УДК 004.451.36:681.5

РОЗРОБЛЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ЗАХИСТУ ПОЛІГРАФІЧНИХ ПІДПРИЄМСТВ ТА ВИДАВНИЦТВ

В. І. Сабат, В. Т. Драгомірова

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Системи захисту поліграфічних підприємств та видавництв орієнтовані на виявлення і протидію зовнішнім та внутрішнім загрозам, які призводять до атак і порушень їхнього нормального функціонування. Сьогодні більшість захищених організацій використовують у своїй діяльності мережні технології та засоби зв'язку, тому важливо забезпечити їхню безперебійну роботу в режимі зовнішніх загроз та атак і розробити стратегію на рівні політики безпеки для контролю і протидії виникненню можливих негативних факторів. Проаналізовано сучасні системи виявлення вторгнень (IDS) у комплексі систем захисту поліграфічних підприємств та видавництв, описано небезпечні події, які вони можуть відстежувати, наведено засоби протидії та контролю можливим атакам і випадковим подіям, що не мають ознак атак, на основі чого запропоновано алгоритм розгортання IDS для протидії зовнішнім атакам. Важлива увага приділена процесу проєктування IDS, їхнього встановлення та налаштування в системі захисту організацій. Особливість таких систем виявлення вторгнень полягає у тому, що, окрім загальних глобальних налаштувань, прийнятих програмно при інсталяції, надається можливість визначити локально небезпечні події, що можуть негативно вплинути на роботу поліграфічних підприємств та видавництв, встановити допустимі межі для різних ознак атак та відповідні контрзаходи для запобігання їхньому здійсненню. Обґрунтовано, що для успішної роботи IDS, які проєктуються для автоматизованих систем документообігу (АСДО) при управлінні поліграфічним виробництвом (ПВ), доцільно використовувати вузлові IDS (HIDS), а для розпізнавання і протидії зовнішнім атакам — мережні IDS (NIDS). На основі проведених досліджень різних засобів IDS, цілей їхнього використання та методів опрацьовування небезпечних подій, які виникають при порушені безпеки у ПВ, запропоновано загальний принцип роботи системи захисту поліграфічних підприємств та видавництв з IDS у вигляді функціональної схеми.

Ключові слова: *системи захисту, системи виявлення вторгнень, атаки, поліграфічні виробництва, автоматизовані системи документообігу.*

Постановка проблеми. Сучасні системи захисту будь-яких організацій базуються на поєднанні традиційних фізичних засобів захисту із сучасними мережними інформаційними технологіями, які дозволяють в реальному режимі часу відслідковувати небезпечні події, надавати попереджувальні сигнали про небезпеку

відповідним службам захисту і прогнозувати можливі атаки через контроль трафіка мережі. Це дозволяє виявити процес здійснення атаки ще на початку її створення та убезпечити організацію від можливих інцидентів і наслідків від зовнішніх чи внутрішніх атак. Такі дії, як атаки, при відсутності відповідних контрзаходів зазвичай призводять до значних збитків організації, а в деяких випадках ці збитки можуть завдати непоправної шкоди. Впровадження систем виявлення вторгнень (IDS) в захищені інформаційні системи поліграфічних виробництв (ПВ), до яких можуть належати активи ПВ у вигляді комп'ютерних систем, поєднаних у локальну мережу, засобів їхнього обслуговування і надання додаткових послуг користувачам, серверів та засобів захисту, полягає в тому, щоб не тільки відслідковувати будь-які небезпечні події, але й унеможливлювати їхній подальший розвиток і здійснення.

Аналіз останніх досліджень та публікацій. Виконані дослідження з цієї тематики присвячені аналізу сучасних систем виявлення атак та запобігання вторгненням в інформаційно-телекомунікаційних системах [1, 2], розробленню технологій виявлення атак і вторгнень [3, 4], методів ідентифікації аномальних станів для систем виявлення вторгнень [5]. Водночас недостатньо уваги приділено розробленню системи виявлення вторгнень для поліграфічних виробництв, які використовують мережні технології.

Мета статті – розроблення системи виявлення вторгнень в АСДО (автоматизовану систему документообігу) для поліграфічних підприємств та видавництв та вибору алгоритму захисту і протидії атакам.

Виклад основного матеріалу дослідження. Для протидії зовнішнім атакам та запобігання можливим вторгненням в роботу АСДО у будь-якій захищеній організації чи на підприємстві необхідно встановити системи управління вторгнень. Для цього на етапі планування систем безпеки необхідно забезпечити вузлові засоби захисту у вигляді датчиків для кожного робочого місця локальної мережі, а також мережні екрани і датчики для доступу до зовнішньої мережі Інтернет. Служби безпеки з системними адміністраторами повинні розробити політику безпеки для управління IDS і в процесі роботи ПВ впроваджувати її, модифікувати відповідно до будь-яких змін в структурі видавництва, періодично здійснювати сканування вразливостей системи захисту, а також аналізувати журнали подій та будь-яких інцидентів, що порушують політику безпеки ПВ в цілому. Таким чином, впроваджена у ПВ система виявлення вторгнень буде доповнювати наявні системи та засоби захисту від зовнішніх та внутрішніх атак, зменшуючи вразливість роботи як АСДО, так і ПВ та збільшуючи надійність їхнього функціонування.

Перед ухваленням у ПВ рішення про використання IDS (чи то комерційна система, чи некомерційна) керівництво ПВ повинно чітко визначити цілі застосування програми. Правильне налаштування і управління IDS вимагає великих зусиль, які слід якомога ефективніше використовувати для виявлення атак (за допомогою реалізації хорошої програми із забезпечення безпеки).

З урахуванням вищесказаного, якщо ухвалено рішення про застосування IDS, то для успішної реалізації програми необхідно забезпечити наявність всіх потрібних

ресурсів. Якщо цілі програми IDS містять можливість моніторингу атак в цілодобовому і щоденному режимі, співробітникам організації необхідно працювати сім днів на тиждень. В той же час системним адміністраторам потрібно буде працювати із співробітниками, відповідальними за безпеку, для визначення успішного або безуспішного проведення атаки й у разі успішної атаки для визначення методу обробки інциденту. В ідеальному випадку процедура з обробки інциденту повинна бути створена і протестована перед застосуванням системи IDS.

Система виявлення вторгнень може тільки видавати звіти про ті події, на виявлення яких вона налаштована. Конфігурація IDS складається з двох компонентів — це ознаки атак, запрограмовані в системі, та будь-які додаткові, визначені адміністратором, події, що також становлять загрозу. Серед цих подій можуть бути певні типи трафіка або повідомлень журналу.

За умови правильної конфігурації можна навести чотири типи подій, про які повідомлятиме система IDS [4]:

1. Події дослідження.
2. Атаки.
3. Порушення політики.
4. Підозрілі або нез'ясовані події, яким приділятиметься велика частина часу.

До подій дослідження можна віднести усі дії, пов'язані із спробами зловмисника зібрати інформацію про систему захисту перед тим, як її атакувати. Це приховане сканування трафіка передання інформації через мережу Інтернет, сканування портів, антивірусних програм та вразливостей системи на впровадження шкідливого коду, відстеження документообігу в системі АСДО. Зокрема, відстеження електронних документів та дозволів на їхнє використання, що відбувається всередині ПВ, передання інформації локальною мережею, тому виявити такі дії можуть лише вузлові системи виявлення вторгнень (HIDS), які працюють за принципом зчитування інформації про порушення безпеки за допомогою вузлових датчиків. Такі датчики встановлюються на кожну робочу станцію та сервер, що контролює обмін інформації між користувачами і працює в системі управління доступом.

При виявленні події, яка входить у категорію та ознаку атаки, необхідно негайно приймати відповідні дії щодо її усунення та задіяння контрзаходів з припинення реалізації атаки ще на початку її локалізації. Зазвичай зовнішні атаки розпізнають мережні системи виявлення вторгнень (NIDS), які містять усі ознаки виявлення та впровадження атак за допомогою мережних датчиків та аналізу трафіка інформації, що йде із зовнішньої мережі Інтернет. Наприклад, якщо мета IDS полягає у виявленні атак, а IDS розташована в мережі Інтернет за межами міжмережного екрана ПВ, то використовують NIDS, яка буде відстежувати весь трафік, що надходить на міжмережний екран, для виявлення вхідних атак. NIDS можна ще розмістити в межах зони локальної мережі, що захищається міжмережним екраном, для визначення тих атак, які успішно подолали міжмережний екран. Це дозволить збільшити імовірність того, що атака буде виявлена і локалізована до її повного впровадження зловмисником.

Необхідно звернути особливу увагу на те, як повинні оброблятись події та які контрзаходи повинні використовуватись насамперед для того, щоб визначити тип атаки і встановити подальший алгоритм необхідних заходів протидії. При цьому важливим є завдання не тільки розпізнавання подій, але й забезпечення безперервної роботи системи, особливо, якщо її функціонування тісно пов'язане з мережними технологіями. Це можуть бути, наприклад, електронні комунікативні зв'язки з постачальниками послуг або клієнтами, замовниками продукції. У цьому випадку будь-які дії, що призведуть до обмеження доступу до мережі ПВ санкціонованих користувачів, можуть негативно вплинути на іміджеву рекламу компанії і спровокувати подальше відсіювання потенційних клієнтів. Тому переважно використовують пасивну обробку подій, коли після розпізнавання атаки і визначення її рівня ризику для ПВ (у доступних межах) системний адміністратор з відповідними службами визначають подальші дії для її усунення. При активних контрзаходах може бути автоматично здійснено переривання роботи системи з метою уникнення значних збитків від впровадження атаки. Це в основному стосується DDoS-атак, але в цьому випадку зростає імовірність помилкового визначення події як атаки і відмови в обслуговуванні легітимних користувачів. Тому необхідно провести детальний аналіз потенційних можливостей помилкових сигналів тривоги, перш ніж виконувати відповідну операцію.

При порушенні політики безпеки насамперед аналізуються внутрішні дії співробітників та суб'єктів АСДО щодо дотримання заходів та процедур, описаних в політиці безпеки. Це може бути, наприклад, недотримання політики використання паролів в системі, використання недозволених процедур при роботі з інформацією, документами, електронною поштою, зовнішніми сайтами в мережі інтернет тощо.

Особливий розділ в системі виявлення вторгнень присвячений виявленню підозрілих подій, тобто таких подій, що не входять в ознаки атак, тому їх не можна розпізнати, але їхня дія може тим чи іншим способом призвести до значних збитків ПВ. Наприклад, це може бути змінений з незрозумілої причини ключ реєстру OS Windows на робочій станції. У повідомленнях, що видаються системою IDS, немає достатньо відомостей для чіткого визначення конкретної ситуації і з'ясування того, що відбулося — нешкідлива помилка чи атака, тому такі події вимагають подальшого системного аналізу.

Не менш підозрілим може стати несподівано великий мережний трафік, що виник у внутрішній мережі. Якщо робоча станція починає запрошувати дані з інших систем, то це може бути як наслідок атаки, так і неправильної конфігурації. Підозрілі події необхідно досліджувати настільки, наскільки дозволяють це робити наявні ресурси. Дослідження таких подій зазвичай повинно бути також прописано у політиці використання IDS у вигляді процедур, які складаються з певних кроків, щоб визначити, чи є подія вдалим вторгненням або спробою проникнення, чи вона має нешкідливий характер. При цьому необхідно насамперед ідентифікувати джерело системи, з якої здійснюються підозрілі події, і записувати в журнал ведення подій про додатковий трафік між джерелом і пунктом призначення.

Алгоритм розгортання IDS

На основі вищеописаного можна скласти наступний алгоритм розгортання IDS для ПВ, що потребує надійного захисту та використовує в процесі свого функціонування АСДО і мережні засоби зв'язку (рис.):

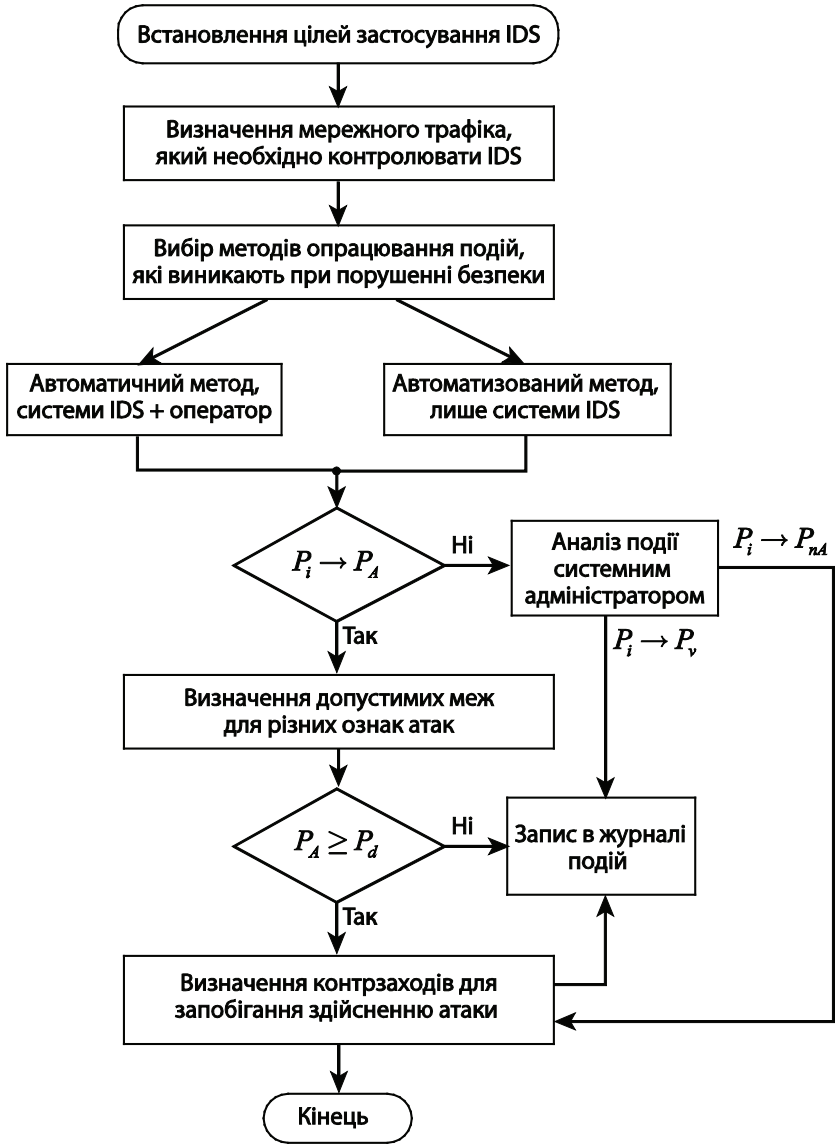

Рис. Функціональна схема аналізу і виявлення небезпечних подій у системі захисту ПВ за допомогою IDS із засобами протидії атакам:

P_i — і-та подія, що досліджується IDS; P_A — небезпечна подія, яка підлягає ознакам атак в NIDS; P_d — допустимі значення атак, які не завдають збитків організації або належать до випадкових подій; P_v — випадкова подія, яка не несе будь-якої загрози для функціонування ІС. P_{nA} — подія, яка належить до підозрілих, опису яких немає в NIDS.

1. При встановленні систем виявлення вторгнень необхідно скласти план розгортання IDS. При цьому важливим завданням є визначення відповідальних служб та осіб в організації, яких потрібно залучати для виконання цього завдання.

2. Якщо планується встановлення мережної IDS, то необхідно визначити місце встановлення датчика NIDS, виділити для цього комп'ютер і встановити на нього Linux, FreeBSD або іншу версію операційної системи сімейства Unix.

3. Необхідно завантажити останню версію програми Snort (безкоштовна IDS) з сайту http://www.snort.org/. Згідно з інструкціями із встановлення виконати інсталяцію програми Snort. Можна також встановити ряд додаткових програмних пакетів для спрощення процесу управління і конфігурації.

4. Під'єднати датчик до мережі – найкраще зробити це за допомогою концентратора, проте можна також використовувати порт розгалужувача на комутаторі.

5. Розмістивши датчик на потрібному місці, прогляньте файли журналів, щоб з'ясувати, які події в них фіксуються. Також можна використовувати програму Acid для перегляду файлів журналу через вебінтерфейс (Acid — це вебінтерфейс, використовуваний для аналізу даних програми Snort).

За наявності деякого досвіду роботи з операційною системою Unix нескладно розібратися з програмою Snort. Вказаний алгоритм допоможе виконати кроки зі встановлення датчика NIDS на будь-яку мережну ІС. Проте якщо планується використання його як дієвого датчика в організації, необхідно заручитися підтримкою мережних і системних адміністраторів організації. Таке налаштування датчика та оцінка результатів його роботи потребує деяких витрат часу та знань управління мережею.

Висновки. Розроблення та впровадження IDS в систему захисту АСДО для ПВ вимагає значних ресурсів і попередніх заходів для процесу налаштування системи, створення її політики використання, а також в процесі функціонування IDS залучення усіх служб та підрозділів видавництва до виконання правил політики безпеки. Проте за допомогою впровадження IDS зменшується вразливість системи до зовнішніх та внутрішніх атак, а при правильному її використанні збільшується надійність ПВ та АСДО, яка функціонує в ньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мєшков В. І., Віролайнен В. О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf.
2. IPS/IDS — системы обнаружения и предотвращения вторжений. URL: https://selectel.ru/blog/ips-and-ids/.
3. Технологии обнаруженя атак вторжений. URL: https://present5.com/texnologii-obnaruzheniya-atak-vtorzhenij-intrusion-detection-system/.
4. Предотвращение вторжений. URL: https://bstudy.net/812160/informatika/predotvraschenie_vtorzheniy.
5. Корченко А. Методи ідентифікації аномальних станів для систем виявлення вторгнень : монографія. Київ, ЦП «Компринт», 2019. 361 с.

REFERENCES

1. Mieshkov, V. I., & Virolainen, V. O. Analiz suchasnykh system vyiavlennia ta zapobihannia vtorhnen v informatsiino-telekomunikatsiinykh systemakh. Retrieved from https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf (in Ukrainian).
2. IPS/IDS — sistemy obnaruzhenija i predotvrashhenija vtorzhenij. Retrieved from https://selectel.ru/blog/ips-and-ids/ (in Russian).
3. Tehnologii obnaruzhenja atak vtorzhenij. Retrieved from https://present5.com/texnologii-obnaruzheniya-atak-vtorzhenij-intrusion-detection-system/ (in Russian).
4. Predotvrashhenie vtorzhenij. Retrieved from https://bstudy.net/812160/informatika/predotvraschenie_vtorzheniy (in Russian).
5. Korchenko, A. (2019). Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen. Kyiv, TsP «Komprynt» (in Ukrainian).

doi: 10.32403/1998-6912-2021-2-63-126-133

DEVELOPMENT OF AN INTRUSION DETECTION SYSTEM FOR THE PROTECTION OF PRINTING COMPANIES AND PUBLISHING HOUSES

V. I. Sabat, V. T. Dragomirova

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
v_sabat@ukr.net

The protection systems of printing companies and publishing houses are focused on detecting and counteracting external and internal threats that lead to attacks and violations of their normal functioning. Today, most protected organizations use network technologies and communications, so it is important to ensure their smooth operation in the face of external threats and attacks and to develop a security policy strategy to control and counteract possible negative factors. The article analyses modern intrusion detection systems (IDS) in the complex protection systems of printing companies and publishing houses, describes dangerous events that they can track, provides tools to counter and control possible attacks and accidental events that do not show signs of attacks, based on which the algorithm deploys IDS to counter external attacks. The significant attention is paid to the process of IDS designing, their installation and configuration in the security system of organizations. The peculiarity of such intrusion detection systems is that in addition to the general global settings adopted by the software during the installation, it is possible to identify locally dangerous events that may adversely affect the work of printing companies and publishing houses, set limits for various signs of attacks and appropriate countermeasures to prevent their implementation. It is substantiated that for the successful work of IDS, which is planned to be installed for automated document management systems (ASD), in the management of printing production (PP),

it is advisable to use IDS (HIDS), and to recognize and counter external attacks – IDS network (NIDS). Based on the research of various IDS tools, the purposes of their use and methods of dealing with dangerous events that occur when security is violated in the PP, the general principle of protection of printing companies and publishing houses with IDS is suggested in the form of a functional diagram.

Keywords: *protection systems, intrusion detection systems, attacks, printing production, automated document management systems.*

Стаття надійшла до редакції 11.08.2021.
Received 11.08.2021.