових моделей $P_0^{opt\ VR}(t)$.

Вказані задачі вирішуються шляхом введення експертом з ІБ додаткових частинних критеріїв $I_j=\Phi_j\left[\lambda_i(t),\mu_i(t),T,P_0(t)\right]$, що характеризують той чи інший аспект функціонування СІБ (Φ_j — функції, що мають неперервні частинні похідні за $\lambda_i(t)$ та $\mu_i(t)$). Частинні критерії I_j є компонентами r-мірного векторного критерію $I_0=\overline{I_1,I_r}$, який обмежений допустимою областю $I_0\in M$. Наприклад, додатковими частинними критеріями є ресурс (Р) гравця КБз I_2, Р гравця КБн I_3. Процедура багатокритерійного оцінювання реалізується із застосуванням відповідної багатокритерійної диференціально-ігрової моделі [11]. Так, усі частинні критерії I_j надходять на блок нормалізації, де реалізується процедура їх нормалізації шляхом зведення до безрозмірної величини I_{0j}. У блоці оптимізації та оцінювання здійснюється процедура регуляризації вихідної некоректної задачі моделювання процесів КБн за багатокритерійною диференціально-ігровою моделлю, забезпечується суттєве спрощення проблеми динамічної векторної оптимізації.

Оцінювання ефективності СІБ. Третій етап є заключним. Він передбачає реалізацію диференціально-ігрової процедури оцінювання ефективності СІБ [11], що проектується. Так, при проектуванні СІБ експерт вирішує завдання забезпечення вибору найефективнішої альтернативи $I_{0\theta}^{(j)*}$ з можливих, тобто $I_{0\theta}^{(j)*}\in\{I_{0\theta}^{(j)}\}$ (j — рівень ієрархії частинних критеріїв, θ-ї властивості, що оцінюється). На основі багатокритерійного диференціально-ігрового методу оцінювання ефективності СІБ [12], знаходяться кількісні та якісні оцінки ефективності системи $\{I_{0\theta}^{(j)*}, I_{\text{ЕФ}}\}$ ($I_{\text{ЕФ}}$ — базова терм-множина лінгвістичної змінної, яка визначається п'ятьма термами: $I_{\text{ЕФ}}=\bigcup_{i=1}^{5} I_{\text{ЕФ}}=$ = {«абсолютно неефективна» (АН), «недостатньо ефективна» (НЕ), «ефективна» (Е), «достатньо ефективна» (ДЕ), «абсолютно ефективна» (АЕ)}). Застосування методу [12] забезпечує оцінювання ефективності СІБ на різних рівнях ієрархії, що сприяє розширенню діапазону його практичного застосування на процедури оцінювання ефективності комплексних СІБ, як діючих, так і перспективних.

У результаті застосування методології формується звіт, у якому відображаються результати 1—3 етапів. Отримані результати можуть бути використані для формування додаткових наборів вхідних даних, які слід враховувати при проектуванні та створенні прогресивних СІБ, наприклад, інтелектуальних систем захисту інформації на основі технології розпізнавання образів [13].

6. Висновок

На основі запропонованої методології можливо будувати як програмні, так і програмно-апаратні СІБ, інтегровані до новостворюваних ІТ, що призначені для забезпечення в реальному масштабі часу прогнозованого РЗ ІР від кібератак прогнозованого класу. Застосування методології також забезпечує вибір найкращого варіанту побудови прогресивної СІБ, що ґрунтується на інтегральному показнику ефективності системи на базі розроблених моделей та методів моделювання.

Литература

1. Хорошко, В. О. Информационная безопасность Украины. Основные проблемы и перспективы [Текст] / В. О. Хорошко // Захист інформації. — 2008. — № 40 (спец. вип.). — С. 6—9.
2. Ленков, С. В. Методы и средства защиты информации : монография. В 2-х томах. Т. 2. Информационная безопасность [Текст] / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. — К. : Арий, 2008. — 344 с.
3. Голубев, В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями [Текст] : монография / В. А. Голубев. — Запорожье: ЗИГМУ, 2003. — 336 с.
4. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] / А. А. Малюк. — М.: Горячая линия-Телеком, 2004. — 280 с.
5. Скопа, О. О. Принципи вибору формальних параметрів при побудові профілей захисту інформаційних ресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Восточно-Европейский журнал передовых технологий. — 2012. — Т. 5, № 2(59). — С. 31—33.
6. Казакова, Н. Ф. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем [Текст] / О. О. Скопа, Н. Ф. Казакова // Системи обробки інформації: Безпека та захист інформації в інформаційних системах. — Х. : ХУПС ім. І. Кожедуба. — 2009. — № 7(79). — С. 48—54.
7. Скопа, О. О. Статистичне тестування симетричних криптографічних перетворень [Текст] / О. О. Скопа // Східно-Європейський журнал передових технологій. — 2011. — Т. 4, № 9(52). — С. 15—18.
8. Богуш, В. М. Інформаційна безпека держави [Текст] / В. М. Богуш, О. К. Юдін. — К.: «МК-Прес», 2005. — 432 с.
9. Домарев, В. В. Безопасность информационных технологий. Системный подход [Текст] / В. В. Домарев. — К.: ООО «ТИД ДС», 2004. — 992 с.
10. Корченко, О. Г. Системи захисту інформації [Текст] : монографія / О. Г. Корченко. — К.: НАУ, 2004. — 264 с.

11. Грищук, Р. В. Багатокритерійний синтез систем інформаційної безпеки [Текст] / Р. В. Грищук, І. А. Пількевич, В. О. Хорошко, В. І. Котков // Східно-Європейський журнал передових технологій. — 2012. — № 5/9(59). — С. 40—44.
12. Грищук, Р. В. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси [Текст] / Р. В. Грищук, О. Г. Корченко // Захист інформації. — 2012. — № 3(56). — С. 115—122.
13. Пількевич, І. А. Моделювання системи розпізнавання та аналізу текстових даних [Текст] / І. А. Пількевич, Н. М. Лобанчикова, І. В. Шульга, Р. С. Лазюта // Східно-Європейський журнал передових технологій. — 2013. — № 4/9(64). — С. 23—29.

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ МНОГОКРИТЕРИЙНЫХ ДИФФЕРЕНЦИАЛЬНО-ИГРОВЫХ МОДЕЛЕЙ И МЕТОДОВ

В работе предложена методология синтеза и анализа многокритериальных дифференциально-игровых моделей и методов моделирования процессов кибернападения. Результаты методологии отображаются как в количественной, так и качественной форме, что не противоречит основным положениям теории сложных систем. Применение методологии способствует процессу интеграции прогрессивных систем информационной безопасности во вновь создаваемые информационные технологии.

Ключевые слова: процесс кибернападения, уровень защищенности, многокритериальная дифференциально-игровая модель, информационный ресурс.

***Грищук Руслан Валентинович**, доктор технічних наук, старший науковий співробітник, Науковий центр, Житомирський військовий інститут імені С. П. Корольова, Україна,* ***e-mail: RuslanGRV@rambler.ru**.*

***Грищук Руслан Валентинович**, доктор технических наук, старший научный сотрудник, Научный центр, Житомирский военный институт имени С. П. Королева, Украина.*

Hryshchuk Ruslan**, Zhytomyr Military Institute named after Sergey Korolyov, Ukraine,* ***e-mail: RuslanGRV@rambler.ru

УДК 621.391:519.72

Казакова Н. Ф.

АНАЛИТИЧЕСКОЕ ОБОСНОВАНИЕ ИСПОЛЬЗОВАНИЯ GFSR-ГЕНЕРАТОРОВ В ЗАДАЧАХ КРИПТОГРАФИИ

Проведен анализ проблем, связанных с теоретическим и практическим обоснованием принципов построения комбинированных генераторов псевдослучайных последовательностей на основе регистров сдвига с обобщенной обратной связью. Определены проблемы, связанные с проектированием и оценкой качества рекуррентных генераторов псевдослучайных последовательностей комбинированного типа, которые объединяют рекуррентные способы формирования шифрующих последовательностей с нелинейной фильтрацией выходного потока

Ключевые слова: *потоковый шифр, комбинированный генератор, фильтр с памятью, GFSR-генератор, вихрь Мерсенна.*

1. Введение

Генераторы (ГН) псевдослучайных последовательностей (ПСП) применяются в задачах криптографии и моделирования. Они являются частью многих криптографических систем: формирование ключей, шифрование сообщений и т. д. Их эффективность при моделировании доказана давно. Что касается криптографии, то здесь требования к равномерности распределения вероятностей формируемых чисел выше [1—3]. Этим определяется тот факт, что в настоящее время в этой области появилось большое число новых идей и подходов. Ранее для формирования ПСП использовались различные методы, среди которых наиболее значимый основан на линейных сдвиговых регистрах с обратной связью (*англ.:* Linear Feedback Shift Register — LFSR). Они экономичны, поскольку для реализации применяют сдвиговые, логические и линейные операции. Однако, для обеспечения заданной криптографической стойкости в их состав необходимо введение нелинейных функций и, т.о., они представляют собой некоторый инженерный компромисс между указанным подходом и ГН со сложными нелинейными преобразованиями. Следовательно, обоснованием актуальности является анализ проблем, связанных с проектированием и оценкой качества рекуррентных ГН ПСП комбинированного типа [1, 2], объединяющих рекуррентные способы формирования шифрующих последовательностей с нелинейной фильтрацией выходного потока [3].

2. Анализ литературных данных и постановка проблемы

В [4] сказано, что многие алгоритмы не обеспечивает приемлемой равномерности распределения вероятностей чисел, формируемых на выходе ГН ПСП. Там же приведен анализ проблем, связанных с усовершенствоанием алгоритмов, построенных на основе LFSR, а также краткая аннотация по нелинейным алгоритмам. Показано, что к ГН 1-го типа применима некоторая общая математическая теория, а в основу алгоритмов 2-го типа заложены обособленные математические задачи. В [5—8] показано, что поскольку экономия вычислительных ресурсов, криптостойкость и производительность формирования ПСП являются наиболее актуальными задачами, разработчики потоковых систем шифрования