**Подус Олексій Сергійович**

*студент 4-го курсу, спеціальності 125*

*«Кібербезпека»*

*Національний Технічний Університет України «Київський Політехнічний Інститут імені ІГОРЯ СІКОРСЬКОГО», м.Київ, Україна*

**МЕТОДИКА ДИНАМІЧНОГО ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО МОБІЛЬНИХ ГАДЖЕТІВ**

В сучасному світі мобільні гаджети стали невід'ємною частиною нашого життя. Ми використовуємо їх для спілкування, роботи, розваг та зберігання важливої інформації. Проте, з кожним днем збільшується кількість загроз, пов'язаних з несанкціонованим доступом до наших мобільних пристроїв. У цій статті ми розглянемо методику динамічного виявлення несанкціонованого доступу до мобільних гаджетів та її застосування для захисту даних користувачів.

Метою цієї статті є розглянути методику динамічного виявлення несанкціонованого доступу до мобільних гаджетів, її важливість для захисту даних користувачів мобільних пристроїв та негативні аспекти роботи методики. Також будуть надані варіанти усунення негативних аспектів та описано переваги використання даної методики для забезпечення безпеки користувачів мобільних пристроїв.

Методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів є комплексним підходом, який дозволяє виявляти загрози безпеці мобільних пристроїв в реальному часі. Ця методика базується на використанні аналізу поведінки мобільного пристрою та детекції незвичних дій користувача.

Основна ідея методики полягає в тому, що кожен користувач має свій унікальний стиль поведінки при використанні мобільного пристрою. Наприклад, користувач може відповідати на повідомлення через певний час, натискати певні кнопки з певною частотою тощо. Методика динамічного виявлення несанкціонованого доступу використовує ці характеристики, щоб виявляти незвичайну поведінку користувача, яка може бути пов'язана з несанкціонованим доступом до мобільного пристрою.

Щоб застосувати методику динамічного виявлення несанкціонованого доступу до мобільних гаджетів, необхідно використовувати спеціальний програмний засіб, який збирає інформацію про поведінку користувачів та аналізує її за допомогою алгоритмів машинного навчання та штучного інтелекту. Це дозволяє виявляти незвичну поведінку користувача та автоматично генерувати алерти про можливу загрозу безпеці даних.

Одним з основних переваг методики динамічного виявлення несанкціонованого доступу є те, що вона дозволяє виявляти незвичайну поведінку користувача в реальному часі. Це дозволяє швидко реагувати на можливу загрозу та запобігати несанкціонованому доступу до даних[1].

Крім того, методика динамічного виявлення несанкціонованого доступу може бути застосована для різних типів мобільних пристроїв, включаючи смартфони, планшети та ноутбуки. Це дозволяє захистити важливу інформацію користувачів, незалежно від того, на якому пристрої вона зберігається.

Звичайно, методика динамічного виявлення несанкціонованого доступу не є універсальним рішенням для захисту мобільних пристроїв. Іноді вона може давати хибні сигнали про можливу загрозу безпеці даних. Тому, для максимальної ефективності захисту мобільних пристроїв, необхідно поєднувати методику динамічного виявлення несанкціонованого доступу з іншими методами захисту, такими як використання паролів, шифрування даних та програмного забезпечення для виявлення вірусів[2].

Отже, методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів є важливим інструментом для захисту даних користувачів від можливих загроз. Цей підхід дозволяє виявляти незвичну повед інку користувача та швидко реагувати на можливі загрози безпеці даних. Незважаючи на те, що методика динамічного виявлення несанкціонованого доступу не є універсальним рішенням для захисту мобільних пристроїв, вона може бути використана разом з іншими методами захисту для максимальної ефективності та захисту важливої інформації[1].

Як використовувати методику динамічного виявлення несанкціонованого доступу до мобільних гаджетів? Для початку, необхідно встановити спеціальне програмне забезпечення, яке здійснюватиме моніторинг дій користувача. Потім програмне забезпечення збиратиме дані про активність користувача, наприклад, які програми він використовує, які дії виконує, чи робить він несподівані рухи з пристроєм, та інші деталі.

Далі, на основі зібраних даних програмне забезпечення застосовує алгоритми машинного навчання та штучного інтелекту для аналізу активності користувача.

Якщо виявляється незвичайна поведінка користувача, програмне забезпечення генерує алерти про можливу загрозу безпеці даних[3].

Незважаючи на те, що методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів є досить ефективною та важливою для захисту даних користувачів, існують деякі негативні аспекти її роботи.

По-перше, методика динамічного виявлення може збирати дуже велику кількість даних про користувачів, що може порушувати їх приватність та безпеку даних. Це може стати проблемою, якщо такі дані потраплять в руки зловмисників. Також, занадто чутливі дані, такі як паролі, банківські реквізити та інші особисті дані, можуть бути відправлені до сторонніх серверів, що порушує конфіденційність цих даних.

По-друге, методика динамічного виявлення несанкціонованого доступу може бути вразливою до атак з боку хакерів та зловмисників, які можуть використовувати методики обхіду захисту для зламування системи.

Для усунення цих негативних аспектів роботи методики динамічного виявлення несанкціонованого доступу до мобільних гаджетів можна застосувати наступні підходи[1]:

1. Зменшення обсягу зібраних даних: Розробники програмного забезпечення можуть зменшити обсяг зібраних даних та обмежити збір даних, що стосуються конфіденційних або особистих даних користувачів.

2. Застосування шифрування: Розробники програмного забезпечення можуть застосовувати шифрування для захисту конфіденційної інформації та інших даних користувачів, які передаються через мережу.

3. Перевірка безпеки програмного забезпечення: Розробники програмного заб еспечення можуть проводити регулярні перевірки безпеки для виявлення та виправлення можливих вразливостей та ризиків безпеки.

4. Підвищення обізнаності користувачів: Користувачі мобільних пристроїв повинні бути більш обізнані з можливими ризиками безпеки та засобами захисту своїх даних, включаючи методики динамічного виявлення несанкціонованого доступу.

5. Використання мультифакторної аутентифікації: Використання мультифакторної аутентифікації, такої як використання паролів та кодів доступу, може забезпечити додатковий рівень захисту від несанкціонованого доступу.

6. Розвиток технологій: Розвиток нових технологій захисту, таких як біометрична аутентифікація та розпізнавання обличчя, може забезпечити більш ефективний захист даних користувачів.

Узагалі, методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів є важливим інструментом захисту особистої інформації та даних користувачів, проте розробники програмного забезпечення повинні забезпечити захист конфіденційної інформації та зменшити можливі ризики безпеки. Крім того, користувачі також повинні дотримуватися заходів безпеки та бути більш обізнані з можливими ризиками, щоб захистити свої дані. З огляду на все більшу популярність та широке використання мобільних пристроїв, таких як смартфони та планшети, ризики несанкціонованого доступу до даних користувачів також збільшуються. Тому методика динамічного виявлення несанкціонованого доступу дозволяє забезпечити захист особистої інформації та даних користувачів.

Застосування методики динамічного виявлення несанкціонованого доступу до мобільних гаджетів дозволяє виявляти можливі порушення безпеки, такі як шкідливі програми, злочинні дії, спам-розсилки та інші види атак. Це допомагає запобігти можливому втраті конфіденційної інформації та зберегти дані користувачів в безпеці[2].

Крім того, застосування методики динамічного виявлення несанкціонованого доступу до мобільних гаджетів може забезпечити захист від шкідливих програм та вірусів, які можуть негативно вплинути на роботу пристрою та викликати його несправність.

Також методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів може забезпечити захист від крадіжки особистої інформації та даних користувачів. Завдяки цьому користувачі можуть впевнено використовувати свої мобільні пристрої та не хвилюватися про можливу втрату чи пошкодження своїх даних.

Отже, використання методики динамічного виявлення несанкц іонованого доступу до мобільних гаджетів є дуже важливим для забезпечення безпеки користувачів мобільних пристроїв. Захист даних та особистої інформації є критичним аспектом в добу цифрової технології та підвищеного ризику кібератак. Користувачі мобільних пристроїв повинні мати можливість впевнено використовувати свої пристрої та не хвилюватися про можливість втрати своїх даних.

Застосування методики динамічного виявлення несанкціонованого доступу до мобільних гаджетів допомагає підвищити рівень безпеки та зменшити ризики несанкціонованого доступу до даних користувачів. Це забезпечує захист від шкідливих програм, злочинних дій, спам-розсилок та інших видів атак.

Крім того, використання методики динамічного виявлення несанкціонованого доступу допомагає забезпечити стійкість та безпеку мобільних пристроїв в цілому, що дозволяє користувачам зберігати свої дані в безпеці та уникати негативних наслідків від можливих атак.

У підсумку, методика динамічного виявлення несанкціонованого доступу до мобільних гаджетів є важливим інструментом для забезпечення безпеки та захисту особистої інформації та даних користувачів. Це дозволяє користувачам впевнено використовувати свої мобільні пристрої та не хвилюватися про можливу втрату чи пошкодження своїх даних.

**Література:**

1. Лаптєв О.А Програмно-апаратне забезпечення та захист мобільних пристроїв URL: <https://evnuir.vnu.edu.ua/bitstream/123456789/21574/1/PAZZMP.pdf> (дата звернення 09.05.2023)
2. Шаров С.В.Розробка комп’ютерної програми для захисту виконуваних файлів Windows URL: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjntKnYk-n-AhUVDRAIHW0PD_wQFnoECA8QAQ&url=http%3A%2F%2Fperspectives.pp.ua%2Findex.php%2Fnts%2Farticle%2Fdownload%2F3833%2F3854&usg=AOvVaw2hHrgqJMxpfeu9uW1YUc99> (дата звернення 09.05.2023)
3. Петренко О. Я. Використання комунікаційних мобільних пристроїв URL:<https://dspace.nuft.edu.ua/jspui/bitstream/123456789/29626/1/mobilni_pristroi.pdf> (дата звернення 09.05.2023)