DOI: https://doi.org/10.17721/ISTS.2020.1.40-49
УДК 004.056.5

ВИМОГИ ДО МЕХАНІЗМІВ ЗАХИЩЕНОСТІ ОС В РАМКАХ КЛАСУ ВИКОРИСТАННЯ

Бичков Олексій [1]
orcid.org/0000-0002-9378-9535

Шестак Яніна [2]
orcid.org/0000-0002-1703-0316

Україна, м. Київ, Київський національний університет імені Тараса Шевченка,
e-mail: bos.knu@gmail.com[1], lucenko.y@ukr.net[2]

Історія статті:
Надійшла до редакції 02.01.2020
Прийнято 16.01.2020
Ключові слова:
захищеність;
операційна система;
класифікація;
вимоги;
рівень;

Key words:
security;
operating system;
classification;
requirements;
level;

Анотація: Одним з компонент сучасних інформаційних систем є комп'ютерна техніка загального призначення, на якій встановлене спеціалізоване програмне забезпечення, або з якої ведуть роботу із спеціалізованим програмним забезпеченням. Для роботи цієї комп'ютерної техніки необхідна операційна система загального призначення. Для захисту інформаційної системи необхідно захистити усі її ланки, в тому числі операційну систему. Зокрема, у випадку клієнт-серверних технологій слід приділити увагу як захисту серверної компоненти, так і захисту клієнтської компоненти. Захист операційної системи вимагає розуміння, в рамках якої інформаційної системи буде працювати ОС, які умови роботи та обмеження накладаються на захищене середовище, захист від яких загроз буде потрібен захищеному середовищу, якими механізмами можна забезпечити потрібну нам захищеність середовища та яка буде «ціна» їх застосування чи незастосування та інше. Тому безпека програмного забезпечення має спиратися на політику безпеки операційної системи, розширюючи та уточнюючи її та наскільки це є можливим. При розробці програмного забезпечення слід спиратися на механізми безпеки, які передбачені операційною системою або інформаційної системою. Це потрібно для уніфікації та спрощення системи безпеки, полегшення її обслуговування, за рахунок зменшення кількості механізмів, які створені для розв'язання однієї і тієї ж задачі. Також слід застосовувати типові та загальновідомі компоненти та стандарти, по можливості уникати компонентів з закритим вихідним кодом, або компонентів, які не підтримують, або некоректно підтримують типові стандарти.

Очевидно, що неправильний захист операційної системи може привести до провалу системи безпеки в цілому, бо робота спеціалізованого програмного забезпечення та робота з периферійними пристроями відбувається саме під контролем операційної системи.

В статті детально розглянуті пропозиції щодо вимог до механізмів захисту операційних систем. Ці вимоги орієнтовані не на універсальні потреби, а враховують різні варіанти використання комп'ютерних пристроїв.

Abstract: One of the components of modern information systems is general-purpose computer equipment on which specialized software is installed or on which specialized software is working. This computer equipment requires a general-purpose operating system. To protect the information system it is necessary to protect all its links, including the operating system. In particular, in case of client-server technologies it is necessary to pay attention both to protection of server component and to protection of a client component. Protection of an operating system demands understanding, within what limits of what information system the OS will work, what working conditions and restrictions are imposed on the protected environment, what threats to the protected environment is required, what mechanisms is it possible to provide with protection of the environment necessary to us and what "price" of their application or nonapplication and other will be. Therefore, software safety should rely on a policy of safety of an operating system, expanding and specifying it and as much as possible. It is necessary to rely on safety mechanisms which are provided by an operating system or information system at software working out. This is necessary for unification and simplification of system of safety, simplification of its service, at the expense of reduction of quantity of the mechanisms created for the decision of the same problem. It is also necessary to apply typical and well-known components and standards, to avoid components with the closed source code as much as possible, or components which do not support, or incorrectly support typical standards.

Obviously, incorrect protection of the operating system can lead to the failure of the security system as a whole, because the operation of specialized software and work with peripherals is under the control of the operating system.

In article in detail offers concerning requirements to mechanisms of protection of operating systems are considered. These requirements are focused not on universal requirements, and consider various variants of use of computer devices-

1. ВСТУП

Сучасний світ - це світ інформаційних технологій, які увібрали в себе всю суть нашого буття. Інформаційна безпека є наріжним каменем загальної безпеки держави. Як відомо, хто володіє інформацією, той володіє світом.

Є багато думок про те, з чого починати будувати захист свого інформаційного простору, робочого місця, відділу, підприємства, держави [2-7]. Всіма інформаційно-телекомунікаційними системами керують комп'ютери. Комп'ютери працюють під управлінням операційних систем (ОС). Отже, фундаментом інформаційної безпеки є забезпечення безпеки на рівні операційної системи.

Авторами в [1] розроблена класифікація варіантів використання захищених операційних систем в інформаційно-телекомунікаційних системах.

Наведемо деякі визначення з [1].

Будемо вважати операційну систему захищено., якщо вона забезпечує збереження інформації і цілісність даних власними засобами без використання допоміжного програмного забезпечення [8].

2. МЕТА СТАТТІ

Метою статті є розроблення пропозицій щодо вимог до механізмів захисту операційних систем. Дана стаття є продовженням досліджень, що були запропановані в [1].

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В [1] наведено таку класифікацію операційних систем за варіантами використання:

1. ОС для використання на робочій станції, не підключеній до мережі передачі даних.
2. ОС для використання на робочій станції, підключеній до внутрішньої мережі інтранет.
3. ОС для використання на робочій станції, підключеній до зовнішньої мережі інтернет.
4. ОС для використання на серверах, підключених у внутрішній мережі інтранет.
5. ОС для використання на серверах, підключених в зовнішній мережі інтернет.

У "Помаранчевій книзі" пропонується така класифікація рівнів захищеності операційних систем:

- високий (A), - середній (B), - умовний (C), - неприпустимий (D).

У відповідності до класифікації операційних систем за варіантами використання, сертифікат класу B1 буде позначати, що ОС використовується на робочих станціях, що не підключений до Інтернет і інтранет і має рівень захищеності «середній».

Будемо вважати рівень захищеності ОС «неприпустимим», якщо ОС не задовольняє хоча б одному пункту рівня захищеності С.

3.1. ПАРАМЕТРИ, ЗА ЯКИМИ МОЖНА ПРИСВАЮВАТИ СТУПІНЬ ЗАХИЩЕНОСТІ

Основною задачею захищеної операційної системи є запобігання несанкціонованому доступу до даних із зовнішніх (по відношенню до неї) джерел. Тому ми будемо класифікувати операційні системи, по особливостях алгоритмів управління ресурсами – локальні і мережеві ОС [9-11].

Локальні ОС управляють ресурсами окремого комп'ютера. Мережеві ОС беруть участь в управлінні ресурсами мережі.

Наведемо параметри, за якими необхідно надавати рівні захищеності.

Для класу використання 1.

Умовним рівнем захищеності буде називатися ОС, при наявності таких критеріїв:

- отримати права адміністратора безпеки можна тільки після виконання явних, що протоколюються дій;
- аутентифікаційна інформація повинна бути захищена від несанкціонованого доступу
- повинен бути реалізований механізм управління процесами в системі
- користувачі повинні пройти ідентифікацію і аутентифікацію перш ніж виконувати будь - які дії в системі
- управління системними сервісами і драйверами можливо тільки адміністратором або групою довірених осіб
- можливість локально заблокувати доступ до системи на час відсутності користувача
- процеси і об'єкти ядра не повинні мати можливість за власною ініціативою змінювати дані інших процесів або об'єктів ядра.
- повинно бути задано явне і недвозначне перерахування допустимих типів доступу (читання, запис, виконання, виконання з більш вищими привілеями) для кожного суб'єкта або групи по відношенню до об'єкта (ресурсу).
- повинен проводиться і записуватися моніторинг ключових подій в системі - контроль доступу повинен бути застосовний до кожного об'єкту і кожному суб'єкту.
- можливість змінювати правила доступу має надаватися виділеним суб'єктам (адміністраторам, довіреною групам).

Середнім рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного рівня):
- можливість відновлення системи після збою, ушкодження системних файлів, можливість створення контрольної точки відновлення
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання)
- вхід в систему під single-user повинен вимагати авторизації
- кожне реєстроване дія повинна асоціюватися з конкретним користувачем
- повинна здійснюватися очищення тимчасових системних файлів
- вся інформація про успішні і неуспішних спробах авторизації повинні записуватися в файл
- всі події в системі, які мають відношення до роботи системи

безпосередньо, до безпеки і до призначених для користувача додатків повинні фіксуватися і записуватися
- в системі повинні бути інтегрована можливість здійснювати криптографічно стійкий захист даних від несанкціонованого доступу

Високим рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного і середнього рівня):
- повинна здійснюватися очищення (обнулення, знеособлення) звільняються областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів. Очищення здійснюється довільної записом в звільнену область пам'яті, раніше

використану для зберігання даних, що захищаються (файлів).
- архівування результатів моніторингу з метою економії займаного місця
- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо вважати дані при знятті накопичувача і підключення його до іншого комп'ютера
- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо вважати дані при знятті накопичувача і підключення його до іншого комп'ютера
- наявність механізму, який би на рівні ядра забороняв виконання коду з адресного сегмента даних
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання)
- при виявленні несанкціонованої модифікації системних файлів (при завданні відповідної опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії.
- механізм встановлення паролів не повинен допускати установки слабких паролів менше 8 символів і мають осмислене значення.

Для класу використання 2.

Умовним рівнем захищеності буде називатися ОС, при наявності таких критеріїв:

- отримати права адміністратора безпеки можна тільки після виконання явних, що протоколюються дій;
- аутентифікаційних інформація повинна бути захищена від несанкціонованого доступу
- повинен бути реалізований механізм управління процесами в системі
- користувачі повинні пройти ідентифікацію і аутентифікацію перш ніж виконувати будь-які дії в системі
- управління системними сервісами і драйверами можливо тільки адміністратору або групі довірених осіб
- можливість локально заблокувати доступ до системи на час відсутності користувача
- процеси і об'єкти ядра не повинні мати можливість за власною ініціативою змінювати дані інших процесів або об'єктів ядра.
- повинно бути задано явне і недвозначне перерахування допустимих типів доступу (читання, запис, виконання, виконання з більш вищими привілеями) для кожного суб'єкта або групи по відношенню до об'єкта (Ресурсу).
- повинен проводиться і записуватися моніторинг ключових подій в системі
- контроль доступу повинен бути застосовний до кожного об'єкту і кожному суб'єкту.
- можливість змінювати правила доступу має надаватися виділеним суб'єктам (адміністраторам, довіреною групам).

Середнім рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного рівня):

- можливість відновлення системи після збою, ушкодження системних файлів, можливість створення контрольної точки відновлення
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання)
- вхід в систему під single-user повинен вимагати авторизації
- кожне реєстроване дія повинна асоціюватися з конкретним користувачем
- повинна здійснюватися очищення тимчасових системних файлів
- можливість управляти настроюванням підключення до мережі і параметрами підключення тільки адміністратору або групі довірених осіб
- вся інформація про успішні і неуспішних спробах авторизації повинна записуватися в файл
- всі події в системі, які мають відношення до роботи системи безпосередньо, до безпеки і до призначених для користувача додатків повинні фіксуватися і записуватися
- в системі повинні бути інтегрована можливість здійснювати криптографічно стійкий захист даних від несанкціонованого доступу

Високим рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного і середнього рівня):

- повинна здійснюватися очищення (обнулення, знеособлення) звільняються областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів. очищення здійснюється довільної записом в звільнену область пам'яті, раніше використану для зберігання даних, що захищаються (файлів).
- архівування результатів моніторингу з метою економії займаного місця
- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо вважати дані при знятті накопичувача і підключення його до іншого комп'ютера
- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо вважати дані при знятті накопичувача і підключення його до іншого комп'ютера
- наявність механізму, який би на рівні ядра забороняв виконання коду з адресного сегмента даних
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання)

- можливість управління правами доступу до мережі для різних користувачів
- при виявленні несанкціонованої модифікації системних файлів (при завданні відповідної опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії;
- наявність пакетного фільтра з можливістю створення правил для вхідного і вихідного мережевого трафіку з можливістю запису пакетів і переглядом мережевих з'єднань, а також правилами, що допускають вільне безперешкодне переміщення внутрішніх пакетів на локальні інтерфейси і адреса 127.0.0.1
- механізм встановлення паролів не повинен допускати установки слабких паролів менше 8 символів і мають осмислене значення.

Для класу використання 3

(ОС для використання на робочої станції, підключеної до зовнішньої мережі інтернет)

Умовним рівнем захищеності буде називатися ОС, при наявності таких критеріїв:

- отримати права адміністратора безпеки можна тільки після виконання явних, що протоколюються дій;
- аутентифікаційна інформація повинна бути захищена від несанкціонованого доступу;
- повинен бути реалізований механізм управління процесами в системі;
- користувачі повинні пройти ідентифікацію і аутентифікацію перш ніж виконувати будь-які дії в системі;
- управління системними сервісами і драйверами можливо тільки адміністратору або групі довірених осіб;
- можливість локально заблокувати доступ до системи на час відсутності користувача;
- процеси і об'єкти ядра не повинні мати можливість за власною ініціативою змінювати дані інших процесів або об'єктів ядра;
- повинно бути задано явне і недвозначне перелічення допустимих типів доступу (читання, запис, виконання, виконання з більш вищими привілеями) для кожного суб'єкта або групи по відношенню до об'єкта (ресурсу);
- повинен проводиться і записуватися моніторинг ключових подій в системі;
- контроль доступу повинен бути застосовний до кожного об'єкту і кожного суб'єкту;
- можливість змінювати правила доступу має надаватися виділеним суб'єктам (адміністраторам, довіреною групам).

Середнім рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного рівня):

- можливість відновлення системи після збою, ушкодження системних файлів;
- можливість створення контрольної точки відновлення;
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання);
- вхід в систему під single-user повинен вимагати авторизації;
- кожна реєстрована дія повинна асоціюватися з конкретним користувачем;
- повинно здійснюватися очищення тимчасових системних файлів;
- можливість управляти настроюванням підключення до мережі і параметрами підключення надається тільки адміністратору або групі довірених осіб;
- вся інформація про успішні і неуспішні спроби авторизації повинні записуватися в файл;
- всі події в системі, які мають відношення до роботи системи безпосередньо, до безпеки і до призначених для користувача додатків повинні фіксуватися і записуватися;
- в системі повинна бути інтегрована можливість здійснювати криптографічно стійкий захист даних від несанкціонованого доступу.

Високим рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного і середнього рівня):

- повинна здійснюватися очищення (обнулення, знеособлення) областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів, що звільняються. Очищення здійснюється довільним записом в звільнену область пам'яті;
- архівування результатів моніторингу з метою економії займаного місця;

- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо зчитати дані при знятті накопичувача і підключення його до іншого комп'ютера;
- наявність механізму, який би на рівні ядра забороняв виконання коду з адресного сегмента даних;
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання);
- можливість управління правами доступу до мережі для різних користувачів;
- при виявленні несанкціонованої модифікації системних файлів (при завданні відповідної опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії;
- наявність пакетного фільтру з можливістю створення правил для вхідного і вихідного мережевого трафіку з можливістю запису пакетів і переглядом мережевих з'єднань, а також правилами, що допускають вільне безперешкодне переміщення внутрішніх пакетів на локальні інтерфейси і адреси 127.0.0.1;
- підтримка стабільної роботи системного моніторингу протягом 15 хвилин атаки з повним фіксуванням дій атакуючого і паралельної відправкою на сервер резервних копій;
- система не повинна давати інформацію про своє найменування, версії і версій працюючих сервісів неавторизованих користувачів;
- механізм встановлення паролів не повинен допускати установки слабких паролів.

Для класу використання 4

Умовним рівнем захищеності буде називатися ОС, при наявності таких критеріїв:

- отримати права адміністратора безпеки можна тільки після виконання явних, що протоколюються дій;
- аутентифікаційна інформація повинна бути захищена від несанкціонованого доступу;
- повинен бути реалізований механізм управління процесами в системі;
- користувачі повинні пройти ідентифікацію і аутентифікацію перш ніж виконувати будь-які дії в системі;
- управління системними сервісами і драйверами можливо тільки адміністратору або групі довірених осіб;
- наявність пакетного фільтра з можливістю створення правил для вхідного і вихідного мережевого трафіку;
- можливість локально заблокувати доступ до системи на час відсутності користувача;
- процеси і об'єкти ядра не повинні мати можливість за власною ініціативою змінювати дані інших процесів або об'єктів ядра;
- повинно бути задано явне і недвозначне перерахування допустимих типів доступу (читання, запис, виконання, виконання з більш вищими привілеями) для кожного суб'єкта або групи по відношенню до (ресурсу);
- повинен проводиться і записуватися моніторинг ключових подій в системі;
- контроль доступу повинен бути застосовний до кожного об'єкту і кожного суб'єкту.
- можливість змінювати правила доступ має надаватися виділеним суб'єктам (адміністраторам, довіреним групам).

Середнім рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного рівня):

- можливість відновлення системи після збою, ушкодження системних файлів, можливість створення контрольної точки відновлення;
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання);
- вхід в систему під single-user повинен вимагати авторизації;
- кожне реєстроване дію має асоціюватися з конкретним користувачем;
- повинно здійснюватися очищення тимчасових системних файлів;
- можливість управляти настроюванням підключення до мережі і параметрами підключення тільки адміністратору або групі довірених осіб;
- в систему повинен бути вбудований механізм, що забезпечує передачу даних на

віддалений сервер резервного копіювання;
- механізм встановлення паролів не повинен допускати установки слабких паролів менше 8 символів і мати осмислене значення;
- вся інформація про успішні і неуспішні спроби авторизації повинні записуватися в файл;
- всі події в системі, які мають відношення до роботи системи безпосередньо, до безпеки і до призначених для користувача додатків повинні фіксуватися і записуватися;
- в системі повинні бути інтегрована можливість здійснювати криптографічно стійкий захист даних від несанкціонованого доступу;
- наявність пакетного фільтра з можливістю створення правил для вхідного і вихідного мережевого трафіку з можливістю запису пакетів і переглядом мережевих з'єднань, а також правилами, що допускають вільне безперешкодне переміщення внутрішніх пакетів на локальні інтерфейси і адресу 127.0.0.1.

Високим рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного і середнього рівня):
- повинно здійснюватися очищення (обнулення, знеособлення)
областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів, що звільняються. Очищення здійснюється довільної записом в звільнену область пам'яті;
- архівування результатів моніторингу з метою економії займаного місця;
- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо зчитати дані при знятті накопичувача і підключення його до іншого комп'ютера
- наявність механізму, який би на рівні ядра забороняв виконання коду з адресного сегмента даних;
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання);
- можливість управління правами доступу до мережі для різних користувачів;
- при виявленні несанкціонованої модифікації системних файлів (при завданні відповідної опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії;
- підтримання стабільної роботи системного моніторингу протягом 15 хвилин атаки з повним фіксуванням дій атакуючого і паралельної відправкою на сервер резервних копій;
- система не повинна давати інформацію про своє найменування, версії і версії працюючих сервісів неавторизованих користувачів.

Для класу використання 5.

Умовним рівнем захищеності буде називатися ОС, при наявності таких критеріїв:
- отримати права адміністратора безпеки можна тільки після виконання явних, що протоколюються дій;
- аутентифікаційна інформація повинна бути захищена від несанкціонованого доступу;
- повинен бути реалізований механізм управління процесами в системі;
- користувачі повинні пройти ідентифікацію і аутентифікацію перш ніж виконувати будь-які дії в системі;
- управління системними сервісами і драйверами можливо тільки адміністратору або групі довірених осіб;
- наявність пакетного фільтра з можливістю створення правил для вхідного і вихідного мережевого трафіку;
- можливість локально заблокувати доступ до системи на час відсутності користувача;
- процеси і об'єкти ядра не повинні мати можливість за власною ініціативою змінювати дані інших процесів або об'єктів ядра;
- повинно бути задано явне і недвозначне перелічення допустимих типів доступу (читання, запис, виконання, виконання з більш вищими привілеями) для кожного суб'єкта або групи по відношенню до об'єкта (ресурсу);
- повинен проводиться і записуватися моніторинг ключових подій в системі;
- контроль доступу повинен бути застосовний до кожного об'єкту і кожного суб'єкту.
- можливість змінювати правила доступу має надаватися виділеним суб'єктам (адміністраторам, довіреним групам).

Середнім рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного рівня):

- можливість відновлення системи після збою, ушкодження системних файлів, можливість створення контрольної точки відновлення;
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання)
- вхід в систему під single-user повинен вимагати авторизації;
- кожна реєстрована дія має асоціюватися з конкретним користувачем;
- механізм встановлення паролів не повинен допускати установки слабких паролів менше 8 символів і мати осмислене значення;
- повинно здійснюватися очищення тимчасових системних файлів;
- можливість управляти настроюванням підключення до мережі і параметрами підключення тільки адміністратору або групі довірених осіб;
- вся інформація про успішні і неуспішні спроби авторизації повинні записуватися в файл;
- всі події в системі, які мають відношення до роботи системи безпосередньо, до безпеки і до призначених для користувача додатків повинні фіксуватися і записуватися;
- в системі повинен бути вбудований механізм, що забезпечує передачу даних на віддалений сервер резервного копіювання;
- в системі повинна бути інтегрована можливість здійснювати криптографічно стійкий захист даних від несанкціонованого доступу;
- наявність пакетного фільтра з можливістю створення правил для вхідного і вихідного мережевого трафіку з можливістю запису пакетів і переглядом мережевих з'єднань, можливістю створення окремих правил для всіх мережевих інтерфейсів.

Високим рівнем захищеності буде називатися ОС, при наявності таких критеріїв (в сукупності з критеріями умовного і середнього рівня):

- повинно здійснюватися очищення (обнулення, знеособлення) областей оперативної пам'яті ЕОМ і зовнішніх накопичувачів, що звільняються. Очищення здійснюється довільним записом в звільнену область пам'яті;
- архівування результатів моніторингу з метою економії займаного місця;
- система повинна використовувати інтегроване шифрування файлової системи, при якому неможливо вважати дані при знятті накопичувача і підключення його до іншого комп'ютера;
- наявність механізму, який би на рівні ядра забороняв виконання коду з адресного сегмента даних;
- наявність системних таблиць з описом прав доступу для підключення пристрою для кожного користувача з встановленими дозволами використання (читання, запис, виконання);
- можливість управління правами доступу до мережі для різних користувачів;
- при виявленні несанкціонованої модифікації системних файлів (при завданні відповідної опції адміністратором) проводиться автоматичне відновлення файлів з резервної копії;
- підтримка стабільної роботи системного моніторингу протягом 15 хвилин атаки з повним фіксуванням дій атакуючого і паралельної відправкою на сервер резервних копій;
- система не повинна давати інформацію про своє найменування, версії і версії працюючих сервісів неавторизованих користувачів;
- наявність пакетного фільтра з можливістю створення правил для вхідного і вихідного мережевого трафіку з можливістю запису пакетів і переглядом мережевих з'єднань, правилами, що допускають вільне безперешкодне переміщення внутрішніх пакетів на на локальні інтерфейси і адресу 127.0.0.1.
- можливість створення правила «Що явно не дозволено - заборонено». Створення правил, для яких більш часто виконується відповідність, повинні бути написані вище за правила, для яких відповідність виконується рідше.
- останнє правило в розділі повинно блокувати і заносити в лог всі пакети для даного інтерфейсу і напрямку;

- при блокуванні небажаних пакетів на них не повинена відправлятися відповідь, тобто щоб атакуючий не знав чи досягли його пакети мети;
- можливість створення динамічних правил для відбиття атак типу «відмова в обслуговуванні».

4. ВИСНОВОК

Захист операційної системи починається з відповіді на питання:
- в рамках якої інформаційної системи працює ОС ?
- який зміст вкладається в термін «захищене середовище» ?
- які умови роботи та обмеження, які ми накладаємо на захищене середовище ?
- які задачі стоять перед захищеним середовищем?
- захист від яких загроз буде потрібен захищеному середовищу?
- чи виконано всі типові дії (industry standard security actions) по забезпеченню належного рівня захищеності середовища?
- якими механізмами можна забезпечити потрібну нам захищеність середовища та яка буде «ціна» їх застосування чи незастосування?

Відповіді на ці питання є різними у різних проектах та задачах, тому необхідно для кожного конкретного випадку розробляти документ, який містить відповіді на ці питання, які відображають спільну точку зору керівництва та технічного персоналу. Цей документ носить назву «політика безпеки». Рекомендується, щоб цей документ мав ієрархічну будову, тобто розглядав загальні поняття, поступово їх уточнюючи (переходячи від задач, які виконує інформаційна система чи її уповноважені користувачі – до загроз реалізації цих задач, і від цих загроз - до механізмів активного, реактивного, проактивного, пасивного захисту інформаційної системи).

В статті запропоновано класифікацію операційних систем за варіантами використання, критерії захищеності, вимоги до механізмів захищеності ОС в рамках класу використання Для всіх класів операційних систем розроблені також критерії, при наявності яких можна присвоїти операційній системі відповідний рівень захищеності: умовний, середній або високий**.**

7. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] О.С. Бичков. Про концепцію захищеної операційної системи реального часу // Безпека інформаційних систем і технологій. №1(1). – 2019. – с. 42-56.

[2] Multilevel Secure Operating Systems // Journal Of Information Science And Engineering 15, 91-106 (1999).

[3] Bell E., LaPaduIa L. Secure Computer Systems: A Mathematical Model // MITRE Technical Report 2547, Volume II, 1973.

[4] Л.И. Фроимсон, С.В. Кутепов, О.В. Тараканов, А.В. Шереметов. Основные принципы построения защищенной операционной системы для мобильных устройств. Спецтехника и связь. – 2013.- №1.-С.43-47.

[5] P. Colp, M. Nanavati, J. Zhu, W. Aiello, G. Coker, T. Deegan, P. Loscocco, and A. Warfield. Breaking Up is Hard to Do: Security and Functionality in a Commodity Hypervisor. In SOSP'11: 23rd Symposium on Operating Systems Principles, pages 189–202, Cascais, October 2011. 14, 26, 27.

[6] N. Ferguson and B. Schneier. A Cryptographic Evaluation of IPsec. Counterpane Internet Security, Inc, December 2003. 14, 135.

[7] T. Garfinkel and M. Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In NDSS'03: 10th Network and Distributed System Security Symposium, pages 191–206, San Diego, February 2003. 19, 70.

[8] E. I. Brycova, "Basic principles of construction of secure operating systems", Vestn. Astrakhan State Technical Univ. Ser. Management, Computer Sciences and Informatics, 2013, no. 2, 52–57.

[9] Apple. iOS Security. http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf, February 2014. 147.

[10] P. A. Karger and D. R. Safford. I/O for Virtual Machine Monitors: Security and

Performance Issues. IEEE Security & Privacy, 6(5):16–23, September 2008. 19.

[11] H. Härtig, M. Hohmuth, N. Feske, C. Helmuth, A. Lackorzynski, F. Mehnert, and M. Peter. The Nizza Secure-System Architecture. In CollaborateCom'05: 1st Conference on Collaborative Computing: Networking, Applications and Worksharing, San Jose, December 2005. 15, 139.

***Шестак Яніна Володимирівна**, кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Основними напрямами наукових досліджень є процес оцінювання захищеності від зовнішніх впливів інформаційних систем.*

***Бичков Олексій Сергійович**, доктор технічних наук, доцент,*

***Бичков Олексій Сергійович**, доктор технічних наук, доцент, завідувач кафедри Програмних систем і технологій Київського національного університету імені Тараса Шевченка.*

Область наукових інтересів: Математичні моделі систем захисту інформації, теорія гібридних автоматів, теорія можливості.