DOI: https://doi.org/10.33216/1998-7927-2021-268-4-49-52

УДК 519.806:004.681

КОНТРОЛЬ ТЕХНІЧНОГО СТАНУ СКЛАДОВИХ ЕЛЕМЕНТІВ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Дегтярьова Л.М., Вакуленко Ю.В., Одарущенко О.Б.

CONTROL OF TECHNICAL CONDITION OF COMPONENT ELEMENTS OF INFORMATION PROTECTION SYSTEMS

Degtyaryova L.M., Vakulenko Y.V., Odarushchenko O.B.

В статті виконано аналіз підходів до вибору і побудови систем контролю технічного стану систем захисту інформації. Система контролю повинна обробляти інформацію про ступінь працездатності контрольованої системи на підставі вимірювання змінних процесів. Ця система може мати два види контролю: динамічний та статистичний, кожен з яких має власні дії, що визначаються двома факторами: часом контролю і достовірністю контролю.

Ключові слова: *динамічна система, технічний захист інформації, загрози інформаційної безпеки, інформаційні процеси.*

Постановка проблеми. Широке застосування комп'ютерної техніки в системах зв'язку, автоматизованих інформаційних системах, наукових дослідженнях та інших сферах життєдіяльності людини в даний час є пріоритетним спрямуванням, але останнім часом актуальними стає проведення так званих інформаційних атак або війн. Серед визначенні головних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та цілей захисту. Вимогами до забезпечення захисту інформації в системі контролюється цілісність програмних та технічних засобів захисту інформації [1]. Технічний захист інформації забезпечується організаційними, нормативно-правовими та технічними заходами, методами і засобами для забезпечення конфіденційності, цілісності та доступності інформації, яка циркулює в інформаційно-телекомунікаційних системах. Ефективність технічного захисту інформації може бути досягнута лише за умови застосування відповідних засобів забезпечення технічного захисту інформації різноманітного рівня складності.

Саме загрози технічного спрямування, які пов'язані з використанням різноманітних фізичних, апаратних і програмних та їх сполуки (програмно-апаратних методів та засобів), призводять до збитків, що потенційно можуть отримати власники інфотелекомунікаційних ресурсів завдяки процесам несанкціонованого доступу (спотворення, витоку, знищення) до інформації.

Мета статті полягає у розвитку теорії комплексної безпеки складних систем, а саме технічного стану складових елементів систем захисту інформації.

Основна частина. Основи стратегії захисту інформації включають необхідність використання двох термінологічних понять: стратегія технічного захисту інформації і стратегія безпеки інформації, яка захищається [2, 3].

Аналізуючи роботи [2-7, 9, 10] з позиції використання засобів технічного захисту інформації, можна зазначити, що великим мережам властиві наступні відмінні риси та проблеми, вирішення яких вимагають аналізу для розробки алгоритму вирішення цих проблем:

велика мережа має складну структуру, яка може бути побудована хаотично;

різниця швидкості передачі даних на різних ділянках великих телекомунікаційних мереж створює серйозні проблеми при розробці та використанні систем безпеки;

використання апаратно-технічних мережевих пристроїв з власними характеристиками продуктивності, базовими технологіями, відношенням до конкретних апаратних платформ, які можуть бути впровадженні в інформаційну структуру мережі;

наявність фахівців високої кваліфікації, які спроможні вирішувати специфічні проблеми під час моделювання ситуацій, пов'язаних з сумісністю різних платформ і версій операційних систем, засобів і технологій прикладного програмного забезпечення

при виконанні завдань з забезпечення питань політики безпеки;

вирішення проблем інформаційної безпеки часто надають другорядне значення в порівнянні з іншими проблемами, які розв'язуються в процесі створення і розвитку великої мережі;

можливість уникнути або звести до мінімуму ймовірність виникнення тимчасових інтервалів зупинки деяких компонентів системи безпеки, які потенційно можуть бути реалізовані на базі різнорідних апаратно-технічних засобів або елементів системи, географічно віддалених один від одного.

Згідно класифікації засобів технічного захисту інформації, яка проводиться за ознаками [8]:

– функціональним призначенням засобів ТЗІ щодо захисту інформації від загроз витоку технічними каналами та загроз спеціального впливу на засоби обробки інформації, оцінки ефективності ТЗІ та виявлення закладних пристроїв;

– показниками функціонального призначення засобів ТЗІ;

– особливостями конструктивного виконання.

Рис. Модель використання технічних засобів захисту інформації

При аналізі систем захисту інформації необхідно враховувати, що це складна система, яка складається з підсистем з багатьма функціями: власне системи захисту, системи контролю (засоби автоматичного контролю) і системи підтримки прийняття рішення.

Велика кількість пристроїв, що входять до складу обчислювальної системи, і їх складність вимагають суттєвого скорочення часу контролю, як кожного пристрою так окремих його складових завдяки використанню засобів автоматизованих системи контролю. Скорочення інтервалу часу, відведеного на проведення контролю, під час контролю викликає виникнення перехідного режиму у роботі пристрою, що підлягає контролю, і, крім того, самі вимірювані процеси зазнають значних змін. Система контролю повинна викликати інформацію про ступінь працездатності контрольованої системи на підставі опрацювання даних процесів, що змінюються. Саме це є завданням динамічного контролю, а саме сукупності дій, спрямованих на визначення технічного стану системи, пристроїв або вузлів за результатами вимірювання сигналів, які будуть змінюватись в часовому інтервалі проведення контролю.

При цьому слід зазначити, що системи контролю стану систем захисту і самі системи захисту є динамічними.

На противагу цьому статичним контролем вважається сукупність дій, спрямованих на визначення технічного стану системи, пристроїв і/або вузлів за результатами фіксації даних перевірки, які є практично постійними протягом часового інтервалу під час контролю сигналів контрольованого об'єкта.

В цьому контексті поняття динамічної та статичної системи цілком протилежні. У статичній системі попередній стан системи і попередня зміна вхідних сигналів не впливають на миттєві значення вихідних сигналів, і які залежать тільки від відповідних миттєвих значень вхідних сигналів. На відміну від статистичної системи, поведінка динамічної системи залежить як від миттєвих значень вхідних сигналів, так і від стану системи, обумовленого попередніми змінами вхідних і вихідних сигналів.

Динамічна система - математична модель деякого об'єкта, процесу або явища, які можуть бути представлені як система, для якої описані деякі стани, коли динамічна система описує поведінку цього процесу як послідовність переходів з одного стану в інший.

Сукупність усіх допустимих станів динамічної системи утворює її фазовий простір. Таким чином, система в якості своїх базових параметрів повинна спиратись на початковий стан і закон, за яким вона переходить з одного стану в інший.

Спираючись на попередні визначення можна зазначити, що математична модель динамічної системи повинна враховувати як попередні значення своїх параметрів, так і їх зміну в будь-який час існування системи, у фіксований період діяльності, власне, в період обслуговування системи безпеки інформаційної системи та її складових. Отже, представлення динамічної системи у вигляді математичної моделі містить змінні початкового стану системи і змінні, що характеризують перетворений стан, враховуючи взаємозалежність змінних:

- фіксований інтервал часу та часові показники в будь-який момент часу (t_i) з вказаного інтервалу часу (T);

- миттєві значення вхідних сигналів (x);

- допустимі значення вхідних сигналів в певні моменти часу (x_t);

- миттєві значення вихідних сигналів (y);

- допустимі значення вихідних сигналів в певні моменти часу (y_t);

- стани системи (Ss);

- параметри системи (p);

- функція (закон), що відображається диференційним рівнянням ($D(y)$) і враховує значення вихідних сигналів: $D(y)=f(t, x, Ss, p)$.

Але досить часто складну систему важко або взагалі неможливо оцінити, враховуючи тільки один показник зі всього комплексу параметрів, які впливають на стан захищеності інформації. Досить часто ці показники можуть бути суперечливими, тобто по-

ліпшення системи за одними показниками призводить до її погіршення за іншими. У таких випадках необхідно або якимось чином об'єднати ці показники в один, узагальнений, або визначити один з них як основний - домінуючий, а решту розглядати як деякі специфічні обмеження. Зрозуміло, що таке завдання більш-менш добре вирішується, якщо ці показників ефективності мають чисельне значення і є математичні вирази для їх розрахунку.

Засоби підсистеми технічного захисту інформації дозволяють в деякій мірі оцінити ступінь забезпечення функціональних властивостей захищеності інформації застосованими засобами захисту або можливу ступінь забезпечення функціональних властивостей захищеної інформації засобами, які проектуються для запровадження, забезпечуючи достатні показники функціональних властивостей захищеності, а саме: цілісність, достовірність та доступність інформації. Величину потенційної шкоди, якої може зазнати інформація в системі можна оцінити, аналізуючи вартість часових характеристик процесів, пов'язаних з організацією та здійсненням контролю, тривалості затримки в наданні відповідних послуг з використання певного ресурсу або елементу системи захисту даних.

Висновки. Здійснення контролю роботи складових елементів динамічної системи захисту інформації полягає у формуванні вхідних сигналів, фіксації вихідних сигналів, і, користуючись отриманою інформацією, здійснення аналізу змін цих параметрів і, як слідство, встановлення рівня працездатності системи шляхом порівняння отриманих значень зафіксованих сигналів з їх допустимими значеннями. Ефективність використання певного підходу або математичного апарату обґрунтовується такими факторами: наявність або відсутність достатньо точної інформації щодо складу та характеристик елементів системи, представлення (тип або форма) вхідної і вихідної інформації, прилади або програмне забезпечення, які діють в межах єдиної системи захисту даних тощо.

Література

1. Постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні»
2. Хорошко В.А., Юрьев А.Н. Методологический подход к оптимальному выбору комплекса мероприятий по защите информации // Защита информации: Сб. науч. тр. К.: НАУ, 2001. С. 132-136.
3. Лахно В.А., Петров А.С., Скрипкина А.С. Построение дискретных процедур распознавания и поиска уязвимостей информации // Інформаційна безпека, 2010. № 2 (4). С. 5–13.
4. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К. издательство Юниор, 2003. 504 с.
5. Безштанько В. Аналіз існуючих програмних засобів та методик оцінки стану інформаційної безпеки організації//Бизнес и безопасность, №1. 2007. с.32 – 35.
6. Єжова Л.Ф., Мачалін І.О., Невойт Я.В., Хорошко В.О. Управління інформаційною безпекою. К.: Вид. ДУІКТ, 2011.
7. Дегтярьова Л.М., Волошко С.В., Лоза В.В., Буланкіна А.О. Використання інформаційних технологій обробки даних в сучасних системах транспортної логістики//Сучасні інформаційні технології у сфері безпеки та оборони, № 1(37)/2020. К: Національний університет оборони України імені Івана Черняховського, 2020. с. 139-144
8. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 29.08.2012 № 472
9. Котенко И.В., Степашкин М.В., Чечулин А.А., Дойникова Е.В., Котенко Д.И. Инструментальные средства анализа защищенности автоматизированных систем //Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. 5-10 июля 2010 года /СПб.: Изд-во Политехнического университета. 2010. С. 115–116.
10. Федотов А. М. Информационная безопасность в корпоративной сети//Проблемы безопасности и чрезвычайных ситуаций. М.: ВИНИТИ, 2008. № 2. С. 88–101.

References

1. Postanova Kabinetu ministriv Ukrayiny vid 08.10.1997 № 1126 «Pro zatverdzhennya Kontseptsiyi tekhnichnoho zakhystu informatsiyi v Ukrayini»
2. Khoroshko V.O., Yur'yev A.N. Metodolohichnyy pidkhid do optymal′noho vyboru kompleksu zakhodiv shchodo zakhystu informatsiyi // Zakhyst informatsiyi: Zb. nauch. tr. K .: NAU, 2001. S. 132-136.
3. Lakhno V.A., Petrov A.S., Skrypkina A.S. Pobudova dyskretnykh protsedur rozpiznavannya i poshuku vrazlyvostey informatsiyi // Informatsiyna bezpeka, 2010. № 2 (4). S. 5-13.
4. Khoroshko V.O., Chekatkov A.A. Metody i zasoby zakhystu informatsiyi. K. vydavnytstvo Yunior, 2003. 504 s.
5. Bezshtan′ko V. Analiz isnuyuchikh prohramnykh ZASOBIV ta metodyk OTSINKY stanu informatsiynoyi bezpeky orhanyzatsyy // Byznes y bezopasnost′, №1. 2007. s.32 - 35.
6. Yezhova L.F., Machalin I.O., Nevoyt YA.V., Khoroshko V.O. Upravlinnya informatsiynoyu bezpeky. K .: Vyd. DUIKT, 2011 roku.
7. Dehtyar′ova L.M., Voloshko S.V., Loza V.V., Bulankina A.O. Vykorystannya informatsiynykh tekhnolohiy Obrobka danykh v SUCHASNYKH systemakh transportnoyi lohistyky // Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony, № 1 (37) / 2020. K: Natsional′nyy universytet oborony Ukrayiny imeni Ivana Chernyakhovs′koho, 2020. s. 139-144
8. ND TZI 1.5-002-2012 Klasyfikator ZASOBIV tekhnichnoho zakhystu informatsiyi, uchet nakazom administratsiyi Derzhspetszv'yazku vid 29.08.2012 № 472
9. Kotenko I.V., Stepashkin Stanislav Ivanovych M.V., Chechulyn A.A., Doynykova YE.V., Kotenko D.I. Instrumental′ni zasoby analizu zakhyshchenosti avtomatyzovanykh system // Metody i tekhnichni zasoby zabezpechennya bezpeky informatsiyi. Materialy KHIX Zahal′norosiys′koyi naukovo-tekhnichnoyi konferentsiyi. 5-10 lypnya 2010 hoda / SPb .: Yzd-vo Politekhnichnoho universytetu. 2010. C. 115-116.

10. Fedotov A. M. Informatsiyna bezpeka v korporatyvniy merezhi // Problemy bezpeky ta nadzvychaynykh sytuatsiy. M .: VINITI, 2008. № 2. S. 88-101.

Degtyaryova L.M., Vakulenko Y.V., Odarushchenko O.B. Control of technical condition of component elements of information protection systems.

The article analyzes the approaches to the selection and construction of control systems for the technical state of information security systems. The control system should process information on the degree of operability of the controlled system based on the measuring changing processes. This system can have two types of control: dynamic and statistical, each of which has its own actions, which are determined by two factors: control time and control reliability. In the analysis information security systems, it is necessary to take into account that this is a complex system consisting of subsystems with many functions: the security system, the control system and the decision support system. It should be noted that the control systems for the state of protection systems and the protection systems themselves are dynamic.

A dynamic system is a mathematical model of some object, process or phenomenon, which can be represented as a system for which some states are described, when a dynamic system describes the behavior of this process as a sequence of transitions from one state to another.

Static control is mainly used to determine systems in which the amplitude or other parameters are constant.

The mathematical representation of a dynamic system, that contains variables of the initial state of the system and the variables characterizing the transformed state, taking into account the interdependence of the variables: a set of points in time, a set of instantaneous values of input signals, a set of permissible input signals, a set of output signals, a set of permissible output signals, set of system states and set of system parameters. The task of monitoring a dynamic system is to generate input signals, measure output signals based on these changes in parameters and the degree of system operability by comparing the obtained parameter values with their permissible values.

The efficiency of using a specific approach or mathematical apparatus is justified by the following factors: the presence or absence of sufficiently accurate information about the composition and characteristic of the system elements, the type or forms of input and output information, devices and software of a unified protection system.

Keywords: *dynamic system, technical protection of information, information security threats, information processes*

Дегтярьова Л.М. – доцент кафедри Інформаційних систем та технологій Полтавської державної аграрної академії;

Вакуленко Ю.В. – доцент, керівник Навчально-наукового інституту комунікаційних та інноваційних освітніх технологій Полтавської державної аграрної академії;

Одарущенко О.Б. – доцент кафедри Інформаційних систем та технологій Полтавської державної аграрної академії

Стаття подана 21.05.2021.