



## Рада національної безпеки і оборони України

29.06.2017

### Олександр Турчинов: Одним з механізмів поширення небезпечного комп'ютерного вірусу була система оновлення програмного забезпечення бухгалтерської звітності



Одним з механізмів поширення небезпечного комп'ютерного вірусу була система оновлення програмного забезпечення бухгалтерської звітності та документообігу. Про це сказав Секретар Ради національної безпеки і оборони України Олександр Турчинов під час засідання Національного координаційного центру кібербезпеки.

Під час засідання було проаналізовано останню найпотужнішу кібератаку на інформаційні системи підприємств та відомств України, яка розпочалась 27 червня. Окремо було обговорено ефективність запровадження протоколу швидкого реагування та взаємодії між Державною службою спеціального зв'язку та захисту інформації України, СБУ та Кіберполіції під час протидії кіберагресії.

«Поширення цього комп'ютерного вірусу та аналіз зламу інформаційних систем дає нам змогу говорити, що це складова гібридної війни, яку веде проти нас Росія», - наголосив Секретар РНБО.

За словами О.Турчинова, вже можна говорити, як поширювалась кібератака: «Насамперед, це відбувалось за рахунок системи оновлення програмного забезпечення бухгалтерської звітності та документообігу. Також був задіяний хостинг-майданчик одного з інтернет-провайдерів, до якого вже мало питань СБУ щодо співпраці з російськими спецслужбами».

«В той же час, - додав він, - активно використовувались системи «сірого інтернету», зокрема, можливості VPN, TOR тощо, які активно рекламуються на російських ресурсах, доступ до яких було заборонено рішенням РНБО».

О.Турчинов наголосив, що багато державних установ зазнали пошкоджень через те, що системно не виконували рішення РНБО та доручення Національного координаційного центру кібербезпеки. «Хочу підкреслити, що це не просто відсутність дисципліни. Ця бездіяльність - злочин, за який посадовці, які не забезпечили інформаційну безпеку своїх установ, повинні нести, в тому числі, і кримінальну відповідальність», - сказав він.

Водночас Секретар РНБО повідомив, що всі інформаційні ресурси, які підключились до захищеного контуру, а саме були під'єднані до захищеного вузла інтернет-доступу ДССЗЗІ, не зазнали пошкоджень під час атаки. «Насамперед це стосується потужних державних інформаційних реєстрів, які були надійно захищені, і кіберзлочинці не змогли пробити цей захист», - наголосив він, додавши, що це зайве свідчення необхідності в обов'язковому порядку підключення всіх державних інформаційних систем до захищеного контуру безпеки.

«Окрім того, необхідно вирішити питання підключення до державної системи кіберзахисту також і об'єктів критичної інфраструктури незалежно від їх форми власності», - зазначив Секретар РНБО.

«Об'єкти критичної інфраструктури - це безпека держави, і всі вони, незалежно від того, хто є їх власником, також мають працювати за єдиним безпековим протоколом», - сказав він, додавши, що відповідний законопроект вже напрацьовано та буде внесено найближчим часом до парламенту.

Також, за словами О. Турчинова, однією з проблем, яка призводить до подібних наслідків кіберагресії, є

«відсутність на законодавчому рівні засад кібернетичного захисту країни».

«Хочу нагадати, що протягом цього року було близько десяти спроб у Верховній Раді прийняти закони, що стосуються кіберзахисту та інформаційної безпеки держави. Але демагогія і популізм представників різних політичних сил призвели до того, що ці рішення досі не ухвалено», - додав Секретар РНБО.

Він підкреслив, що сьогодні в Україні на законодавчому рівні не працює механізм відповідальності учасників інтернет-простору за пасивну або активну співпрацю з кіберзлочинцями. «Також, - сказав він, - необхідно збільшити фінансування заходів з кібернетичної безпеки та інформаційного захисту держави, тому що негативні наслідки від кібератак значно перевищують суму видатків на ці напрямки».

За його словами, втрати, яких зазнає держава, втрати, яких зазнає наша економіка, значно більші фінансових ресурсів, «які необхідні для забезпечення елементарної інформаційної безпеки».

Окрім того, на думку Секретаря РНБО, останній кіберінцидент продемонстрував дуже низький рівень фахівців з кібербезпеки, які працюють в державних установах через низький рівень зарплатні державних службовців, що не дозволяє залучати до цієї роботи висококласних професіоналів. «Тому це питання потребує негайного вирішення», - додав він.

Олександр Турчинов поінформував присутніх, що напрацьовані Національним координаційним центром кібербезпеки конкретні заходи будуть покладені в основу рішення РНБО, яке має відбутись найближчим часом.

[Фотогалерея](#)

---

Усі права на матеріали, розміщені на цьому сайті, належать Апарату Ради національної безпеки і оборони України.