Продолжение таблицы 1

11. Выход из системы.	1. Подготовка к выключению. 2 .Выключение ПК.	1. Выполнение утилит подготовки к выключению.	1. Некорректное завершение работы, которое приводит к автоматическому сохранению данных. 2. Модификация файлов из-за некорректного завершения работы.

IV Выводы

1. Предложена методика систематизации характеристик типовых компьютерных систем, позволяющая учесть их особенности при разработке системы защиты обрабатываемой информации от несанкционированного доступа.
2. Методика заключается в следующем:
   - формализуются этапы подготовки документов в типовой КС;
   - с учетом общих принципов политики безопасности формализуются и детализируются действия пользователей при формировании файлов документов;
   - систематизированным действиям пользователя ставятся в соответствие действия операционной системы и угрозы.
3. Результат применения методики – модель угроз, в основе которой лежат:
   - основные принципы политики безопасности;
   - формализованные действия пользователя при формировании файлов документов;
   - действия операционной системы по обеспечению задач, выполняемых пользователем;
   - угрозы, сопровождающие действия операционной системы.

На основе ранее предложенной политики безопасности [1] и рассмотренной методики систематизации характеристик получена модель угроз для типовой компьютерной системы на основе одномашинного многопользовательского комплекса.

4. Предложенные в статье подходы могут стать основой методики систематизации и для многомашинного многопользовательского комплекса с одновременной обработкой информации с ограниченным доступом.

5. Методику предполагается применить для проведения сравнительного системного анализа операционных систем Windows NT, -2000, Novell Net Ware и Unix с целью оценки соответствия встроенных услуг защиты и аудита предлагаемой политике безопасности.

Литература: 1. Яковив И. Б., Черноног А. А. «Анализ образующих сред типовых компьютерных систем» // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – Вип. 2. – с. 129–132. – К., 2001. 2. Нормативный документ системы технической защиты «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа» от 28. 04. 1999 г. // НД ТЗИ 2.5 – 004 – 99. 3. Нормативный документ системы технической защиты «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа» от 28. 04. 1999 г. // НД ТЗИ 2.5 – 004 – 99.

УДК 681.324

КЛАСИФІКАЦІЯ І АНАЛІЗ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Ігор Яковів, Олександр Корнейко*, Олександр Черноног*

*Національна академія СБУ, * ВІТІ НТУУ «КПІ»*

Анотація: **Найбільший розвиток теоретичних досліджень в області захисту інформаційних систем отримало формальне моделювання систем і процесів захисту інформації. З метою аналізу забезпечення чіткого розподілу між багаточисельними методами та моделями систем і процесів захисту проведена їх класифікація.**

Summary: **The greatest development of the theoretical researches in the field of a security of information systems has received a formal simulation of systems and processes for the protection of the information. To**

ensure the analysis of the precise distinction between numerous methods and models of the security systems and processes their classification is considered.
Ключові слова: **Інформація, комп'ютерна система, захист інформації, метод моделювання, модель.**

I Вступ

У сучасний час розроблений та апробований на практиці дуже показовий арсенал методів моделювання, що дозволяють ефективно вирішувати задачі аналізу та синтезу великих систем, а також управління процесами їх функціонування. Використання цих методів в області забезпечення безпеки комп'ютерних систем привело до розробки великої кількості формальних моделей безпеки. Тільки за допомогою цих моделей можливо довести безпеку системи, спираючись при цьому на об'єктивні та незаперечні постулати математичної теорії.

II Критерії системної класифікації

Системна класифікація моделей може бути здійснена за сукупністю трьох критеріїв наступного змісту:

1) спосіб моделювання, тобто той основний прийом, який покладено в основу побудови моделі;
2) характер системи – показник, що визначає взаємозв'язки між належними визначенню на моделі значеннями характеристик системи, що моделюється, і параметрами системи та зовнішнього середовища, що впливають на них;
3) масштаб моделювання – показник, який відбиває рівень характеристик, що визначаються на моделі.

За першим критерієм усі моделі можуть бути поділені на аналітичні та статистичні. Аналітичні моделі подаються у вигляді деякої сукупності аналітичних та (або) логічних залежностей та дозволяють визначати необхідні характеристики шляхом проведення обчислень за вказаними залежностями. При статистичному моделюванні система, що моделюється, подається у вигляді деякого аналога, що відображає для характеристик, що визначаються, залежності реальної системи. Само визначення значень цих характеристик здійснюється шляхом багаторазової імітації реалізації залежностей характеристик від суттєво значимих параметрів реальної системи і зовнішнього середовища та статистичною обробкою отриманих при цьому результатів;

Сформульованих в п. 2 залежностей взагалі дуже багато, але на вибір методів моделювання найбільш визначне значення має рівень певності вказаних залежностей. За цією ознакою системи, що моделюються, поділяються на детерміновані та стохастичні: по-перше, усі залежності строго та однозначно визначені, по-друге, на них чинять визначний вплив випадкові фактори;

За третім критерієм моделі можливо поділити на загальні та часткові. Загальні моделі будуються з метою визначення значень деяких узагальнених характеристик систем, що моделюються, часткові – з метою визначення значень часткових, локальних характеристик системи.

III Системна класифікація моделей та методів моделювання

Системна класифікація моделей в залежності від способів моделювання, масштабу моделей та характеру систем, що моделюються, може бути наочно зображена у вигляді, наведеному на рис. 1 [1].

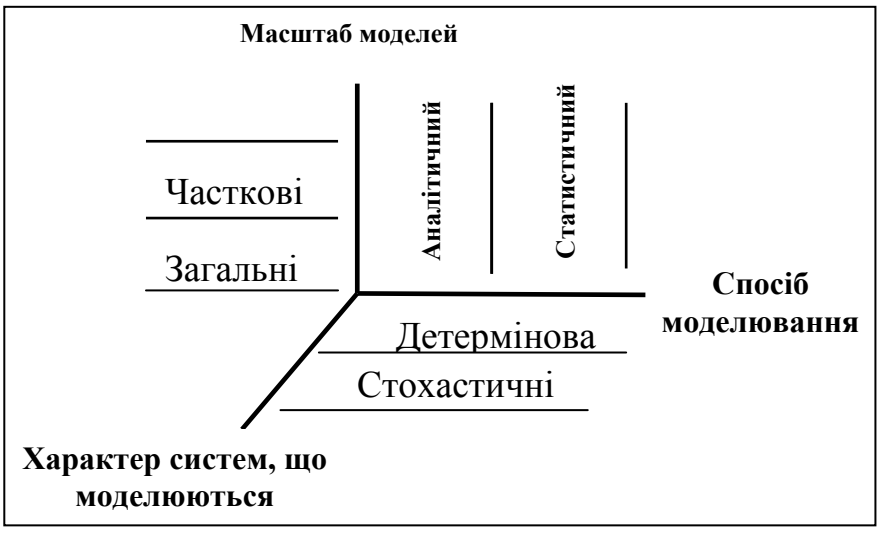

Рисунок 1 – Системна класифікація моделей

Моделювання полягає в побудові моделі системи, що вивчається або розробляється, та імітації на ній процесів функціонування реальної системи з метою одержання необхідних характеристик цієї системи. Методи моделювання є способами (прийомами) дослідження системи з метою побудови її моделі та імітації на ній процесів функціонування реальної системи. В зв'язку з цим класифікація методів моделювання відповідає системній класифікації моделей.

Виходячи з цілей моделювання методи розподіляються на наступні:

1) методи побудови моделей, або інакше – опису структури і процесів функціонування систем, що моделюються;
2) методи імітації процесів функціонування систем.

При аналітичному моделюванні структура системи, що моделюється, та процеси її функціонування подаються у вигляді деяких виразів, що відбивають залежність характеристик системи, що визначаються, від її параметрів та параметрів зовнішнього середовища. Імітація процесів функціонування систем є виродженою, вона зводиться до розрахунку за вказаними вище виразами значень характеристик, що визначаються, для заданих значень параметрів системи та зовнішнього середовища. Іншими словами, в аналітичних моделях структура систем, що моделюються, та процеси їх функціонування подаються в неявному вигляді.

При статистичному моделюванні структура системи, що моделюється, адекватно відображається в моделі, а процеси її функціонування програються (імітуються) на збудованій моделі. При цьому ступінь адекватності моделі реальній системі та процесів імітації на моделі реальним процесам функціонування системи, що моделюється, визначаються цілями моделювання, тобто тими характеристиками системи, які мають бути отримані в процесі моделювання. Значення характеристик, що визначаються в процесі моделювання, мають відповідати (крайня міра, з точністю до цілей моделювання) значенням тих характеристик, які будуть чи можуть мати місце в процесі функціонування реальної системи.

Побудова статистичної моделі міститься в опису структури та процесів функціонування системи, а імітація процесів функціонування – в програванні тим чи іншим способом зміни в часі станів моделі системи та прийнятті на кожному кроці імітації тих рішень, які зумовлені створеною ситуацією та правилами функціонування реальної системи.

Розглянемо методи моделювання статистичних часткових моделей для стохастичних систем. Опис структури системи, що моделюється, повинен містити, по-перше, перелік усіх її істотно значимих елементів, по-друге, взаємні зв’язки між елементами, та по-третє – характер цих взаємозв’язків. Опис структури може бути здійснений наступними методами:

1) теорії множин;
2) теорії нечітких множин;
3) теорії графів;
4) неформальної теорії систем;
5) нестрогої математики.

Для опису процесів функціонування стохастичних систем необхідні засоби відображення впливу випадкових факторів. Такі засоби містяться у ряді наступних методів:

1) статистичних випробувань (або Монте-Карло);
2) теорії масового обслуговування;
3) теорії ймовірносних автоматів;
4) неформальної теорії систем, основними частинами якої є:
   - методи структурування компонентів систем;
   - **неформальні методи оцінювання (найбільш відомі – методи експертних оцінок);**
   - неформальні методи пошуку оптимальних рішень;
5) нестрогої математики.

Відповідно до наведеної класифікації розглянемо найбільш відомі приклади моделей (табл. 1 та табл. 2).

Таблиця 1 – Порівняльні характеристики аналітичних загальних моделей для детермінованих систем

Назва моделі	Основна ідея, співвідношення з іншими моделями	Математичні основи
Модель матриці доступів HRU (модель безпеки Харрисона-Рузо-Ульмана) [2].	Дискреційна модель. Система захисту подається як кінцевий автомат. Функціонування системи розглядається тільки з точки зору змін у матриці доступів.	Теорія відношень.

Продовження таблиці 1.

Типізована матриця доступу (TAM) [3].	Розвиток моделі HRU, доповнена концепцією типів.	Теорія відношень.
Модель розповсюдження прав доступу Take-Grant [2].	Дискреційна модель. Стан системи описується її графом доступів. Перехід системи з стану в стан зумовлюється операціями або правилами перетворення графів.	Теорія графів.
Поширена модель Take-Grant [2].	Розглядаються шляхи виникнення інформаційних потоків, а також їх вартість в системах з дискреційним розмежуванням доступу.	Теорія графів.
Класична мандатна модель Белла-Лападули [3].	Вводиться функція рівня безпеки та решітка рівней безпеки, які разом визначають усі допустимі відношення доступу між сутностями системи.	Теорія відношень, апарат решіток.
Модель безпечного переходу [3].	Розвиток моделі Белла-Лападули. Регламентуються зміни рівнів безпеки при переході від стану до стану за допомогою додаткових правил.	Теорія відношень, апарат решіток.
Модель з уповноваженими суб'єктами [3].	Розвиток моделі Белла-Лападули шляхом виділення підмножини уповноважених суб'єктів, яким дозволяється ініціювати переходи, внаслідок яких у сутностей системи змінюються рівні безпеки.	Теорія відношень, апарат решіток.
Модель спільного доступу [3].	Розвиток моделі Белла-Лападула з метою забезпечення спільного доступу суб'єктів до об'єктів.	Теорія відношень, апарат решіток.
Модель безпечного переходу для системи спільного доступу [3].	Розвиток моделі Белла-Лападула. Враховуються спільні доступи групових суб'єктів.	Теорія відношень, апарат решіток.
Модель спільного доступу з уповноваженими суб'єктами [3].	Розвиток моделі Белла-Лападула. Формулюється умова авторизації функції переходу для системи з уповноваженими суб'єктами.	Теорія відношень, апарат решіток.
Модель Trusted Math [3].	Модель станів та подій, використовує оператор наступного значення, який визначає нові значення, що привласнюються змінним і нові становища після подій, що відбулися.	Теорія предикатів.
Модель Белла для мереж комутації пакетів (B-модель) [5].	Введені правила безпечного виконання операцій однобічного з'єднання, видалення прав на з'єднання. Може бути частково описана в термінах TAC та SP-моделей.	Теорія відношень.
Модель Low-Water-Mark (LMW) [2].	Пропонується порядок безпечного функціонування системи у випадку, коли по запиту суб'єкта йому завжди необхідно надавати доступ на запис в об'єкт.	Теорія відношень.
Схематична модель (SP-модель) [4]	Модель матриці доступу зі строгою типізацією ресурсів. Може бути описана в термінах TAC-моделі.	Теорія множин.
Модель трансформації прав доступу (TAC-модель) [4].	Модель описує розмежування прав доступу на основі наданого суб'єкту в даний момент часу тільки одного права доступу. Може бути описана в термінах SP-моделі.	Теорія множин.
Модель безпеки воєнної системи передачі даних (MMS-модель) [4].	Модель з адміністратором безпеки для керування доступом до даних та пристроїв глобальної мережі передачі даних.	Теорія множин.
Модель з графом захисту (PRG-модель) [4].	Визначає безпечне виконання операцій запозичення, передачі прав в термінах теорії графів.	Теорія графів.
Ієрархічна модель (H-модель) [4].	Опис керування доступом для паралельних обчислень. Базується на понятті критичного інтервалу. Може бути описана в термінах TAC-моделі.	Теорія предикатів.

Продовження таблиці 1.

Ролева політика безпеки [3].	Управління доступом та призначення повноважень здійснюється не реальними користувачами, а абстрактними ролями. Абстрактні ролі розглядаються як учасники визначеного процесу обробки інформації.	Теорія відношень.
Політика доменів і типів (DTE) [3].	Практична реалізація моделі типізованої матриці доступу в системах, побудованих на базі операційної системи UNIX.	Теорія відношень.
Модель систем розмежування доступу до ресурсів комп'ютерної системи [1].	Сформульована система формальних правил регулювання доступу та збудована алгоритмічна процедура управління доступом.	Апарат бульових функцій.

Таблиця 2 – Порівняльні характеристики аналітичних загальних моделей для стохастичних систем

Назва моделі	Основна ідея, співвідношення з іншими моделями	Математичні основи
Загальна модель процесу захисту інформації [1].	В загальному випадку відбиває процес захисту інформації, як процес взаємодії дестабілізуючих факторів, впливаючих на інформацію, та засобів захисту інформації, заважаючих дії цих факторів.	Теорія ймовірностей.
Узагальнена модель системи захисту інформації [1].	Розвиток загальної моделі процесу захисту інформації. Відбиваються процеси розподілення ресурсів.	Теорія ймовірностей.
Модель загальної оцінки загроз інформації [1].	Відбиває взаємозв'язки усієї сукупності параметрів, що визначають міру загроз інформації від усієї сукупності, чи від окремо взятих дестабілізуючих факторів, причому у співвідношенні з тими збитками, що можуть мати місце при реалізації загроз.	Теорія ймовірностей.
Модель безпеки інформаційних потоків [2].	Розглядаються два підходи до визначення безпеки інформаційних потоків, заснованих на поняттях інформаційного невиведення та інформаційного невтручання.	Теорія ймовірностей.
Модель автомата системи захисту GM [2].	Система захисту подається детермінованим автоматом. При інтерпретації детермінованості автомату, використовуючи події з ймовірністю (0, 1) інформаційне невтручання розглядається як частковий випадок відповідного поняття моделі безпеки інформаційних потоків.	Теорія ймовірностей.

Необхідно відмітити, що на даний час серед моделей систем та процесів захисту інформації не зустрічаються моделі, які відносяться до статистичних загальних для стохастичних систем. Пояснюється це труднощами, пов'язаними з відсутністю у теперішній час уявлень про закони розподілу ймовірностей великого числа випадкових подій, що є суттєво визначними для функціонування систем захисту інформації.

IV Висновки

З розгляду методів моделювання та моделей систем і процесів захисту інформації випливає, що суть усіх моделей безпеки однакова, оскільки вони призначені для вирішення однакових завдань. Метою створення моделі є отримання формального доказу безпеки системи при дотриманні визначених умов, а також визначення достатнього критерію безпеки.

Виходячи з різноманітності моделей та методів їх моделювання, цілком зрозуміло, постає питання вибору для використання в тому чи іншому випадку найкращої моделі. Відповідь на це питання полягає у наступному. Безпекою є успішне протистояння загрозам, тому сама модель безпеки не забезпечує захист, а лише надає основоположний принцип архітектури системи, реалізація якого і має забезпечити покладені в моделі властивості безпеки. Отже, безпека системи у рівному ступені визначається трьома факторами: властивостями самої моделі, її адекватністю загрозам, що впливають на систему, та тим, наскільки коректно вона реалізована. Оскільки при існуючому різноманітті теоретичних розробок в області інформаційної безпеки вибір моделі, адекватної заданим загрозам, не є проблемою, останнє, вирішальне слово лишається за її реалізацією в захищеній системі.

Література: 1. Герасименко В. А. Защита информации в АСОД (в 2-х томах). – М.: Энергоатомиздат, 1994. – 400 с. 2. Девянин П. Н., Михальский О. О. и др. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000. – 192 с. 3. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия. – Телеком, 2000. – 452 с. 4. Богданов А. М., Корнейко А. В. и др. Моделирование безопасной обработки информации в компьютерных системах. – К.: Наукова думка, 2000. – 160 с. 5. Denning D. E. A lattice model of secure information flow // Coinroun. ACM. – 1976. – V. 19, № 5. – P. 236 – 243.

УДК.681.324

МЕТОДИКА АВТОМАТИЗИРОВАННОГО ВЫЯВЛЕНИЯ ПОБОЧНЫХ ИНФОРМАТИВНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ СВЯЗИ И ОБРАБОТКИ ИНФОРМАЦИИ

Алексей Богатырев, Владимир Настрадин, Александр Черноног*
*Национальная академия СБ Украины, *ВИТИ НТУУ "КПИ"*

Аннотация: **Рассмотрена методика обнаружения побочного излучения радиотехнических средств, основанная на использовании различия законов затухания электромагнитного поля в ближней, промежуточной и дальней зоне от источника радиоволн.**
Summary: **The technique of detection of accessory radiation of radio engineering resources based on usage of distinction of the laws of fading of an electromagnetic field in short-range, intermediate and far-field region from a source of radio waves is considered.**
Ключевые слова: **Побочные излучения, защита информации, канал утечки информации, метод двух антенн.**

I Введение

Одним из основных каналов утечки информации является канал ПЭМИ (побочных электромагнитных излучений) аппаратуры связи, хранения и обработки информации. Излучения такого рода обусловлены разными факторами, например:

- наличием в схемах генераторов синусоидальных и импульсных сигналов;
- применением нелинейных преобразований высокочастотных сигналов, приводящих к появлению кратных гармоник;
- возникновением при определенных условиях паразитной генерации;
- старением и выходом из строя деталей узлов блокировки, фильтрации по питанию и т. п.;
- недостаточной экранировкой высокочастотных узлов и аппаратуры в целом, окислением в местах механического соединения частей экранировки и т. д.

Как правило, работа любой аппаратуры сопровождается целой гаммой излучаемых частот в очень широком спектре с самой разной интенсивностью, среди которых имеются частоты, модулированные информационной составляющей. Последние представляют реальную опасность, если они имеют за границей контролируемой зоны достаточный для перехвата уровень. В литературе достаточно подробно освещены методики снятия информации с канала побочного излучения, которые используются специалистами как спецслужб, так и промышленного шпионажа. Чем меньше размеры контролируемой зоны, тем жестче требования по соблюдению безопасных норм уровней побочного излучения. Поэтому задача своевременного обнаружения побочного излучения аппаратуры связи, хранения и обработки информации всегда представлялась весьма актуальной и является одной из основных составляющих комплекса мероприятий по защите информации.

II Постановка задачи

Задача обнаружения побочного излучения радиотехнических средств во всех случаях представляет собой многоальтернативную задачу обнаружения сигнала с заранее неизвестными параметрами: частотой, амплитудой, шириной спектра и т. д.

На практике применяются разные методики, использование которых в основном требует специального дорогостоящего оборудования и больших затрат времени. Например, один из традиционных путей решения задачи обнаружения побочного электромагнитного излучения включает в себя: