Кшиштоф Бжозовскі (Польща):

Я зроблю презентацію про плани захисту критичної інфраструктури. Два дні тому я мав цікаву дискусію в Польщі щодо розуміння терміну «критична інфраструктура». У нас в країні є велика кількість зацікавлених сторін, і їхні думки з цього приводу можуть істотно відрізнятися. Тому саме досягнення розуміння цієї проблеми є досить складним процесом. Але під час дискусії було запропонована влучна аналогія з тілом людини. Якщо ми порівняємо критичну інфраструктуру з тілом людини, і поставимо таке питання: чи зможу я прожити без моєї руки, ока, ноги? Відповідь: так, хоча це не буде комфортний спосіб життя, але я, все ж таки, буду жити. Чи зможу я прожити без мозку або без серця? Однозначно, ні. І це є відповіддю на питання про те, що таке критична інфраструктура. Ми повинні захистити життєво важливі органи. Безумовно, я би хотів мати всі елементи свого тіла, але без критичних органів я не зможу жити, і вони мають бути захищені на найвищому рівні. Аналогічна ситуація і з критичною інфраструктурою (КІ).

У Польщі ми почали з виявлення важливих елементів КІ та кращого розуміння завдання щодо їх захисту. Наша робота розпочалася під егідою Міністерства внутрішніх справ, але потім державним секретарем було утворено Центр безпеки. Тобто, ми розпочали свою роботу в рамках міністерства, але потім усвідомили необхідність створення окремої структури.

Польській досвід показує, що в цій сфері, у цілому, є три головні проблеми: удосконалення законодавчої бази, визначення якісних критеріїв для віднесення об’єктів до КІ, підтримка якості партнерства шляхом обміну важливою інформацією між зацікавленими сторонами.

У Польщі ми маємо систему захисту критичної інфраструктури (ЗКІ), що включає багато сторін, до основних з яких належать Урядовий центр з безпеки, оператори об'єктів КІ, міністерства відповідальні за ЗКІ. ЗКІ є обов'язком оператора. При цьому оператори об’єктів КІ зобов’язані готувати плани захисту об’єктів, а також призначати контактних осіб, відповідальних за підтримку відносин з державними органами.

З отриманням інформації, що об’єкт включено до списку КІ оператор повинен упродовж 9 місяців підготувати План захисту критичної інфраструктури об’єкту. До цього плану включаються загальні дані про об’єкти, серед яких назва та місце розташування об’єкту, його реєстраційний номер, номера у Комерційному регістрі, Національному судовому реєстрі, відповідальна особа, характеристика об'єкта КІ і основні технічні параметри. Наступним елементом плану є аналіз ризиків для об'єкту КІ з урахуванням виявлених загроз та впливів, визначення рівня ризику для об’єкту та винесення рішення щодо його прийнятності.

Вкрай важливим моментом є співпраця з владою на всіх рівнях (урядовий, місцевий), а також з Агентством внутрішньої безпеки у випадку реагування на терористичну загрозу. У Польщі є Національний план управління в кризових ситуаціях, що включає такі загрози як повінь, епідемії, хімічне забруднення, порушення у подачі електроенергії, порушення у

подачі рідкого палива, порушення подачі газу, сильні морози / сильний снігопад, урагани, лісові пожежі, епізоотія тощо.

План ЗКІ повинен мати повний опис захисних заходів у 6 напрямах, що включають фізичну безпеку, технічну безпеку, безпеку персоналу, інформаційну та кібербезпеку, правовий захист, плани відновлення. Він має передбачати варіанти дій у разі надзвичайної ситуації, для забезпечення безперервного управління, відновлення частини або всього об'єкта КІ. План має включати положення про співробітництво з місцевими органами управління кризовими ситуаціями та національними адміністраціями.

План ЗКІ має бути погоджений протягом 14 днів, та узгоджений у відповідній частині з територіальними органами поліції, пожежної служби, управлінням водопостачання, інспектором будівельного контролю, ветеринарним інспектором, санітарним лікарем, директором Морського бюро, а також упродовж 45 днів — з міністерством, відповідальним за даний об’єкт КІ.

Начальник державного Центру з безпеки має 90 днів для аналізу та затвердження Плану захисту критичної інфраструктури. Якщо плану бракує необхідної інформації або рівень ЗКІ не є достатнім, він повертається до оператора для внесення змін. Плани захисту критичної інфраструктури мають оновлюватися кожні два роки. План захисту КІ містить конфіденційну інформацію, що повинна бути захищена.