каря, на діагностику, оплатити консультацію чи діагностику. У системі є можливість відстежувати аналізи та заключення лікаря, що не потребує наявність пацієнта у лікарні та очікування своєї черги.

В роботи проводиться аналіз особливостей реалізації внутрішніх алгоритмів керування основними ресурсами комп'ютера (процесорами, пам'яттю, пристроями), розглядається відмінність відповідних апаратних платформ.

ЗАХИСТ НАШОГО ЖИТТЯ В ІНТЕРНЕТІ

Воронов Д.М.
Науковий керівник – ***Булаєнко М.В., канд. техн. наук, доцент***

Комп'ютерні пристрої зберігають наші дані та є порталом до нашого життя. Що ми маємо зробити, щоб захистити наші пристрої?

Використовувати антивірусні та антишпигунські програми – зловмисне програмне забезпечення (ПЗ), таке як віруси, троянські коні, хробаки, програми-здирники та шпигунські програми, встановлюються на комп'ютерних пристроях без нашого дозволу, щоб отримати доступ до комп'ютера та даних. Віруси можуть знищити дані, уповільнити роботу комп'ютера або взяти його під контроль. Шпигунське програмне забезпечення може контролювати наші дії в Інтернеті, збирати нашу особисту інформацію або відкривати небажані спливаючі вікна з рекламою у нашому веб-браузері під час роботи в Інтернеті. Антивірусне програмне забезпечення призначене для сканування комп'ютера та вхідної електронної пошти на наявність вірусів та їх видалення. Іноді антивірусне програмне забезпечення також містить антишпигунське ПЗ.

Комп'ютерні пристрої, зокрема ПК, ноутбуки, планшети або смартфони, повинні бути захищені паролем для запобігання несанкціонованому доступу. Збережена на них інформація, а особливо важливі або конфіденційні дані, повинна бути зашифрована. На мобільних пристроях потрібно зберігати лише необхідну інформацію, з урахуванням того, що ці пристрої можуть бути вкрадені або втрачені, коли ви перебуваєте далеко від дому, таким чином злочинці можуть отримати доступ до всіх наших даних через постачальника послуг хмарного сховища, наприклад iCloud або Google Drive.

Напевно, ви маєте більше ніж один обліковий запис в Інтернеті, і для кожного з них слід використовувати унікальний пароль. Використання однакового пароля для усіх облікових записів в Інтернеті - це те саме, що й використання одного ключа для замикання усіх дверей. Таким чином, доводиться пам'ятати багато паролів. Одним із способів уникнення повторного використання паролів або вибору слабких па-

ролів є встановлення менеджера паролів. Менеджер паролів зберігає та шифрує всі наші різні та складні паролі. Він може допомогти нам автоматично входити до облікових записів в Інтернеті. Потрібно лише пам'ятати свій майстер-пароль, щоб отримати доступ до менеджера паролів і керувати всіма обліковими записами та паролями.

Це мінімум, який може зробити кожен, але це допоможе безпечно використовувати інтернет ресурси.

БЕЗПЕКА І ВСЕОСЯЖНИЙ ІНТЕРНЕТ

Смислова М.І.
Науковий керівник – ***Булаєнко М.В., канд. техн. наук, доцент***

Чим більше розміри і інтеграція рішення Всеохоплюючого Інтернету, тим більш децентралізованою стає мережа. Це забезпечує ще більше точок доступу в мережу, що має на увазі багато вразливостей. Дуже багато пристроїв, підключених один до одного по всеосяжному Інтернету, будуть обмінюватися даними з незахищених місць розташування, цей процес повинен бути захищений. Основною проблемою для фахівців із забезпечення безпеки є потенційні ризики, пов'язані з наданням доступу до мережі організації для незахищених пристроїв.

На даний час тактика випередження загроз є основною стратегією системи мережевої безпеки. Подібно до того, як лікарі намагаються запобігти новим хвороби, борючись з поточним діагнозом пацієнта, фахівці мережевої безпеки прагнуть попередити можливі загрози, зводячи до мінімуму наслідки від вдалих атак.

Підхід до забезпечення безпеки повинен бути:

- Послідовним і автоматизованим, а також досягати захищених кордонів інших організацій.
- Динамічним для поліпшеного розпізнавання загроз безпеки за допомогою попереджувального аналізу в реальному часі.
- Інтелектуальним для забезпечення повного контролю усіх підключень і елементів інфраструктури.
- Адаптивним і здатним реагувати на загрози в реальному часі.
- Комплексним, повноцінним рішенням.

Рішення повсюдної системи безпеки дозволяє уникнути ізольованих засобів захисту, які складні в управлінні і вимагають великого штату і великих технічних знань.

З урахуванням потреб надавачів послуг, яким потрібна відкрита, гнучка і програмована інфраструктура, компанія Cisco розширила можливості удосконаленого загрозоорієнтованого захисту, і тепер вони доступні для вирішень Evolved Programmable Network (EPN). Платфо-