Розпізнавання аномальних станів в інформаційно-телекомунікаційних системах при нечіткому описі подій

© Зубок В.Ю. © Захарченко О.І. © Бєланов Ю.О.
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»,
Київ, Україна
vitaly.zubok@gmail.com zakharchenko1995@ukr.net belano8@ukr.net

Анотація

У роботі розглянуто найнебезпечніші сучасні кібератаки, зокрема, групи «ransomware», та фази їхнього проходження. З'ясовано, що корпоративні системи захисту є недостатньо надійними супротив атак класу «ransomware». Однією з причин є те, що виявлення пасивних ботів системами антивірусної перевірки дедалі ускладнює через змінність програмного коду, поведінку ботів, їхню різноманітність, в той час як існуючі системи виявлення кібератак здебільшого спираються на макрооприси (сигнатури тощо), що представляють попередньо ідентифіковані відомі загрози безпеці.

Водночас, у складі будь-якої ІТС присутні системи моніторингу (контролю працездатності). Програмне забезпечення моніторингу численних параметрів мережі а також стану і працездатності серверів використовує гнучкий механізм повідомлень, що дозволяє користувачам налаштовувати оповіщення по e-mail, sms, онлайн-месенджерам практично для будь-якої події. Накопичення та аналіз даних від таких підсистем дозволяє вести спостереження за груповими відхиленнями від звичайного стану в компонентів ІТС. Такі відхилення, в свою чергу, можуть бути наслідками прихованого шкідливого зовнішнього впливу чи використання ІТС для реалізації кібератак.

Знання принципів і механізмів реалізаіції кібератак дає можливість сформулювати критерії зміни стану системи під впливом кібератаки. Матеріали, викладені в роботі, демонструють, що для виявлення таких змін стану можуть бути використані звичайні системи контролю працездатності (моніторингу) ІТС. Багатовекторний аналіз даних, отриманих від систем моніторингу працездатності, дає можливість виявлення шкідливого зовнішнього впливу при відсутності чітких характеристик такого впливу та без попереднього опису притаманних такому впливові подій. Це відкриває перспективу підвищення ефективності виявлення інфікованих об'єктів в ІТС.

В роботі приведено огляд деяких методів аналізу, прийнятних для поставленої задачі, та певний функціональний підхід до розпізнавання аномальних станів в ІТС за допомогою популярних систем моніторингу працездатності.

1 Вступ

Протягом останнього часу зростає кількість та складність кібератак на промислові підприємства, органи влади та державні установи. Атаки виконуються шляхом впливу на веб-сайти, інші мережеві служби, телекомунікаційне обладнання, спрямовані на загрозу конфіденційності, цілісності, доступності даних, а також на послаблення спостережності і керованості системами, де передається, оброблюється, зберігається інформація [1,2,3].

Зазвичай вважається, що виявлення атак є функцією окремих спеціалізованих та коштовних програмно-апаратних комплексів. В той же час у складі будь-якої ІТС присутні системи моніторингу (контролю працездатності). Програмне забезпечення моніторингу численних параметрів мережі а також стану і працездатності серверів використовує гнучкий механізм повідомлень, що дозволяє користувачам налаштовувати оповіщення по e-mail, sms, онлайн-месенджерам практично для будь-якої події. Це дає можливість швидко зреагувати на проблеми. Таке програмне забезпечення пропонує широкі можливості звітності і візуалізації, базуючись на зібраних даних. Інструменти моніторингу найчастіше чудово піддаються горизонтальному і вертикальному масштабуванню і можуть бути використані для виявлення факту зміни стану системи під впливом кібератаки.

Отже, моніторинг стану підсистем ІТС є рутинною процедурою. Накопичення та аналіз даних від таких підсистем дозволяє вести спостереження за груповими відхиленнями від звичайного стану в компонентів ІТС. Такі відхилення, в свою чергу, можуть бути наслідками прихованого шкідливого зовнішнього впливу чи використання ІТС для реалізації кібератак.

Будь-яка атака, в залежності від механізму, залишає слід у вигляді зміни кількісних і якісних характеристик багатьох параметрів. Наприклад, якщо DDoS порівняно легко ідентифікується з боку жертви, то з боку ураженого комп'ютера-бота атаку виявити складно. Проте, наявність в підконтрольній мережі декількох комп'ютерів, що одночасно виконують однакові мережеві операції, виявити набагато легше.

2 Постановка задачі

Існуючі системи виявлення кібератак здебільшого спираються на макрооописи (сигнатури тощо), що представляють попередньо ідентифіковані відомі загрози безпеці. Системи моніторингу ІТС відстежують критичні характеристики мережі в режимі реального часу або з певною періодичністю, та сигналізують про перехід числових характеристик через певні встановлені рівні. Багатовекторний аналіз накопичених даних такого моніторингу може слугувати альтернативним джерелом інформації для виявлення шкідливого зовнішнього впливу при відсутності чітких характеристик такого впливу та без попереднього опису притаманних такому впливові подій. Для цієї мети необхідно:

- розробити моделі збору та накопичення даних за допомогою існуючих та широко вживаних систем моніторингу
- обрати методи та моделі дослідження даних, зібраних та накопичених системами моніторингу для автоматичного виявлення аномалій, спричинених шкідливим зовнішнім впливом на ІТС.

3 Найбільш небезпечні кібератаки та проблеми їхнього виявлення

Попри різноманіття сучасних кібератак, найбільш небезпечними вважаються атаки типу розподілена атакак відмови в обслуговуванні (DDoS) та програми-здирники (Ransomware) [4].

Як відомо, атаки типу DDoS направлені на «виснаження ресурсів». Взагалі відмова сервісу здійснюється примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу. Інший варіант – заняття комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість інформаційного обміну перестає відповідати встановленим для нього вимогам. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто синтаксично некоректним з точки зору протоколу, на якому він формулюється). Таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що це можна кваліфікувати як порушення доступності.

Програми-здирники (ransom – викуп) після завантаження на комп'ютер виконують проникнання в операційну систему та за командою активації (канали отримання цих команд не описуються в даній роботі) блокують роботу користувача в операційній системі, замість того демонструючи попередження із загрозою і з зазначенням суми викупу, яку треба заплатити за «порятунок» всієї інформації. Ці повідомлення розрізняються залежно від типу шкідливої програми. Атака на цілісність інформації в сучасних версіях ботів реалізується шляхом шифрування вмісту комп’ютерних носіїв, при чому ключ від шифру ніби-то існує в зловмисника і може бути «придбано» в нього.

Обидва описані типи найбільш небезпечних сучасних кібератак мають принаймні дві фази: фазу інфікування та активну фазу. Шкідливий програмний код заховано усередині іншого файлу або програми, яка виглядає настільки безвинно, що користувач спокійно їх відкриває: вкладення в електронні листи, відео зі сторінок сумнівного походження або навіть системні оновлення від особи надійних програм, таких як Windows або Adobe Flash.

У випадку атак класу DDoS інфіковані елементи однієї підмережі (так звані боти) часто використовуються для атак на іншу мережу. У випадку атак класу Ransomware активна фаза атаки спрямована безпосередньо на користувачів власної мережі. Події останніх років довели слабку ефективність корпоративних систем захисту супротив зараження комп’ютерів ботами, зокрема, класу Ransomware. Однією з причин є те, що виявлення пасивних ботів системами антивірусної перевірки дедалі складнішає через змінність програмного коду, поведінку ботів, їхню різноманітність [5]. Така сама проблема і з ботами, що приймають участь в атаках DDoS. Але у зв’язку з іншою архітектурою активної фази таких атак, власник інфікованих пристроїв може не зазнати жодних втрат і навіть не дізнатись про участь в атаці, а отже – і про наявність ботів у власній ІТС.

Отже, необхідні нові методи та інструменти виявлення ботів, які б збільшили вірогідність виявлення першого етапу атаки (інфікування), та якомога швидше ідентифікували ботів в той момент, коли вони вступають в активну фазу атаки. Такі методи можуть полягати в дослідженні групових відхилень від звичайного стану роботи різноманітних підсистем ІТС.

4 Виявлення аномальних станів сучасних ІТС

В попередньому розділі показано, що необхідні нові методи та інструменти, які б дозволили виявляти атаку на етапі зараження. Такі методи можуть полягати в дослідженні групових відхилень від звичайного стану роботи різноманітних підсистем ІТС.

Загалом, аномалії можуть досліджуватись:

- в загальному трафіку та в трафіку окремих елементів ІТС (загальний обсяг, кількість сесій, групування по адресі джерела, адресі призначення, протоколах тощо);
- в активних елементах ІТС, насамперед в серверах, а також в окремих програмних процесах (кількість, час виконання, групування по запитах, відповідях тощо).

В залежності від місця дослідження мають бути обрані засоби збору та накопичення даних, а також та методи їхнього дослідження.

Для визначення атаки за характером трафіку, система повинна навчатись визнавати нормальну активність системи. Для цього потрібні дві фази: тренування, де будується профіль звичайної поведінки, та тестування, де поточний трафік чи картина подій порівнюється з профілем, створеним на етапі навчання. Аномалії виявляються кількома способами, найчастіше з використанням методів штучного інтелекту. Вже понад 10 років досліджується можливість повністю автоматичного поведінкового аналізу трафіку з метою виявлення атак.

В роботі [6] використовується навчання детектора «типовому» профілю трафіку та виявлення аномалій на осонові відстані Магаланобіса. Детектор аномалії фіксує вхідні "корисні навантаження" (payload) та перевіряє корисне навантаження на його узгодженість (або відстань) від моделі центроїда. Це досягається шляхом порівняння двох статистичних розподілів.

Використовувана метрика відстані являє собою метрику відстані Магаланобіса, яка застосовується до кінцевої дискретної гістограми частоти символів, що обчислюються на етапі навчання. Будь-яке нове тестове корисне навантаження, яке виявилося занадто далеким від нормального очікуваного корисного навантаження, вважається аномальним та генерує попередження.

Попередження може бути співвіднесено з іншими даними датчиків, і процес прийняття рішення може відповісти кількома можливими діями. Залежно від політики безпеки захищеного сайту, можна фільтрувати, переадресовувати або навпаки, перехоплювати мережеве з'єднання та доправляти "отруйний" трафік на дослідження.

В роботі [7] пропонуються методи виявлення вторгнень шляхом складання профілю легітимних користувачів. Запропоновано трактування аномалії як події, які впливають на "спектр" трафіку, де обсязг трафіку є одним з показників. Такий трафік-аналіз аналіз має дві основні переваги.

По-перше, це дозволяє виявити аномалії, які важко ізолювати дослідженням обсягу трафіку. Деякі аномалії такі як сканування (probing) або специфічні атаки DOS прикладного рівня можуть мати незначний вплив на обсяг трафіку магістральної лінії, і, мабуть, краще можуть бути виявлені шляхом систематичного аналізу змін в розподілі замість зміни обсягу.

По-друге, незвичайні розподіли виявляють цінні відомості про структуру інформаційних аномалій, які відсутні при вимірюванні обсягів трафіку. Досліджується структура впливу аномалії на характер трафіку і за допомогою цього проводиться автоматична класифікація аномалій по значимих категоріях. Автори вважають це прогресом порівняно з евристичним дослідженням аномалій, заснованим на правилах, бо саме такий метод може виявити нові, невідомі аномалії.

Важливим напрямком захисту є виявлення аномалій в поведінці користувачів шляхом аналізу протоколів рівня застосувань. В роботі [8] запропоновано розширену напівмарківську модель (HsMM) для опису поведінки веб-користувачів. Щоб зменшити обсяг обчислень, пов’язану з просторовою складністю моделі, запропоновано модифікований алгоритм.

У якості критерію вимірювання нормальності користувача використовується ентропія його HTTP-запитів. Поведінка користувача описується як періодична зміна станів між «кліком» на гіперпосилання та читанням отриманого матеріалу і описується за допомогою прихованої напівмарківської моделі (HsMM). Веб-сайт, яки є потенційно атакованим, описується за допомогою марківського простору станів. Кожен основний напівмарковський стан використовується для представлення унікальної веб-сторінки, натиснутою веб-користувачем. Таким чином, матриця ймовірності стану переходу представляє відношення гіперпосилання між різними веб-сторінками. Тривалість стану представляє кількість HTTP-запитів, отриманих веб-сервером, коли користувач переходить за «кліком» на відповідну сторінку. Вихідна символьна послідовність кожного стану представляє ті запити на натиснутій сторінці, які проходять через всі проксі або кеш браузера і, нарешті, надходять на веб-сервер.

Метод містить декілька послідовностей спостереження за поведінкою декількох користувачів, отримується алгоритм переоцінки HsMM для декількох послідовностей спостережень за частотою в цій статті. Автори розробили алгоритм переоцінки, встановлюється новий HsMM для опису звичайної поведінки веб-користувачів, просуваючи модель із набору послідовностей запитів, зроблених багатьма звичайними користувачами. Визначається відхилення від середньої ентропії даних тренувань і це й є аномалія спостережуваної послідовності запиту, яку виконує користувач. Чим менше відхилення, тим вище нормальність спостережуваної послідовності.

4 Огляд та перспективи використання систем моніторингу працездатності ІТС з метою виявлення прихованих впливів

Існує багато вдалих та широко вживаних рішень з автоматизації такого моніторингу, зокрема, для серверів на базі UNIX-подібних операційних систем. Збір, накопичення та збереження даних для такого аналізу можуть виконувати системи моніторингу працездатності. Найбільш широко вживаними системами, за власними спостереженнями автора, є Nagios, Cacti та Zabbix.

Система Nagios складається з двох складових. Перша - це серверна частина (Nagios Core), основне завдання якої - обробка даних (отриманих від агентів і зовнішніх програм) і оповіщення при досягненні

критичних станів. Сервер Nagios встановлюється тільки на Unix-подібні ОС. Для включення в моніторинг будь-якого сервісу чи системи необхідно в конфігураційних файлах прописати їх параметри, а також підключити графіки і плагіни. Статистика може виводитися по хостах, по процесах і службах, по помилках, як окремо, так і у вигляді груп. В результаті виходить сформований звіт зі зведеними таблицями і діаграмами в процентному і числовому співвідношенні за потрібний період, який є помічником при аналізі інцидентів. Можливість розширення штатного функціоналу Nagios досягається за рахунок підключення великої кількості плагінів (ручна установка), які дозволяють створювати свої способи перевірки служб і обробників подій.

Система Cacti є веб-застосунком, збирає статистичні дані за певні часові інтервали і дозволяє відобразити їх у графічному вигляді. Переважно використовуються стандартні шаблони для відображення статистики по завантаженню процесора, виділенню оперативної пам'яті, кількістю запущених процесів, використання вхідного та вихідного трафіку. Для візуалізації використовується стандартний інструмент реєстрації даних RRDtool. Так Cacti дозволяє користувачеві опитати послуги за заданими інтервалами та графік отриманих даних. Він зазвичай використовується для графіка даних про часові ряди таких показників, як завантаження процесора та використання пропускної здатності мережі. Також звичайно використовується для моніторингу мережевого трафіку шляхом опитування мережевого комутатора або інтерфейсу маршрутизатора через простий протокол керування мережею (SNMP).

Основними особливостями Cacti є:

- гнучкість конфігурування джерел даних за допомогою шаблонів;
- гнучкість механізму та періодичності отримання даних;
- необмежена кількість графічних елементів;
- автоматична побудова мережі у вигляді графа;

Окремої згадки потребує **RRDTool**. «Round Robin Database Tool» - це програмний засіб для зберігання, впорядкування та аналізу великої кількості даних від моніторингу. Частина аналізу даних RRDtool базується на здатності швидко генерувати графічні уявлення значень даних, зібраних протягом певного періоду часу.

RRDtool приймає дані про часові змінні в інтервалах певної довжини. Цей інтервал, який зазвичай називається «крок», вказується при створенні файлу RRD і не може бути змінений пізніше. Оскільки дані не завжди доступні в потрібний час, RRDtool буде автоматично інтерполювати будь-які надані дані, щоб відповідати його внутрішнім крокам часу.

Значення для певного кроку, який був інтерполізований, називається первинною точкою даних (PDP). Кілька PDP можуть бути об'єднані відповідно до функції консолідації (CF) для формування консолідованої точки даних (CDP). Типова функція консолідації - середня, мінімальна, максимальна.

Після того, як дані були об'єднані, результуючий CDP зберігається в циклічному архіві (RRA). Циклічний архів зберігає фіксовану кількість CDP і вказує, скільки PDP потрібно об'єднати в один CDP і який CF використовувати. Коли архів добіг останнього «кроку», він буде «обертатися»: наступна вставка перезапише найстаріший запис. Завдяки цій властивості бази даних RRDTool завжди мають однаковий фіксовний об’єм.

Аналіз та візуалізація даних моніторингу є типовими сферами застосування RRDTool.

Система Zabbix також є системою моніторингу, яка складається з декількох компонентів. Zabbix-сервер - ядро системи, яке може віддалено перевіряти мережеві сервіси і є сховищем, в якому зберігаються всі конфігураційні, статистичні та оперативні дані. До функцій сервера також належить оповіщення. Zabbix-проксі збирає дані про продуктивність і доступність від імені Zabbix-сервера.

Всі зібрані дані заносяться в буфер на локальному рівні та передаються Zabbix-сервера, до якого належить проксі-сервер. Він може бути також використаний для розподілу навантаження одного Zabbix-сервера. В цьому випадку, проксі тільки збирає дані, тим самим на сервер лягає менше навантаження на процесор і системи введення-виведення. Zabbix-агент - програма контролю локальних ресурсів і додатків (таких як накопичувачі, оперативна пам'ять, статистика процесора і так далі) на мережевих системах, ці системи повинні працювати з запущеним Zabbix-агентом.

Отже, обидві системи надають широкі можливості для моніторингу, звітування, візуалізації зібраних даних. Інструменти моніторингу обох систем допрацьовуються до подтреб певної ІТС завдяки широким можливостям конфігураційних параметрів та наявності власних мов скриптового програмування для побудови власних процедур. Також, ці системи чудово піддаються горизонтальному і вертикальному масштабуванню.

Опишемо шляхи практичного використання обох систем з метою виявлення факту зміни стану системи під впливом кібератаки.

Завдяки засобам зберігання та накопичення результатів моніторингу та наявності засобів розширення функціоналу, перелічені системи можуть використовуватись для сигналізування про зміну поведінки елементів системи в разі розробки і підключення модуля для аналізу, який можна назвати аналізом поведінки.

Наступний набір функцій для системи виявлення аномалій дозволить їй функціонувати та розвиватись:

1) збір даних;
2) навчання: визначення характеристик нормального стану;
3) моніторинг;
4) виявлення відхилень;
5) отримання негативного зворотного зв’язку;
6) коригування порогових значень для характеристик нормального стану.

Негативний зворотний зв'язок необхідний для навчання системи. Із плином часу характеристики нормального стану ІТС змінюються, отже для коригування порогових значень необхідно передбачити можливість автокорекції.

Розглянемо приклади деяких даних, збір та накопичення яких необхідно забезпечити системами моніторингу для подальшого профілювання системи та виявлення аномалій стану, викликаних кібератаками:

- аудит подій входу в систему: кількість входів в одиницю часу, кількість вдалих входів, невдалих спроб, причини невдалих спроб;
- аудит керування обліковими записами: створення, видалення облікового запису, зміна паролі чи інших атрибутів автентифікації, як на рівні операційної системи, так і по кожному з сервісів, де є автентифікація;
- кількість унікальних IP-адрес, з яких надходять запити;
- кількість запитів, що надсилаються на адресу певного ресурсу;
- швидкість трафіку на мережевому інтерфейсі загальна, по протоколах, по адресах «внутрішніх» хостів;
- кількість запитів до ресурсу по типах запитів та ідентифікаторах ресурсу (URI);
- кількість невиконаних запитів, по типах помилок.

Перелік є початковим. Передбачається, що по кожному мережевому сервісу, який потенційно може бути використаний із зловмисними цілями, має бути складено окремий перелік параметрів, що повинні спостерігатись (бути включені в моніторинг).

На прикладі основного шляху зараження – повідомлень e-mail, можна скласти більш конкретний перелік, який стосуватиметься спостереження за журналом сервера e-mail та активності роцесів на локальних робочих станціях, перш за все, під керуванням ОС Windows.

6 Висновки

Знання принципів і механізмів реалізаіцї кібератак дає можливість сформулювати критерії зміни стану системи під впливом кібератаки. Для виявлення таких змін стану можуть бути використані звичайні системи контролю працездатності (моніторингу) що широко застосовуються в сучасних ІТС. Таке програмне забезпечення пропонує широкі можливості звітності і візуалізації, чудово піддаються горизонтальному і вертикальному масштабуванню.

Багатовекторний аналіз даних, зібраних цими системами, може бути застосований для виявлення факту зміни стану системи під впливом кібератаки, в тому числі дозволить виявляти аномалії від подій, чіткого опису яких ще не існує. Це відкриває перспективу підвищення ефективності виявлення прихованих атак, а також виявлення та ідентифікації інфікованих об'єктів в ІТС.

Література

1. Internet Security Threat Report 2016. [Електронний ресурс]. Доступно: https://www.symantec.com/security-center/threat-report. Дата звернення: Кві.20, 2017.
2. M-Trends 2017: Trends from the year's breaches and cyber attacks. [Електронний ресурс]. Доступно: https://www.fireeye.com/current-threats/annual-threat-report.html. Дата звернення: Тра.1, 2017.
3. The Ukrainian Power Grid Was Hacked Again. [Електронний ресурс]. Доступно: https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report. Дата звернення: Кві.20, 2017.
4. Комплексный подход по защите от направленных атак и вымогательского ПО типа Ransomware. [Електронний ресурс]. Доступно: https://habrahabr.ru/company/infosecurity/blog/331700/. Дата звернення: Лис.18, 2017.
5. Ботнеты. [Електронний ресурс]. Доступно: https://securelist.ru/botnety/155/. Дата звернення: Лис.16, 2017.
6. Ke Wang. Anomalous Payload-Based Network Intrusion Detection / Ke Wang, Salvatore J. Stolfo // RAID 2004: Recent Advances in Intrusion Detection. - Pages 203-222.
7. A.S.Syed Navaz. Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud / A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi // International Journal of Computer Applications (0975 – 8887). – Vol.62. – No.15. – Jan.2013.
8. Yi Xie. A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors / Yi Xie, Shun-Zheng Yu // IEEE/ACM Transactions On Networking. - Vol. 17. - №1.- Feb. 2009.

Recognition of Abnormal State in Computer Network Systems with Fuzzy Description of Events

© Vitalii Y. Zubok © Olexandr I. Zakharchenko © Yurii O. Belanov
Institute of Special Communication and Information Protection of
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
vitaly.zubok@gmail.com zakharchenko1995@ukr.net belano8@ukr.net

Abstract

In this paper we first of all describe the most dangerous modern cyber attacks, in particular, known as “ransomware”, and their phases. It is considered that computer and network security systems of corporate level are not sufficiently reliable against “ransomware” class of attacks. there are several reasons of it, however one of the main reasons is that the detection of passive bots by traditional antivirus checking systems become too complex ergo less effective due to variability of the malicious program code of bots, the behavior of bots, and their diversity, while existing cyberattack detection systems rely mostly on macro descriptions (e.g. signatures) that represent pre-identified and already known security threats.

At the same time, we can say without any overstatement that any computer network system consists of particular monitoring module or subsystem which is designed for performance and availability monitoring. This software provides monitoring of all “mission-critical” infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. It can use a flexible messaging mechanism that allows users to customize alerts by e-mail, SMS, online messengers for virtually any event.

Accumulation and analysis of data from such subsystems allows monitoring of group deviations from the normal state into computer network system components. Such deviations, in turn, may be the consequence of latent harmful external influences or the use of computer network system for the implementation of cyber attacks.

Knowledge of the principles and mechanisms of the implementation of cyber attacks makes it possible to formulate criteria for changing the state of the system under the influence of cyber attacks. The materials presented in this paper demonstrate that for the detection of such changes of state, computer network system can be used for monitoring the performance (monitoring) of the computer network system. The multi-vector analysis of data obtained from performance and availability monitoring systems allows detection of harmful external influences in the absence of clear characteristics of such impact and without a prior description of the inherent effects of such events. This opens up a pivot point for increasing the effectiveness of detecting infected objects in computer network system.

The paper gives an overview of some methods of analysis that are acceptable for a given task, and a certain functional approach to the recognition of abnormal states in ITS with the help of popular performance monitoring systems.