

району (або районів) Харкова або Харківській області; в) проміжку часу (за останній день, тиждень, місяць та ін.);

- відображення на географічній карті місцевості всіх доступних відеокамер з можливістю перегляду в on-line режимі в реальному часі ситуації в спостережуваному даної відеокамерою (або декількома відеокамерами одночасно) ділянці місцевості;

Ця можливість цікава тим, що дозволяє: а) спостерігати розвиток ситуації під час масових заходів у реальному часі; б) зацікавленим особам (наприклад, родичам) спостерігати ситуацію в реальному часі в місці знаходження спостережуваних осіб (наприклад, дітей або інших близьких родичів);

- відображення на географічній карті місцевості розташування всіх дільничних інспекторів з можливістю перегляду їх контактної інформації та зон їх обслуговування (списку будинків);

- можливість перегляду списку всіх злочинців, які перебувають в даний момент в розшуку, а також осіб, зниклих без вісті;

До функцій реалізації зворотного зв'язку відносяться:

- можливість будь-якому громадянину відправити повідомлення про правопорушення, про яке-небудь небезпечному предмет і ін. по Інтернету з прикріпленням файлу з фотозображенням або відео описуваної події або предмета;

- можливість оцінки ефективності діяльності поліції в режимі інтерактивного опитування (в перспективі).

Кібербезпека як складова частина системи забезпечення національної безпеки України

Байдуж Ю.І.

слухачка магістратури юридичного факультету ДДУВС

Косиченко О.О.

науковий керівник, к.т.н., доцент кафедри економічної та інформаційної безпеки ДДУВС

В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя, керівництво провідних країн приділяє посилену увагу створенню та удосконаленню ефективних систем захисту власного інформаційного простору від зовнішніх та внутрішніх загроз кібернетичного характеру. Так, у процесі розвитку високих технологій

виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережево-комп'ютерної складової. Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Все більш вирішальним чинником досягнення успіху у світовому протиборстві стає інформаційно-технічна дезорганізація систем державного і воєнного управління та інформаційно-психологічна деморалізація населення країн, насамперед складу їх збройних сил.

Під кібербезпекою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі. При цьому важливо визначити, що собою являє кіберпростір, адже кібербезпека є його складовою частиною. Так, кіберпростір - це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Діяльність із формування системи забезпечення національної безпеки України була невід'ємною складовою і чинником державотворчих процесів із початку виникнення незалежної України. Вже в Декларації про державний суверенітет України (16 липня 1990 р.) питання безпеки розглядалися в розділах «Зовнішня і внутрішня безпека», «Міжнародні відносини», «Екологічна безпека». Питання внутрішньої та зовнішньої безпеки аналізуються через призму права України на власні збройні сили, власні внутрішні війська та органи державної безпеки.

Система національної безпеки будь-якої країни базується на концептуальних нормативно-правових документах, у яких викладаються офіційні погляди на роль і місце держави у світі, її національні цінності, інтереси й цілі, способи й засоби запобігання зовнішнім і внутрішнім небезпекам і загрозам. Система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом в кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки повинен супроводжуватись відповідними корективами у

процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором.

Кіберпростір характеризується відсутністю кордонів, динамікою і відносною анонімністю. Забезпечення безпеки в кіберпросторі повинно бути організовано на конституційному рівні.

Останнім часом воєнно-політичне керівництво України здійснює комплекс заходів щодо підвищення ефективності та поліпшення координації діяльності своїх силових структур у сфері кібернетичної безпеки. Війна в кіберпросторі спричиняє нові кіберзагрози. Конкретні загрози в кібербезпековому просторі носять розширений, динамічний і глобальний характер, що ускладнює їх виявлення та реалізацію заходів протидії. Глобальність кіберпростору збільшує його потенційні ризики.

Таким чином, в Україні існують наступні загрози інформаційній безпеці: ведення інформаційної війни проти нашої держави; відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Причинами виникнення постійних інформаційних загроз, безумовно є використання злочинцями людського фактору та вразливість технічних засобів у різних сферах приватного та державного секторів, які обумовлюють сферу національних інтересів.

З метою протидії цим загрозам необхідним є створення та ефективне функціонування національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Отже, забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Очевидною є необхідність створення Національної системи кібербезпеки. Одним із ключових питань організації ефективної роботи якої залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, здійснення координації такої діяльності та забезпечення превентивної та попереджувальної діяльності у кіберпросторі.