Корзаченко О. В., к.е.н.,

доцент кафедри інформаційного менеджменту

Полторак В. І.,

студент 4 курсу спеціальності «Кібербезпека», Київський

національний економічний університет імені Вадима Гетьмана

Korzachenko O. V., PhD Candidate of Economic Sciences,

Associate Professor of the Information Management Department

Poltorak V. I.,

4rd year Student at the "Cybersecurity" speciality,

Kyiv National Economic University named after Vadym Hetman

МЕТОДОЛОГІЧНІ ЗАСАДИ ЩОДО ВИБОРУ IDS/IPS ДЛЯ ОРГАНІЗАЦІЙ

IDS/IPS SELECTION METHODOLOGICAL PRINCIPLES FOR ORGANISATIONS

Анотація. Виявлення вторгнень в комп'ютерні системи — це процес моніторингу подій, які відбуваються в комп'ютерній системі або мережі, та аналізу їх на предмет можливих інцидентів, що є порушеннями або загрозами порушенню політики безпеки комп'ютера, прийнятих політик користування або стандартних практик безпеки. Профілактика вторгнень — це процес виявлення вторгнення та спроби зупинити виявлені інциденти.

Системи виявлення та запобігання вторгнень в основному зосереджені на:

виявленні можливих інцидентів;

реєстрації інформації про них;

спробі їх зупинити;

передачі їх адміністраторам безпеки.

У статті запропоновано вказівки щодо вибору продуктів IDPS для організацій. Обговорено загальні вимоги, яким повинні відповідати продукти IDPS. Розглянуто набір критеріїв, за допомогою яких можна оцінити чотири основні аспекти технологій IDPS: можливості безпеки, продуктивність, управління та вартість життєвого циклу. Наведено принципи проведення практичних оцінок продуктів та у яких випадках кожна з методик оцінювання є найдоцільнішою. Дана стаття передбачає, що організація вже визначила, який саме тип технології IDPS потрібен — мережевий, бездротовий, мережевий аналіз поведінки (NBA), або на основі хоста. Організації можуть використовувати ці критерії як основу для створення конкретного набору критеріїв, що враховує середовище, політику організації та існуючу інфраструктуру безпеки та мережі. Після збору вимог і вибору критеріїв, оцінювачі повинні знайти актуальні джерела інформації про продукти, що підлягають оцінці. Поширені джерела даних про продукцію включають тестувальні лабораторії або практики використання продукції в реальному житті, інформацію про постачальника, огляди товарів сторонніх виробників та попередній досвід IDPS від осіб в організації та довірених осіб інших організацій.

Ключові слова: інформаційна безпека організації, системи запобігання вторгнень, системи виявлення вторгнень, оцінка продуктів IPS/IDS.

Abstract. Detecting intrusions into computer systems is the process of monitoring events that occur in a computer system or network and analyzing them for possible incidents that violate or threaten to violate computer security policies, accepted user policies, or standard security practices. Intrusion prevention is the process of detecting an intrusion and trying to stop the detected incidents.

Intrusion detection and prevention systems are mainly focused on:

identification of possible incidents;
registration of information about them;
an attempt to stop them;
passing them to security administrators.

This article will cover guidelines for choosing IDPS products for organizations. First, the general requirements that IDPS products must meet will be discussed. Next, a set of criteria will be considered to estimate the four main aspects of IDPS technologies: security capabilities, performance, management and life cycle cost. At the end of the article, the principles of practical product evaluations will be outlined and in which cases each of the evaluation methods is most appropriate. This article assumes that the organization has already determined what type of IDPS technology is needed — network, wireless, network behavior analysis (NBA) or host-based.

Organizations can use these criteria as a basis for creating a specific set of criteria that takes into account the environment, organization policies, and existing security and network infrastructure. After collecting the requirements and selecting the criteria, evaluators should find relevant sources of information about the products to be evaluated. Common sources of product data include testing laboratories or real-life product use practices, vendor information, third-party product reviews, and previous IDPS experience from individuals in the organization and agents of other organizations.

Keywords: information security of organization, Intrusion Prevention Systems, Intrusion Detection Systems, IPS/IDS products evaluation.

Вступ. Перш ніж обирати продукт IDPS, організація повинна спочатку визначити загальні вимоги, яким рішення IDPS повинне відповідати. Функції, що надаються продуктами IDPS, та методології, якими вони користуються, значно різняться, тому продукт, який найкраще відповідає вимогам однієї організації, може бути непридатним для задоволення вимог іншої. Крім того, один продукт IDPS може не відповідати всім вимогам організації щодо певного типу технології IDPS (наприклад, на базі мережі), що вимагає використання кількох продуктів IDPS одного типу технологій. Подібна ситуація найчастіше зустрічається у великих середовищах і в середовищах, де технології IDPS обслуговують кілька операційних цілей.

Постановка проблеми: Для вибору продукту спочатку необхідно зрозуміти характеристики системного та мережевого середовища організації, щоб можна було обрати IDPS, яка буде сумісною з ними та матиме змогу моніторити необхідні події в системі та/або мережі. Дана інформація також необхідна для визначення кількості компонентів (наприклад, датчиків, агентів), а також місць їхнього розташування (на-

приклад, які системи будуть запускати агентів IDPS, які мережеві сегменти будуть контролюватися).

Технічні умови IT-середовища включають:

- мережеві діаграми та карти із зазначенням архітектури мережі (як логічної, так і географічної), включаючи всі з'єднання з іншими мережами, а також кількість і місцезнаходження хостів;
- операційні системи (ОС), мережеві сервіси та додатки, якими керує кожен хост, які повинні бути захищені IDPS;
- частини незахищених систем, з якими, можливо, потрібно інтегрувати IDPS, наприклад, системи управління мережею [1].

Виклад основного матеріалу: Зібравши інформацію про існуючі системні та мережеві середовища, необхідно сформулювати технічні, операційні, бізнес цілі та завдання, які потрібно досягти, використовуючи IDPS. Для цього необхідно дати відповіді на такі запитання:

- *Типи загроз, від яких IDPS має забезпечувати захист.* Необхідно максимально точно визначити можливі види загроз, які можуть виникнути як з-поза меж організації, так і зсередини організації (інсайдерські загрози). Внутрішні загрози повинні включати не лише дії зловмисників, які атакують систему зсередини, але й авторизованих користувачів, які перевищують їхні привілеї, порушуючи тим самим політику безпеки організації [2].

- *Потреба контролю використання системи та мережі з метою виявлення порушень використання.* У деяких організаціях існують правила використання системи, спрямовані на поведінку користувачів, які можуть вважатися управлінням персоналом, а не питаннями безпеки системи. Вони можуть включати обмеження доступу до веб-сайтів з сумнівним змістом (наприклад, торренти та відео-хостинги) або використання систем організації для надсилання електронної пошти чи інших повідомлень для залучення людей [3].

Далі необхідно переглянути існуючу політику безпеки та інші політики щодо IT перед тим, як обирати продукти. Політика слугує специфікацією для багатьох функцій, які необхідно забезпечити продуктами IDPS.

Приклади елементів політики, які можуть містити корисну інформацію для вибору продукту IDPS:

- *цілі політики.* Корисно сформулювати цілі, окреслені в політиці, з точки зору стандартних цілей безпеки (цілісність, конфіденційність та доступність), а також більш загальних цілей управління (конфіденційність, захист від витоку, керуваність);

- політика використання системи. Як було сказано вище, багато організацій мають політику щодо використання системи, яка є частиною політики безпеки та інших ІТ-політик;

- процеси вирішення конкретних порушень політики. Корисно мати чітке уявлення про те, що які дії буде виконувати організація у випадку, коли IDPS виявить, що політика була порушена.

Також необхідно визначити, чи організація підлягає нагляду з боку держави чи інших органів влади. Якщо так, потрібно з'ясувати, чи вимагає цей наглядовий орган певний тип IDPS або інші специфічні засоби безпеки. Приклади зовнішніх вимог:

- вимоги законодавства, що стосуються інформаційної безпеки. Наприклад, можуть бути висунуті законодавчі вимоги щодо захисту особистої інформації (наприклад, інформації про заробіток або медичної документації) в системах. Також можуть бути законодавчі вимоги щодо розслідування порушень безпеки подібної інформації;

- вимоги до аудиту щодо найкращих практик безпеки. Вимоги до аудиту можуть визначати функції, які IDPS повинен надавати або підтримувати. Деякі IDPS пропонують функції для задоволення особливих потреб певних галузей промисловості або ринкових ніш, наприклад, звіти, розроблені для задоволення законодавчих вимог щодо охорони здоров'я або фінансових установ [4];

- Вимоги до акредитації системи. Якщо системи організації підлягають акредитації, необхідно визначити та врахувати вимоги органу з акредитації щодо IDPS та інших засобів захисту безпеки.

IDPS захищають системи організації за певною ціною. Мало сенсу витрачати додаткові кошти на функції IDPS, якщо організація не має достатньої кількості систем або персоналу для їх використання. Саме через це необхідно враховувати такі два пункти:

- витрати на придбання та підтримку життєвого циклу обладнання, програмного забезпечення та інфраструктури IDPS. Загальна вартість утримання (підтримки) IDPS значно перевищує витрати на її придбання. Інші витрати можуть бути пов'язані з придбанням систем, на яких можна запускати програмні компоненти, розгортанням додаткових мереж, забезпеченням достатнього місця для зберігання даних IDPS, отриманням спеціалізованої допомоги з встановлення та налаштування системи та навчанням персоналу;

- персонал, необхідний для моніторингу та обслуговування IDPS. Деякі IDPS розроблені за умови, що персонал буде доступний для їх моніторингу та обслуговування цілодобово. Якщо ж

така опція не доступна, тоді необхідно застосовувати IDPS призначені для використання без нагляду або ж розглянути можливість аутсорсингу моніторингу та підтримки IDPS.

Оцінка можливостей безпеки кожного продукту IDPS, очевидно, є надзвичайно важливою. Якщо продукт не може забезпечити необхідні можливості, він, у кінцевому рахунку, недостатній, і слід вибрати або інший продукт, або використовувати його у поєднанні з іншими продуктами IDPS, які мають необхідні функції [5]. Далі будуть розглянуті можливості щодо забезпечення безпеки IDPS у чотирьох категоріях: збір інформації, ведення журналів, виявлення та запобігання.

Можливості збору інформації. Організації повинні визначити можливості збору інформації, необхідні для методологій виявлення та аналізу своїх функцій IDPS, та оцінити кожен розглянутий продукт IDPS щодо його здатності запропонувати ці можливості.

Можливості ведення журналу (логування). Організації повинні ретельно вивчити можливості реєстрації подій і можливості сповіщення щодо кожного прийнятого рішення. Якісні характеристики ведення журналу, такі як повнота та точність, впливають на здатність організації проводити аналіз, підтверджувати точність оповіщень та порівнювати події, що реєструються, з подіями, записаними іншими джерелами (наприклад, іншими засобами безпеки, журналами ОС).

Можливості виявлення. Організації повинні ретельно оцінювати можливості виявлення кожного оцінюваного продукту IDPS. Для більшості продуктів найважливішою функцією є саме можливості виявлення. Порівняння можливостей виявлення є складним завданням, оскільки кожен продукт зазвичай виконує виявлення певного набору подій, використовуючи різні методології. До факторів, які організації повинні враховувати в своїх оцінках, пов'язаних з IDPS, можна включити:

- які види діяльності наразі аналізуються повністю, а які частково, а також майбутні плани щодо введення додаткових можливостей аналізу;

- які типи інцидентів він може виявити, наприклад, DoS атаки, backdoors, порушення політики, сканування портів, шкідливе програмне забезпечення (наприклад, хробаки, троянські коні, руткіти, шкідливий мобільний код) та несанкціоноване використання додатків / протоколів;

- наскільки даний продукт ефективний при виявленні відомих шкідливих подій, таких як напади, сканування чи зловмисне

програмне забезпечення. Методи виявлення на основі підписів, як правило, виявляються кращими, ніж методи виявлення аномалії та методи аналізу протокольних станів при виявленні відомих подій;

- які механізми реагування пропонує продукт. Приклади включають реєстрацію подій (як локально, так до віддалених серверів журналу), відображення сповіщень консолі та надсилання пасток простого протоколу управління мережею (SNMP), електронні листи та текстові повідомлення. Критерій також включає ефективне визначення пріоритетності подій, наприклад, здійснення різних дій, коли відбувається певний тип події або коли подія стосується певної системи чи послуги;

- як адміністратори можуть налаштувати можливості виявлення, змінюючи підписи, політики та інші налаштування. Необхідно врахувати, наскільки легко можна виконати налаштування (наприклад, через графічний інтерфейс, через редагування текстових файлів).

Можливості запобігання. За можливості, зазвичай, бажано мати продукт, який має кілька способів запобігання, а не один, оскільки одні методи в певних ситуаціях ефективніші, ніж інші, а в інших — неефективні. Усі продукти IDPS повинні пропонувати значну деталізацію у параметрах конфігурації методів запобігання, таких як включення або відключення їх лише для конкретних типів інцидентів, відключення методів запобігання для хостів з білого списку та надання адміністраторам можливості визначати, який метод запобігання слід використовувати для кожного інциденту, якщо кілька методів доступні. Деякі продукти пропонують додаткову деталізацію, яка може бути корисною, наприклад, у випадку атаки на певну частину системи.

Вимоги до продуктивності. Порівнювати продуктивність продуктів IDPS складно з таких причин:

- продуктивність сильно залежить від конфігурації та налаштування кожного продукту. Хоча тестування може бути виконано з використанням стандартних налаштувань кожного продукту, деякі продукти розроблені з умовою того, що вони потребуватимуть більш широкого налаштування у майбутньому;

- продуктивність і виявлення часто розбігаються; наявність більш складних і надійних можливостей виявлення часто призводить до погіршення продуктивності, оскільки вони вимагають більшої кількості ресурсів процесора та пам'яті;

- багато компонентів IDPS на базі приладів мають багато апаратних моделей і конфігурацій, кожен з яких має свої експлу-

атаційні характеристики. Інші компоненти IDPS не базуються на приладах, тому їх обладнання, ОС та конфігурації ОС можуть сильно відрізнятися, що може вплинути на продуктивність;

- немає відкритих стандартів для тестування працездатності та загальнодоступних, всебічних, сучасних тестових наборів.

Відповідно, організація повинна зосередитись на загальних характеристиках продуктивності продуктів IDPS та уникати диференціації продуктів за незначними відмінностями у заявлених можливостях. Зазвичай розробники IDPS оцінюють свою продукцію за максимальною потужністю, наприклад, об'єм мережевого трафіку або кількість пакетів у секунду, що моніторяться, для мережевих IDPS, кількість подій, що відстежуються в секунду для IDPS на основі хоста, або потоки, що відстежуються в секунду, та кількість хостів, які можна відстежувати для систем NBA.

Вимоги до управління. Оцінка можливостей управління продуктом IDPS дуже важлива, оскільки якщо продуктом важко керувати або він не пропонує необхідної функціональності для управління, то, найімовірніше, продукт не буде використовуватися з максимальною ефективністю. Вимоги щодо можливостей управління IDPS можна розділити на три основні категорії:

- розробка та впровадження;
- експлуатація та обслуговування;
- навчання, документація та технічна підтримка.

Розробка та впровадження. Більшість аспектів розробки та впровадження IDPS є своєрідними для кожного типу продукту IDPS. На додаток до них, організації також повинні враховувати загальні критерії, пов'язані з надійністю, сумісністю, масштабованістю та безпекою.

Надійність. Організації повинні гарантувати, що обрана ними продукція IDPS буде достатньо надійною для задоволення їхніх потреб. Можливі питання щодо надійності включають такі:

- Які типи резервного обладнання доступні для IDPS (дублюючі джерела живлення, картки мережевого інтерфейсу, пристрої зберігання даних)?

- Які функції відновлення програмного забезпечення вбудовані у продукти, особливо для агентів та сенсорів?

- Чи може продукт використовувати декілька серверів управління, щоб у разі виходу з ладу одного з них, датчики або агенти автоматично перейшли на інший?

Масштабованість. Оцінюючи продукти IDPS, організації повинні враховувати не тільки їх поточні потреби, але й можливі плани на майбутнє, для того, щоб обрати продукт з достатніми

можливостями масштабування. Можливі питання щодо масштабованості включають такі:

- кількість датчиків або агентів, серверів управління, консолей та інших компонентів IDPS, які можуть бути частиною єдиної логічної реалізації;
- кількість датчиків або агентів, які може підтримувати один сервер управління;
- можливість покращення приладів (наприклад, додавання пам'яті, мережевих інтерфейсних карт або пристроїв зберігання даних);
- вартість і ресурси, необхідні для кожного варіанту масштабування.

Експлуатація та обслуговування. Цей критерій орієнтований на можливість користувача та адміністратора щодо постійного управління IDPS. Сюди входить простота виконання щоденних заходів з моніторингу, аналізу та звітності; управління та підтримка IDPS і застосування оновлень.

Організації також повинні врахувати ресурси, доступні адміністраторам і користувачам IDPS для ознайомлення з функціональністю та характеристиками IDPS та отримання допомоги при виникненні проблем. Ці ресурси — різноманітні тренінги, документація та технічна підтримка — повинні враховувати потреби адміністратора та користувача, а також різні рівні досвіду.

Організації повинні порівнювати наявне у них фінансування для продуктів IDPS з передбачуваними витратами на життєвий цикл для кожного з оцінюваних рішень. Кількісна оцінка життєвого циклу рішень IDPS може бути складною, оскільки існує багато факторів, що впливають на вартість, і тому, що зазвичай складним є отримання вигідних витрат, що надаються IDPS. Критерії, представлені нижче, зосереджуються на основних витратах самого рішення IDPS і не враховують потенційне зменшення витрат, досягнуте в результаті використання IDPS.

Початкові витрати. Початкові витрати на придбання та встановлення продукту зазвичай включають:

- обладнання, включаючи прилади, додаткове мережеве обладнання (наприклад, мережу управління, мережеві крани, балансири навантажень IDS) та хости для компонентів (наприклад, консолі);
- плата за ліцензування ПЗ, ПЗ для компонентів IDPS та допоміжного ПЗ (наприклад, інструменти звітності, системи управління базами даних);
- витрати на встановлення та початкову конфігурацію, які можуть включати зовнішню допомогу, а також внутрішню працю;

- витрати на налаштування (розробка програмістами спеціальних сценаріїв та звітів).

Витрати на обслуговування. Очікувані витрати на обслуговування рішень IDPS, як правило, включають:

- праця. Сюди входять витрати на персонал, який здійснює адміністрування та аналіз IDPS;

- плата за ліцензування програмного забезпечення, підписки або договори на обслуговування. Ці витрати, як правило, сплачуються щорічно, зазвичай забезпечують покупця програмним забезпеченням IDPS та оновленнями підписів;

- плата за технічну підтримку. Багато організацій купують договори технічної підтримки для своїх продуктів IDPS; ці договори, як правило, щорічні. Деякі організації сплачують плату за виклик технічної підтримки замість щорічного контракту;

- витрати на навчання. Періодично може знадобитися навчання для підготовки до розгортання нових версій продукту IDPS, а також для нових користувачів та адміністраторів IDPS;

- витрати на налаштування. Під час використання продукту IDPS користувачам і адміністраторам може знадобитися додаткове налаштування продукту, наприклад, програмісти розробляють додаткові спеціальні звіти або змінюють наявні звіти, а також створюють власні аналізатори та підписи;

- професійні послуги або технічна підтримка, що не підпадає під договір технічної підтримки. Приклади включають проектування реалізацій IDPS, виконання установок продукту, настройку датчиків або агентів, створення та налаштування звітів та допомогу в реагуванні на інциденти.

Висновки: Перш ніж оцінювати продукти IDPS, організації повинні спочатку визначити загальні вимоги, яким вони повинні відповідати. Функції, що надаються продуктами IDPS, та методології, якими вони користуються, значно різняться, тому продукт, який найкраще відповідає вимогам однієї організації, може бути непридатним для задоволення вимог іншої. Оцінювачі спочатку повинні зрозуміти характеристики системи, мережевого середовища організації та плани щодо майбутніх змін системи, щоб можна було обрати IDPS, який буде сумісним з ними та мати змогу контролювати події, що цікавлять організацію. Ці знання також необхідні для розробки рішення IDPS. Отримавши розуміння існуючих системних і мережевих середовищ, оцінювачі повинні сформулювати цілі та завдання, які вони хочуть досягти, використовуючи IDPS.

Оцінювачі також повинні переглянути існуючу систему безпеки та інші ІТ-політики перед вибором продуктів. Політика безпеки слугує специфікацією для багатьох функцій, які необхідно забезпечити продуктами IDPS. Крім того, оцінювачі повинні з'ясувати, чи підлягає організація нагляду іншою організацією. Якщо так, вони повинні визначити, чи вимагає цей орган нагляду за IDPS або іншими специфічними ресурсами системи. Обмеження ресурсів також повинне бути враховане оцінювачами.

Крім визначення загальних вимог, оцінювачі також повинні визначити більш спеціалізовані набори вимог:

- можливості безпеки, включаючи збір інформації, ведення журналів, виявлення та запобігання;
- продуктивність, включаючи максимальну потужність та характеристики продуктивності;
- управління, включаючи проектування та впровадження, експлуатацію та технічне обслуговування, навчання, документацію та технічну підтримку;
- витрати життєвого циклу, як початкові, так і витрати на обслуговування.

Організації можуть використовувати ці критерії як основу для створення конкретного набору критеріїв, що враховує середовище, політику організації та існуючу інфраструктуру безпеки та мережі. Після збору вимог і вибору критеріїв, оцінювачі повинні знайти актуальні джерела інформації про продукти, що підлягають оцінці. Поширені джерела даних про продукцію включають тестувальні лабораторії або практики використання продукції в реальному житті, інформацію про постачальника, огляди товарів сторонніх виробників і попередній досвід IDPS від осіб в організації та довірених осіб інших організацій.

Існують основні проблеми при проведенні поглибленого тестування IDPS із задовільними результатами, які часто роблять його нездійсненним. Більшість організацій вважають результати обмеженого тестування IDPS корисними для оцінки щоденного використання, сумісності та вимог безпеки. Організації повинні розглянути можливість використання комбінації кількох джерел даних під час оцінки продукту IDPS. Використовуючи дані інших сторін, організації повинні враховувати достовірність даних. Виконуючи практичне тестування IDPS, організації повинні зосередитись на тих методах тестування, які, найімовірніше, є цінними, і уникати методів, які мають більше шансів порушити діяльність організації.

Aimepamypa

1. A. Valdes and K. Skinner, "Adaptive Model-based Monitoring for Cyber Attack Detection," in Recent Advances in Intrusion Detection Toulouse, France, 2010, pp. 80–92.
2. Dhawal Thakker, Choosing the right intrusion detection system, 2003.
3. Intrusion Detection and Prevention System: Technologies and Challenges, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.87 (2015).
4. Intrusion Detection and Prevention Systems, Karen Scarfone, Peter Mell, Handbook of Information and Communication Security pp 177-192.
5. Intrusion Detection System — Types and Prevention B.Santos Kumar, T.Chandra Sekhara, Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhakar, B. Santos Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013, 77–82.
6. Intrusion Detection System Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan, Volume 5, Issue 2 (March — April 2017), PP. 38–44.
7. M. Rash, A. Orebaugh, G. Clark, B. Pinkard, J. Babbitt: Intrusion Prevention and Active Response: Deploying Network and Host IPS (Syngress, Rockland, Massachusetts 2005).
8. NIST SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme.
9. Open Source Host-based intrusion detection system, 2007. <http://www.ossec.net/>
10. R. Bace: Intrusion Detection (New Riders, Indianapolis 2000).
11. Rebecca Bace and Peter Mell, "NIST Special Publication on Intrusion Detection Systems," 16 August 2001.
12. Survey of Current Network Intrusion Detection Techniques, Sailesh Kumar.

References

1. A. Valdes and K. Skinner, "Adaptive Model-based Monitoring for Cyber Attack Detection," in Recent Advances in Intrusion Detection Toulouse, France, 2010, pp. 80–92.
2. Dhawal Thakker, Choosing the right intrusion detection system, 2003.
3. Intrusion Detection and Prevention System: Technologies and Challenges, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.87 (2015)
4. Intrusion Detection and Prevention Systems, Karen Scarfone, Peter Mell, Handbook of Information and Communication Security pp 177–192.
5. Intrusion Detection System — Types and Prevention B.Santos Kumar, T.Chandra Sekhara, Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhakar, B. Santos Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013, 77–82.

6. Intrusion Detection System Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan, Volume 5, Issue 2 (March — April 2017), PP. 38–44
7. M. Rash, A. Orebaugh, G. Clark, B. Pinkard, J. Babbitt: Intrusion Prevention and Active Response: Deploying Network and Host IPS (Syngress, Rockland, Massachusetts 2005).
8. NIST SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme.
9. Open Source Host-based intrusion detection system, 2007. <http://www.ossec.net/>
10. R. Bace: Intrusion Detection (New Riders, Indianapolis 2000)
11. Rebecca Bace and Peter Mell, "NIST Special Publication on Intrusion Detection Systems," 16 August 2001.
12. Survey of Current Network Intrusion Detection Techniques, Sailesh Kumar.

Статтю подано до редакції 22.09.2019 р.

УДК 004.62

DOI: 10.33111/mise.98.15

Мамонова Г.В., к. фіз.-мат. н.,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
Меднікова М.В.,
студентка 3-го курсу спеціальності «Кібербезпека», Київський
національний економічний університет імені Вадима Гетьмана

Mamonova G.V., PhD in Physics and Mathematics,
Associate Professor of the
Computer Mathematics and Information Security Department,
Mednikova M.V.,
3rd year Student of the "Cybersecurity" speciality,
Kyiv National Economic University named after Vadym Hetman

КРИПТОГРАФІЧНИЙ АНАЛІЗ АЛГОРИТМУ DES

CRYPTOGRAPHIC ANALYSIS OF THE ALGORITHM DES

Анотація. Сьогодні це дуже важлива безпека під час передачі даних. Оскільки все сьогодні передається через Інтернет, дуже ймовірно, що наші дані будуть взяті та використані. Ми провели міні-програмне забезпечення на мові C++, яке робить шифрування файлу у форматі .txt, і те, що ми будемо проводити в цій роботі. — це вимірювання часу шифрування різних розмірів файлів за допомогою алгоритму DES та AES алгоритм різних процесорів за допомогою шифрування файлів, за допомогою яких ми будемо проводити порівняння між двома алгоритмами, а також проводити порівняння між процесорами. Швидко розвиваються комп'ютерні інформаційні технології та вносять помітні зміни в наше життя. Усе частіше поняття «інформація» вико-