МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2021

МАТЕРІАЛИ

IX Всеукраїнської науково-технічної конференції з міжнародною участю

01–03 грудня 2021 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2021

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2021. – 219 с.

У збірнику подано матеріали IX Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

СЕКЦІЯ 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

УДК 004.056

МЕТОДИКА ЕФЕКТИВНОЇ КОМПОНОВКИ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Автори: *Гратій А.О., магістрант; Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Стрімкий розвиток інформаційних технологій, створення відкритого кіберпростору розширює можливості професійної діяльності і суттєво спрощує вирішення побутових проблем сучасної людини. Однак, цифровізація, окрім наочних переваг, має і негативні наслідки, серед яких кіберзлочинність посідає перше місце і завдає шкоди не тільки конкретним особам та організаціям, а й державі в цілому. Протидія кіберзлочинам є складною задачею, яка вирішується в сучасному кіберпросторі за допомогою інтелектуальних систем і нейронних мереж за сценарієм «бот проти бота».

Спеціалізоване програмне забезпечення (ПЗ) для захисту комп'ютерних мереж (КМ) допомагає проводити їх моніторинг, аналізувати в реальному часі отримані результати і автоматично активувати відповідні запобіжні засоби. Відповідно підвищується значимість спеціалізованого ПЗ (СПЗ) в системі захисту інформації (СЗІ). Розробці спеціалізованого ПЗ (СПЗ), вдосконаленню методів його ефективного використання присвячені роботи багатьох вітчизняних та зарубіжних науковців науковців [1-8], в тому числі науковців Національного університету кораблебудування [5, 7, 8].

На даний час існує дуже багато СПЗ для захисту КМ, але методика їх оптимальної компоновки, яка враховувала б особливості СПЗ, їх відповідність вимогам користувача і взаємну узгодженість, а також

особливості програмно-апаратного середовища функціонування, на даний час відсутня.

Метою даної роботи є розробка методики ефективної компоновки спеціалізованого програмного забезпечення для захисту комп'ютерних мереж як складової системи підтримки прийняття рішень (СППР) при формуванні комплексу засобів захисту комп'ютерних мереж.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– провести аналіз нормативно-правової бази побудови захищених КМ і визначити основні вимоги до спектру функцій комплексу засобів захисту (КЗЗ);

– провести аналіз літературних джерел вільного доступу і визначити доцільні для застосування у даній роботі критерії вибору СПЗ для захисту КМ і методи прийняття рішень;

– розробити методику ефективної компоновки СПЗ для захисту КМ на основі визначених критеріїв і методів прийняття рішень.

В результаті аналізу нормативно-правової бази побудови захищених КМ і відкритих літературних джерел [6] визначимо спектр функцій, які повинен виконувати КЗЗ:

– управління подіями інформаційної безпеки;

– статичний та динамічний аналіз файлів (sandbox, «пісочниця» і аналіз контексту файлів);

– захист веб-трафіку;

– фільтрація мережевого трафіку;

– захист мережевого периметру;

– виявлення кіберзагроз;

– реагування на кіберзагрози;

– антивірусний захист;

– запобігання внесенню несанкціонованих змін в серверні систем;

– створення груп користувачів і надання їм прав доступу до мережевих інформаційних ресурсів і пристроїв;

– аудит дій користувачів;

– контроль змін інформаційних ресурсів (файлів та каталогів);

– контроль використання мережевих пристроїв;

– інвентаризація компонентів IT-інфраструктури;

– оцінка стану технічного захисту інформації в інформаційно-телекомунікаційних системах.

В режимі реального часу КЗЗ може забезпечувати:

– обробку артефактів (виявлення артефактів; моніторинг артефактів; аналіз і реагування на артефакти; створення динамічної бібліотеки артефактів;

– обробку вразливостей (виявлення вразливостей; аналіз і реагування на виявлені вразливості; апаратно-програмне забезпечення виявлення і реагування на виявлені вразливості; інформаційна підтримка і координація реагування);

– обробку інцидентів (виявлення інцидентів; аналіз і реагування на інциденти; апаратно-програмне забезпечення виявлення і реагування на інциденти; інформаційна підтримка і координація реагування на інциденти; служби виявлення вторгнень; ведення журналів інцидентів);

– профілактичні сервіси (моніторинг процесів обробки інформації на об’єкті інформаційної діяльності для певних інформаційних технологій, певних інформаційних ресурсів і мережевих пристроїв, інформації з певним рівнем секретності; аналіз і оцінка поточного стану систем безпеки; конфігурація, реконфігурація і підтримка систем безпеки; служби запобіганню вторгненням; поширення інформації, пов'язаної з безпекою; підвищення кваліфікації персоналу);

– управління якістю систем безпеки (аналіз ризиків; оцінка програмних продуктів і апаратного забезпечення; виявлення критичних і підкритичних ситуацій; сповіщення про стан безпеки; планування і забезпечення безперервності робочого процесу; відновлення при аварійних ситуаціях; інформаційна підтримка з питань безпеки).

Вибір СПЗ для захисту КМ будемо здійснювати за наступними критеріями: середовище функціонування; виконувані функції; вартість; вимоги до апаратного забезпечення; ефективність; умови розповсюдження.

Прийняття рішення щодо вибору певної компоновки СПЗ для захисту КМ будемо здійснювати за максимальною бальною оцінкою певної компоновки серед можливих варіантів компоновки з врахуванням можливості дублювання і резервування окремих функцій.

Розроблена методика базується на інформаційній моделі рис.1 [8] і містить 11 етапів.

Етап 1. Визначення актуальних загроз інформації для об'єкта захисту. Загрози виникають в разі наявності вразливостей в системі, можуть порушувати певні властивості захищеності інформації і, відповідно, можуть бути віднесені до одного із стандартних типів (К, Ц, Д, КЦ, КД, ЦД, КЦД [8]); характеризуються ймовірністю появи загрози і ймовірністю успішної реалізації загрози. Ймовірність появи загрози визначається як добуток ймовірності атаки на галузь застосування об'єкта захисту і ймовірності атаки певного типу. Ймовірність успішної реалізації загрози залежить від наявності у КЗЗ певних засобів протидії загрозі і ефективності їх роботи.

Етап 2. Визначення нормативних вимог до послуг безпеки. Реалізується в двох варіантах – для відомого і невідомого профілю захищеності.

Етап 3. Формування переліку вимог користувача до послуг безпеки і структури системи захисту.

Етап 4. Формування ранжованого за важливістю переліку функцій КЗЗ, який має протидіяти множині актуальних загроз інформації за допомогою СПЗ, із визначеними граничними значеннями показників якості їх виконання.

Етап 5. Вибір критеріїв оцінювання якості компоновки СПЗ і обчислення за методом попарних порівнянь вектору їх пріоритетів.

Етап 6. Оцінювання окремих СПЗ на відповідність функціональним вимогам.

Етап 7. Формування варіантів компоновки СПЗ з врахуванням багатошарової структури системи захисту, дублювання і резервування функцій КЗЗ.

Етап 8. Оцінювання варіантів компоновки СПЗ за визначеними на етапі 4 критеріями якості з врахуванням підвищення ефективності КЗЗ в разі функціонального резервування на одному рівні захисту і дублювання функцій різних засобів захисту на різних рівнях.

Етап 9. Відтинання варіантів, які не відповідають визначеним граничним значенням показників якості. Формування списку варіантів компоновки СПЗ, які відповідають граничним вимогам.

Етап 10. Оцінювання компоновок СПЗ із списку варіантів, визначеними на етапі 9, за критеріями, визначеними на етапі 5.

Етап 11. Вибір оптимальної компоновки СПЗ. Візуалізація результатів.

Висновки

В даній роботі проведено на основі аналізу нормативно-правової бази побудови захищених КМ визначені основні вимоги до спектру функцій КЗЗ, критерії вибору СПЗ для захисту КМ і методи прийняття рішень, на основі яких розроблена методика ефективної компоновки СПЗ для захисту КМ

Список літератури:

1. Jankowski D., Amanowicz M. On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks //INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2016, – VOL. 62,- № 3, – PP. 247-252

2. Husák M., J. Komárková J., Bou-Harb E., Čeleda P. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security // IEEE Communications Surveys & Tutorials. – 2019. – Vol.21. – Issue 1. – PP.640–660. [URL]: https://www. researchgate. net/ publication/327449459_Survey_of_Attack_ Projection_ Prediction_and_Forecasting_in_Cyber_Security.

3. Гвоздьов Р. Ю. Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах / Р. Ю. Гвоздьов, Р. В. Олійников // Радіотехніка. – 2020. – Вип. 203. – С. 91-96.

4. Кононова В. О. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, О. В. Харкянен, С. В. Грибков // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 99-104.

5. Левченко М.П. Перспективи технології Honeypot, як засібу виявлення та дослідження атак // Матеріали VIII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2018 – С.130 – 133.

6. Проєкт I-CYBER. URL: https://icdc.gov.ua/diyalnist/projects/realizovani-u-2020-roci/proyekt-i-cyber

7. Турти М. Методика оптимізації систем захисту периметра // Матеріали 8-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2019». 9-14 вересня 2019 р. Харків – Коблеве. – Харків: ХНУРЕ, 2019. – С.254-259.

8. Турти М., Гратій А. Методика вибору спеціалізованого програмного забезпечення для захисту комп'ютерних мереж // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». – Харків: ХНУРЕ, 2020. – С.262-266.

УДК 62-519:004.931

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОГО ЗОРУ В СИСТЕМАХ «РОЗУМНІЙ БУДИНОК»

Автор: *Дідківський О.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Блінцов О.В., д.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

З розвитком і доступністю технологій в сфері мікроконтролерів і програмного забезпечення в наш час все більш набуває попит на систему «Розумний дім», яка за допомогою високотехнологічних датчиків і пристроїв робить життя власника зручним у повсякденних задачах.

Система «Розумний дім» (*розумний будинок/ smart home, digital house*) – система домашніх пристроїв, здатних виконувати дії і вирішувати певні повсякденні завдання без участі людини. Функціонально пов'язуються між собою усі електроприлади будівлі, якими можна керувати централізовано – з пульта-дисплею. Прилади можуть бути під'єднані до комп'ютерної мережі, що дозволяє керувати ними за допомогою ПК та надає віддалений доступ до них через Інтернет. Завдяки інтеграції інформаційних технологій у домашні умови, усі системи та прилади узгоджують виконання функцій між собою, порівнюючи задані програми та зовнішні показники (обстановки).[1]

Система «Розумний дім» створюється за допомогою професійного проектування та програмування компаніями, що займаються розробкою проектів smart-home. Програми, що вводяться до алгоритмів multi-room розумного дому, розраховані на певні потреби мешканців

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2021

IX Всеукраїнська науково-технічна конференція
з міжнародною участю

01–03 грудня 2021 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською, російською та англійською мовами*)

Відповідальна за випуск В. В. Трибулькевич