безпосередньо впливають на процес прийняття і реалізації уповноваженими суб'єктами обґрунтованих управлінських рішень у сфері забезпечення інформаційної безпеки України.

Пізнавальна діяльність в контррозвідці становить не лише систему накопичення, систематизації, аналізу і оцінки інформації для здійснення довгострокових прогнозів і планів протидії розвідувально-підривній діяльності, а і напрацювання на цій основі рекомендацій і пропозицій підвищення ефективності контррозвідувальної діяльності. Окрім цього, результати контррозвідувального пізнання утворюють можливість передбачення розвідувально-підривної діяльності не лише для її попередження і припинення, а і для перехоплення ініціативи, підпорядкування дій спецслужб іноземних держав, організацій та окремих осіб цілям і завданням контррозвідки.

Історія національних спецслужб свідчить про те, що на всіх етапах існування контррозвідувальної діяльності, пізнання як фундаментальна філософська категорія посідало важливе місце у системі забезпечення державної безпеки. Будучи складовою частиною контррозвідувальної діяльності воно відображувало процес формування знань про об'єкти контррозвідки для виявлення, попередження і припинення діяльності іноземних розвідок на шкоду інтересам України.

В сучасних умовах ведення проти України інформаційно-психологічної війни, зважаючи на уразливість державних інформаційних ресурсів до кібератак, недосконалість системи охорони державної таємниці та інші негативні фактори і чинники, пізнавальна діяльність контррозвідників як складний, безперервний, діалектичний процес формування істинних знань відіграє важливу роль у забезпеченні інформаційної безпеки. Результати контррозвідувального пізнання стають запорукою прийняття та реалізації правильних управлінських рішень щодо протидії загрозам безпеці держави в інформаційній сфері та недопущення використання інформаційного простору України в деструктивних цілях.

Література

1. Указ Президента України від 25.02.2017 р. №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

Вацлавик О. М.
Львівський державний університет безпеки життєдіяльності

ПІДВИЩЕННЯ ОБІЗНАНОСТІ ПРО КІБЕРНЕТИЧНУ БЕЗПЕКУ

Напади на критичну інформаційну інфраструктуру стали частішими, та складнішими, оскільки злочинці впродовж останніх років були більш

професійними. Можливості своєчасного реагування та арешти злочинців є дуже обмеженими та вимогливими. Тенденція розвитку ІС для промислового використання, пов'язаного з Інтернетом, призводить до нових вразливостей цих систем. Досвід використання вірусом Stuxnet показує, що важливі промислові об'єкти не захищені від кібернетичних нападів. Кібернетична безпека залишається ключовою для підтримки функціонуючого держави в майбутньому.

Інвестиції в кібернетичну безпеку - це інвестиції в наше майбутнє та наше економічне зростання. Рівень кібернетичної безпеки складається з усіх заходів, як національних, так і міжнародних, прийнятих для захисту доступності ІКТ та цілісності, автентичності та конфіденційності даних в кіберпросторі. Кібернетична безпека повинна базуватися на складному підході, який вимагає обміну інформацією та координації дій. Під час створення системи кібернетичної безпеки необхідно забезпечити співробітництво між військовими та цивільними, громадськими та приватними, міжнародними та національними сферами. Тільки такий підхід забезпечує надійну роботу інфраструктури ІКТ у критичних областях, швидку та ефективну реакцію на кібернетичні напади та правовий захист у цифровому світі. Питання кібернетичної безпеки не може розглядатися як ізольована проблема окремих частин нашого суспільства. Це не тільки міжнародна, міжвідомча громадська або приватна сфера, а проблема всього суспільства. Тому забезпечення кібернетичної безпеки заслуговує на найвищий пріоритет.

Захист критично важливої інформаційної інфраструктури є одним з головних пріоритетів кібернетичної безпеки. Ця інфраструктура являє собою основну частину практично всіх частин критично важливої інфраструктури та стає дедалі важливішою. Як приватна, так і державна сфера мають створювати умови для тіснішої співпраці, що базується на обміні інформацією. Це буде належним чином оцінено там, де заходи безпеки будуть в повній мірі виконані, і де будуть надані додаткові повноваження у разі конкретних нападів та загроз.

Встановлення кібернетичної безпеки не може покладатися лише на технічні засоби. Належна увага повинна приділятися також кінцевим користувачам та адміністраторам систем ІКТ, працівникам з розробки, підрядникам державних контрактів, аудиторам та менеджерам. Недостатня інформація про безпеку систем ІКТ створює серйозні ризики. Відсутність кваліфікованого та обізнаного персоналу та подальша освіта підвищують вразливість та збитки.

Поінформованість громадян про кібернетичну безпеку повинна зростати через поширення відповідної інформації у співпраці з засобами масової інформації. Кібернетична безпека є частиною підготовки державних службовців, і її підтримають також у приватній сфері. Мета - досягти достатнього рівня знань для кожної позиції в галузі кібернетичної безпеки.

Співпраця, спрямована на створення навчальних програм, спрямованих на кібернетичну безпеку, розпочинається з академічної та приватної сфер. Необхідність кваліфікації в кібернетичній безпеці, можливості навчання та іншої освіти оцінюються на регулярній основі. Питання кібернетичної безпеки буде реалізовано на всіх рівнях освіти.

Література

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/96/2016

2. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/boz_2012_2_36.

3. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf.

УДК 351

Величко М. В.
кандидат біологічних наук,
старший науковий співробітник,
професор спеціальної кафедри
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА БІОМЕДИЧНИХ ДОСЛІДЖЕНЬ: МІЖНАРОДНА ПОЛІТИКА

Наприкінці XX сторіччя вченим вдалося розробити ряд нових методів які дали можливість людині уже на рівні геному маніпулювати спадковістю живих організмів. Це відкрило додаткові можливості для біотехнології. Появились нові перспективні науки як генна інженерія, біоінформатика, синтетична біологія тощо. Одночасно людство зрозуміло, що наряду із новими преференціями у біотехнології воно отримало і нові загрози біологічного характеру. В числі перших серед міжнародних інституцій на новітні біозагрози відреагувала Всесвітня організація охорони здоров'я (ВООЗ). Стратегія біологічної безпеки та захисту ВООЗ щодо наукових досліджень в системі охорони здоров'я людини визначає на міжнародному рівні загальні рамки вимог, тобто доцільність та безпечність як для людини так і довкілля, яка схвалена і прийнята на 63-й сесії Всесвітньої асамблеї охорони здоров'я в резолюції WHA63.21 від 2010р.[1].Зазначене в першу чергу було пов'язане з тим фактом, що у XXI сторіччі, дослідни-