Дискусійний майданчик Кібербезпека.

Теми для обговорення:
I. Законодавче забезпечення кібербезпеки в Україні.
II. Кібербезпека і війна.
III. Галузеві CERT.
IV. Кібербезпека і права людини.

I. Законодавче забезпечення кібербезпеки в Україні.

Питання для обговорення:
Чи достатня у нас законодавче забезпечення?
Яка кібербезпека нужнаУкраіне?
Чи готова держава створювати кіберзахист разом з суспільством?
Що необхідно знати законодавцю для підготовки успішних проектів?

Відповіді:

Учасники Майданчику одностайно визнали, що на сьогодні **в Україні є недостатнім законодавче забезпечення питань кібербезпеки щодо рівноправної взаємодії держави, приватного сектору та громадянського суспільства**, ігноруються європейські практики демократичного контролю за діями і повноваженнями влади, насаджуються практики держави агресора і руйнується ІТ сектор економки, а також запропонували поглибити та конкретизувати законотворчу роботу з цих питань.

На понятійному та законодавчому рівні доцільно розмежувати проблеми інформаційної та кібербезпеки.

При розробці законодавчих актів застосовувати різні підходи до захисту та адміністрування державних та приватних інформаційних ресурсів з урахуванням світового досвіду.

Всі законотворчі ініціативи що передбачають роботу з інформаційними ресурсами (системами), мають проходити комплексну громадську експертизу на предмет можливості їх імплементації на апаратному, програмному і комунікаційному рівнях.

До експертизи мають бути залучені експерти з академічної спільноти, фахівці в сфері ІТ та громадських організацій.

II. Кібербезпека та війна.

Питання для обговорення:

- Методи боротьби з шахрайством в сфері електронних платежів і карткових розрахунків, банківській сфері?
- Як бути з невеликими, локальними хакерськими атаками, які вже давно регулярно проводяться різними державами?
- Чи доцільно застосування «фізичних» військових заходів у відповідь на кібернапад?
- Чи виправдано в цьому випадку введення економічних санкцій? Або слід обмежитися кібервідповіддю?

Відповіді:

В умовах не визначення воєнного стану не можливо реалізувати повноцінну належну державну політику щодо кібербезпеки (кіберзахисту).

Держава повинна організувати ефективну взаємодію на усіх рівнях (між силовим блоком, владою, бізнесом та громадянським суспільством) та визначити повноваження та обов'язки, в межах яких неможливо перекладати виконання завдань з одної структуру на іншу.

Створити умови для ефективної співпраці та взаємодії з неформальними громадськими об'єднаннями, які на волонтерських засадах виконують завдання захисту національного кіберпростору та протидіють кібератакам зовнішнього агресора.

При проведенні розслідувань кібератак (кіберінцидентів) доводити до кінця розслідування та інформувати громадськість про їх ефективність.

III. Галузеві CERTи.

<u>Питання для обговорення:</u>

Що змінилося в Україні з 2014 року в ставленні до командам реагування?

Основні проблеми та шляхи їх вирішення?

Чи розуміє держава про рівень відповідальності, гальмуючи розвиток систем захисту?

Чи готова влада розділити ризики при створенні приватних і державних CERT?

Чи готова влада віддати сферу діяльності CERT на саморегулювання?

Відповіді:

Учасники майданчику визнали, що **державна підтримка команд швидкого реагування на кіберінциденти (CERT): фінансового, кадрового, програмно-технічного, методичного тощо – фактично відсутня**.

Водночас, приватний сектор демонструє високу відповідальність та зацікавленість в розвитку приватних CERTів, зокрема створений та отримав міжнародну сертифікацію перший приватний CERT.

IV. Кібербезпека та права людини.

<u>Питання для обговорення:</u>

Як буде виглядати кібербезпека, що започаткована на правовому підході?

Що повинна зробити держава для запровадження цивілізованої практики?

Відповіді:

Учасники не знайшли відповіді на питання чи готова влада та суспільство виконувати закони та Конституцію України, разом з тим держава демонструє прихильність до запровадження антидемократичних методів контролю за комерційними та приватними секторами Інтернет.

Європейські практики демократичного контролю за діями і повноваженнями влади блокуються та насаджуються практики держави агресора.

Резюме:

Державна політика щодо кібербезпеки знаходиться на низькому рівні в цілому, що провокує зловмисників та агресора на провадження активних дій на шкоду національним інтересам України в кіберпросторі.