***Попадюк Р. В.,***
***Ярощук В. О.***
*Харківський національний університет*
*Повітряних Сил імені Івана Кожедуба*

## ШЛЯХИ ЗАПОБІГАННЯ ТА НЕЙТРАЛІЗАЦІЇ КІБЕРЗАГРОЗ ТА КІБЕРБЕЗПЕКА

Національна безпека України істотно залежить від забезпечення кібербезпеки. Технічний прогрес не стає на місці, тому дана залежність від кібератаки зростатиме. Регулювання відносин у кіберпросторі потребує постійного оновлення.

Традиційно, кіберзагрозам, піддаються стратегічно важливі об'єкти економічного, інфраструктурного та військово – оборонного секторів, зокрема, підприємства енергетичної й атомної галузі, транспортування газу та нафти, обслуговування ліній електромереж, що використовують інформаційно-телекомунікаційні системи.

Наслідки терористичних посягань на об'єкти критичної інфраструктури можуть бути руйнівними в економічному й соціальному значенні.

По запобіганню та нейтралізації кіберзагроз під час воєнного стану треба виконувати ряд інструкцій:

- проводити аналіз даних про кіберінциденти;
- систематично оновлювати і сканувати ПК;
- проведення практичних семінарів з питань кіберзахисту;
- розміщення рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;
- використання ліцензійного програмного забезпечення і антивірусного забезпечення;
- сканування портів;
- перевіряти змінні носії;
- блокування шкідливих веб-ресурсів;
- користуватися шифрованими з'єднаннями;
- відстеження видалених робочих місць;
- контроль трафіку;
- зберігання електронних архівів;
- використання надійних паролів.

Сучасні інформаційні технології, локальні та глобальні комп'ютерні мережі надають можливість доступу до великої кількості інформації не лише органам державної влади, але й пересічним громадянам.

Разом з тим, щоденне збільшення обсягів даних та інформації, які обробляються, спонукає до необхідності їх захисту від протизаконних посягань, що, у свою чергу, ставить першочерговим завданням перед правоохоронними органами ефективно та професійно діяти щодо забезпечення кібербезпеки.

У даному напрямі надзвичайно важливо розуміти загрози кіберпростору, серед яких центральне місце посідає кіберзлочинність, і дослідження яких здійснюють провідні світові експерти та міжнародні організації.

В Збройних Силах України, втрата стратегічно важливої інформації, вихід з ладу обладнання – все це є ймовірними наслідками ставлення до ативірусного захисту. Є ряд інструкцій, в яких постає питання кіберзахисту та захисту інформації. Прямий обов'язок кожного військового оператора, їх дотримуватись, для запобігання шкідливої дії комп'ютерних вірусів.

Зазвичай, кібератакам піддаються важливі об'єкти критичної інфраструктури, внаслідок чого в їх роботі з'являються помилки та втрата даних.

Не тільки посадові інструкції, а і аналіз та дослідження автоматизованих комп'ютерних систем, може запобігти знищенню важливої інформації об'єкта.

Особливої уваги треба приділити неліцензованим програмам. В роботі вони не відрізняються від оригінальних, так само виконують свої завдання, але завдяки їм відбувається втрата і контроль над даними, противник має доступ до всієї важливої інформації.

Також важливо, під час копіювання електронного документа з електронного носія, обов'язково має бути виконана перевірка цілісності, достовірності та авторства даних на цьому носії.

При виникненні надзвичайних ситуацій необхідно оперативно визначити, оцінити і обробити загрозу, настання якої впливає на діяльність всієї інфракструри в цілому.

По можливості швидко забезпечити відновлення діяльності роботи системи. Здійснити резервне копіювання баз даних та інших особливо важливих даних.

Добре підготовлені працівники зможуть попередити можливість виникнення інциденту, пов'язаного з кібербезпекою, або принаймні зможуть швидше і краще визначити, що такий інцидент почався.