ОСОБЛИВОСТІ БЕЗПЕЧНОЇ РОБОТИ З ІНФОРМАЦІЄЮ В МВС ТА НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Манжай О.В.
кандидат юридичних наук, доцент
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
м. Харків, Україна

В умовах розвитку інформаційного суспільства, активного впровадження електронного урядування, переходу державних органів на електронний документообіг в Україні все гостріше постає питання якісної розбудови системи інформаційної безпеки як в державі в цілому, так і в окремих державо утворюючих суб'єктах – правоохоронних органах. Особливої актуальності це питання сьогодні набуває для реформованої Національної поліції України як суб'єкта системи кібербезпеки, визначеного Стратегією кібербезпеки України [1].

Потрібно звернути увагу, що на рівні Президента України, Кабінету Міністрів України постійно приймаються підзаконні нормативно-правові акти, спрямовані на убезпечення працівників державних органів під час роботи з інформаційними ресурсами. У цьому сенсі можна, наприклад, назвати Постанову Кабінету Міністрів України «Деякі питання використання доменних імен державними органами в українському сегменті Інтернету» від 21.10.2015 № 851.

У Міністерстві внутрішніх справ України та Національній поліції України також було прийнято низку нормативно-правових актів, які мають на меті убезпечити працівників від необачного ставлення до роботи з інформаційними ресурсами. Серед таких документів можна виділити, наприклад, Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів», у якому серед іншого працівникам Національної поліції рекомендується утриматись від застосування російських інтернет-ресурсів у

позаслужбовий час та наводиться конкретний перелік ресурсів, заборонених до використання у службовий час, за виключенням певних обставин.

Оскільки останнім часом все більша частка суспільства користується у повсякденному житті соціальними мережами, то окрему увагу хотілося б звернути на вимоги безпеки, яких повинні дотримуватись працівники Національної поліції у цій сфері.

Серед іншого потрібно пам'ятати про *заборону:*

- обміну інформацією з обмеженим доступом невстановленими телекомунікаційними каналами;

- передачі облікових даних (імені користувача та паролю), а також відомостей про них (які можуть сприяти скиданню паролю через систему його відновлення) стороннім особам;

- переходу за гіперпосиланнями в сумнівних повідомленнях;

- розміщення фотографій особистого характеру, які можуть дискредитувати особу або орган, у якому вона працює;

- використання у повідомленнях неприйнятних виразів;

- використання «простих» відповідей на секретні питання у системі відновлення паролів тощо.

Також під час роботи в мережі слід пам'ятати, що *необхідно:*

- дотримуватись вимог до складності застосовуваних паролів;

- встановити на своєму робочому місці антивірус та фаєрвол;

- використовувати окремий телефонний номер, невідомий іншим особам, під час реєстрації чутливих профілів (банківський обліковий запис тощо);

- дотримуватись правил надійного збереження особистих даних;

- бути обережним із розміщенням інформації в мережних ресурсах, що використовують для роботи сервери недружніх країн;

- періодично перевіряти Інтернет на наявність фальшивих мережних профілів, асоційованих із працівником поліції та/або його близькими родичами;

- зберігати пильність та навчити близьких правилам безпечної поведінки в мережі;

- регулярно ознайомлюватися із новинами у сфері інформаційної безпеки, які можуть вплинути на особисту безпеку працівника поліції.

Наостанок пропонуємо пошукати свої особисті дані, у тому числі паролі за допомогою пошукових систем. Результат може Вас здивувати!

Література

1. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/96/2016.

Одержано ___.___.2016