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-

рма Cisco EPN – це надійна основа, яка ґрунтується на відкритій мережевій архітектурі та спроектована для того, щоб використовувати всі переваги технологій програмно-визначених мереж (Software Defined Networking (SDN)) і віртуалізації мережевих функцій (Network Functions Virtualization (NFV)). Вона дає змогу зменшити час окупності, витрати і технічні складнощі, зв'язані із впровадженням нових сервісів

ВРАЗЛИВОСТІ СИСТЕМИ БЕЗПЕКИ

Марченко О.А.
Науковий керівник – ***Булаєнко М.В., канд. техн. наук, доцент***

Вразливості системи безпеки - це будь-які дефекти програмного або апаратного забезпечення. Після отримання інформації про вразливість, зловмисники намагаються її використати. Експлойт - це термін, який вживають для опису програми, що написана для використання відомої вразливості. Використання експлойта для вразливості називається атакою. Мета атаки - отримати доступ до системи та розміщених на ній даних або до певного ресурсу.

Вразливості програмного забезпечення зазвичай є наслідками помилок в коді операційної системи або коді застосунку. Незважаючи на всі зусилля компаній з пошуку та виправлення вразливих місць ПЗ, регулярно виявляються нові вразливості. Microsoft, Apple та інші виробники операційних систем випускають виправлення та оновлення майже щодня. Оновлення прикладних програм також є загальноприйнятою практикою. Такі програми, як веб-браузери, мобільні застосунки та веб-сервери часто оновлюються компаніями та організаціями, які за них відповідають.

Програмне забезпечення оновлюється з метою підтримки його актуального стану та запобігання використанню вразливостей. В деяких компаніях наявні групи для тестування проникнення, які спеціалізуються на пошуку та виправленні вразливостей ПЗ до того, як вони будуть використані зловмисниками. Сторонні дослідники у галузі безпеки також спеціалізуються на виявленні вразливостей ПЗ.

Більшість вразливостей програмного забезпечення належать до однієї з наступних категорій:

1. Переповнення буфера (Buffer overflow).
2. Неперевірені вхідні дані (Non-validated input).
3. Стан гонитви (Race conditions).
4. Недоліки реалізації системи безпеки (Weaknesses in security practices).