синтезувати різні варіанти використання «гнучких» і «дбайливих» методологій в один проект.

Таким чином, в даний час питання, пов'язані з оптимізацією процесу розробки ПЗ, незважаючи на різноманіття «гнучких» методологій управління, залишаються актуальними.

Питання оптимізації нерозривно пов’язані з питаннями моделювання та прогнозування. Стосовно процесу розробки програмного забезпечення одним із шляхів вирішення завдання прогнозування є використання підходу, заснованого на оцінці часових витрат на окремі етапи розробки ПЗ, з урахуванням функцій залежно поточного числа активних дефектів додатка від часу, отриманих експериментальним шляхом, а також за допомогою математичного моделювання. Таке комплексне використання апріорних та апостеріорних даних має дозволити врахувати специфіку сучасних методик розробки ПЗ з можливою динамічною зміною (розширенням) рамок проекту за бажанням замовника або з інших причин.

У доповіді запропоновано комплекс математичних моделей процессу розробки программного забезпечення, що включає моделі ініціалізації та реалізації функціоналу ПО. Математична модель етапу ініціалізації процесу розробки ПО заснована на концептуальних положеннях Agile. Це дозволило виділити ряд найбільш важливих параметрів оцінки часових витрат ініціалізації і визначити їх залежності від якісних характеристик учасників проекту. Математична модель етапу реалізації функціоналу ПЗ відрізняється від відомих урахуванням показників безпечного програмування. Це дозволило підвищити точність результатів моделювання на 3%.

УДК 343.98

МИХАЙЛО ОЛЕКСАНДРОВИЧ МОЖАЄВ
кандидат технічних наук, завідувач лабораторії КТТДДВЗ Харківського НДІСЕ
ВІКТОРІЯ ЄВГЕНІВНА РОГ
старший викладач кафедри інформаційних технологій та кібербезпеки факультету №4, Харківського національного університету внутрішніх справ
МАКСИМ ВІТАЛІЙОВИЧ УСАТЕНКО
студент 3 курсу факультету – інституту підготовки кадрів для органів юстиції України, Національного юридичного університету імені Ярослава Мудрого

ДОСЛІДЖЕННЯ ФАКТІВ ЗНИЩЕННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ НА МАГНИТНИХ НОСІЯХ

За останні кілька десятиліть комп'ютерні інформаційні технології міцно увійшли в наше життя і стали складовою частиною документообігу. Спочатку відпрацьовані механізми забезпечення інформаційної безпеки не в повній мірі відповідають загрозам, актуальним для нових комп’ютерних

систем, тому сьогодні потрібно їх істотна модернізація або навіть повний перегляд.

У більшості обчислювальних систем (ОС) в якості основного енергонезалежної носія інформації використовується накопичувач на жорсткому магнітному диску (НЖМД). Тому аналіз можливих можливих несанкціонованих вторгнень в пам'ять інформаційної системи є досить актуальної метою У цей доповіді розглядається визначення фактів знищення інформації у цифрових носіях для уніфікації підходів визначення ознак знищення інформації та їх інтерпретації.

Відомо, що у більшості ОС інформація зберігається в ієрархічних базах даних – файлових системах. Будь-яка файлова система має два типи елементів: файли, що містять прикладні дані та елементи-контейнери (каталоги, папки), які можуть містити файли або інші елементи-контейнери. Файли ідентифікуються за допомогою файлових записів, розташованих у каталогах або спеціальних системних таблицях. Місцезнаходження даних файлу (тобто номера секторів НЖМД, в яких вони записані) частково, а іноді і повністю визначається вмістом його файлового запису.

При видаленні файлу стандартними засобами файлової системи, інформацію, яка містилася в файлі, також не буде перезаписано. Драйвер файлової системи просто фіксує, що відповідній файловий запис не використовується і сектора, що містили дані віддаленого файлу, вільні для запису нової інформації.

Очевидно, що до тих пір, поки дані знищених таким чином файлів не будуть перезаписані, їх можна відновити. Якість відновлення залежить від файлової системи. Так, для поширених файлових систем FAT і NTFS [9, 11] можливості по відновленню файлів відрізняються. У файлової системи родини FAT файл буде повністю відновлений тільки в тому випадку, якщо він не був фрагментований, тобто його дані розташовувалися на диску послідовно, в одному ланцюжку секторів. У файлових системах NTFS файл може бути відновлений при будь-якому рівні фрагментації.

Для того, щоб процес перезапису секторів віддалених файлів стався «природним» чином, в ході звичайної роботи файлової системи може знадобитися тривалий час – тижні або навіть місяці, в залежності від режиму експлуатації.

Якщо інформація на жорсткому диску була переписана, то отримати до неї доступ програмним способом неможливо. Однак, як було вказано вище, сліди вихідного запису можуть зберігатися по краях дискових доріжок навіть після кількох перезаписів. Існує цілий ряд методів, що дозволяють проаналізувати розподіл областей намагніченості на поверхні магнітного диска, що дає потенційну можливість отримати доступ до перезаписаної інформації.

Найбільш ефективними є різні методи візуалізації магнітних полів, що дозволяють створювати візуальне уявлення робочих поверхонь носія з дозволом, достатнім для побітового дослідження інформації. У даний час розроблено понад десяти різних методів візуалізації. На відміну від

прийнятого в техніці магнітного запису трактування поняття «сигналограма», як тимчасового розподілу амплітуд сигналу запису/зчитування, техніка візуалізації даних на магнітних носіях використовує інший підхід. Під магнітною сигналограмою розуміється просторовий розподіл амплітуд залишкової намагніченості. Магнітна сигналограма дає можливість «побачити» дані на носії. Найбільш часто для дослідження магнітних полів носіїв використовуються наступні методи:

– метод Біттера;
– магнітооптичні методи;
– магнітна силова мікроскопія.

Для візуалізації магнітних доменів Біттер застосував колоїдну суспензію магнітних частинок, кожна з яких за формою нагадує мікроскопічну голку розмірами всього декілька мікронів. Перебуваючи в підвішеному стані і практично не відчуваючи тертя, такі частинки можуть швидко переорієнтовуватися в залежності від напрямку прикладеного магнітного поля. Якщо нанести на намагнічену поверхню тонкий шар суспензії, вони концентруються уздовж ділянок зразка, де намагніченість змінює свій знак, формуючи так звані картини Біттера, які можна спостерігати за допомогою оптичного мікроскопа. Для досягнення більшого контрасту зразок іноді поміщують у невелике зовнішнє магнітне поле, спрямоване уздовж його поверхні.

Таким чином, використовував запропонований метод візуалізації магнітних доменів можна отримати інформацію про несанкціоноване вторгнення в систему пам'яті інформаційної системи, та визначити факт знищення інформації.

УДК 004.05
ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ПЕРЕЦЬ
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ
ОКСАНА ПЕТРІВНА МЕЛАЩЕНКО
Старший викладач кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ УСТАНОВЛЕННЯ МІСЦЕЗНАХОДЖЕННЯ РАДІОЕЛЕКТРОННОГО ЗАСОБУ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Одним з основних засобів отримання доказів у кримінальному процесі на стадії досудового розслідування є негласні слідчі (розшукові) дії, завдяки яким доводиться вина особи у вчиненні злочинів та розслідується левина частина тяжких та особливо тяжких злочинів [1]. Одним із таких засобів доказування - негласною слідчою (розшуковою) дією, є використання в діяльності поліції установлення місцезнаходження радіоелектронного засобу.

Як відомо, у сучасному інформаційному суспільстві мобільний телефон стає продовженням нашої особистості і нашого інтелекту. Не дивно,