контролю веде облік і перевіряє, як підконтрольний об'єкт виконує покладені на нього завдання та функції.

Заходи контролю за охороною державної таємниці здійснюються СБУ під час проведення спеціальних експертиз при видачі спеціального дозволу на діяльність, пов'язану з державною таємницею.

За порушення режиму секретності передбачена дисциплінарна, адміністративна чи кримінальна відповідальність.

Список використаних джерел

1. Про державну таємницю. Закон України № 3855-XII від 21.01.94. URL : https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення 15.04.2022)

Корж О.В.
ст. гр.ПДЕБ-12
Хом'юк С.
ст. гр.ПДЕБм-11
Науковий керівник: к. е. н., доцент,
доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет
Будник Л. А.

ЗАГРОЗИ КРИМІНОЛОГІЧНІЙ БЕЗПЕЦІ У КІБЕРПРОСТОРІ

В умовах стрімкого розвитку інформаційних технологій та їх широкого впровадження в усі сфери суспільного життя важливого значення набуває забезпечення кримінологічної безпеки людини, суспільства, держави в такому важливому сегменті інформаційного простору як кіберпростір. Під кібернетичним простором розуміють штучне електронне середовище існування інформаційних об'єктів у цифровій формі, яке утворене в результаті функціонування кібернетичних

комп’ютерних систем управління та оброблення інформації й забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних обчислювальних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу взаємодіяти щодо спільного використання обчислювальних та інформаційних ресурсів (надання інформаційних послуг, ведення електронної комерції тощо) [1].

Забезпечення кримінологічної безпеки у кіберпросторі не знайшло належного дослідження в роботах науковців та практиків, відповідно не достатньо розроблений понятійний апарат. Аналіз наукових джерел дозволяє розглядати кримінологічну безпеку як один із видів юридичної безпеки, який заснований на новітніх підходах до кримінології, до розгляду проблемних питань безпечного існування та розвитку людини, суспільства, держави, а також усунення неузгодженості цілей правоохоронної діяльності з інтересами окремої особи, суспільства, держави. Водночас, необхідність об’єктивного оцінювання результатів діяльності правоохоронних органів вимагає розробки на основі положень кримінологічної безпеки відповідних критеріїв оцінки стану захищеності життєво важливих прав та інтересів людини, суспільства, держави від кримінальних загроз.

Кримінологічну безпеку у кіберпросторі доцільно розглядати як об’єктивно-суб’єктивний стан боротьби з організованою злочинністю і корупцією, захищеності прав та інтересів громадян та держави як у реальному, так і у віртуальному середовищі від зовнішніх та внутрішніх кримінальних посягань і загроз, які пов’язані з використанням кібернетичних комп’ютерних систем [2]. При цьому, враховуючи особливості функціонування кіберпростору, кримінологічну безпеку в ньому можна розглядати як кримінологічну кібербезпеку, а зазначені

кримінальні посягання і загрози – як кримінальні кіберпосягання та кіберзагрози, стан захищеності – як стан кіберзахищеності.

В основі поняття кібербезпеки лежить використання кібернетичних систем: з одного боку - для забезпечення захисту певних об'єктів кіберпростору; з іншого – для готування вчинення кіберпосягання, реалізації кіберзагроз. Під кримінальними кіберпосяганнями слід розуміти кіберзлочини, перелік яких наведено у Конвенції Ради Європи про кіберзлочинність і Додатковому протоколі до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [3]. Хоча у даних актах не дано поняття кіберзлочину, аналіз їх положень дозволяє визначити кіберзлочини як злочини, які пов'язані з несанкціонованим втручанням у роботу кібернетичних комп'ютерних систем чи протиправним використанням таких систем.

Кіберзагроза кримінального характеру є об'єктивно існуючою можливістю учинення кіберзлочинів, у результаті чого можуть наступити несприятливі наслідки як у реальному, так і віртуальному середовищі.

Об'єктом кримінологічної безпеки як у реальному, так і віртуальному середовищі є людина, суспільство, держава. Їх кримінологічна безпека у кіберпросторі забезпечується шляхом захисту від кримінальних посягань і загроз їх інтересам у кіберпросторі, до яких слід віднести: для людини – конституційні права і свободи щодо доступу до інформації та її використання; для суспільства - його духовні, морально-етичні, культурні, історичні, інтелектуальні цінності, інформаційні ресурси; для держави – її конституційний лад, суверенітет, недоторканність інформаційного простору. При цьому, слід враховувати, що користувачі проявляються у кіберпросторі як певні інформаційні об'єкти. Тому, забезпечення кримінологічної кібербезпеки можна розглядати і як забезпечення безпечного існування відповідних інформаційних об'єктів кіберпростору,

їх діяльності щодо використання його ресурсів та взаємодії з іншими об’єктами у віртуальному середовищі.

Забезпечення кримінологічного кіберзахисту - це діяльність у кіберпросторі з охорони певних його об’єктів від злочинних посягань і створення перешкод у реалізації кіберзагроз кримінального характеру. Доцільно виділити такі рівні кримінальної кібербезпеки:

- соціально прийнятний рівень - коли користувачі кіберпростору відчувають себе достатньо захищеними від кримінальних кіберпосягань і кіберзагроз;
- рівень відносної кримінологічної кібербезпеки, що створює складності функціонування відповідних об’єктів у кіберпросторі;
- рівень недостатньої кримінологічної кібербезпеки, що не дозволяє користувачам кіберпростору благополучно реалізувати свої життєво важливі права та інтереси;
- рівень низької кримінологічної кібербезпеки, коли користувачі кіберпростору не відчувають себе захищеними від кримінальних кіберпосягань і кіберзагроз.

Список використаних джерел

1. Сучасні тренди кібербезпекової політики: висновки для України: аналітична записка Нац. ін-ту стратегічних досліджень при Президентові України. URL: http://www.niss.gov.ua/articles/294/ (дата звернення: 15.04.2022).

2. Шеломенцев В. П. Безпека людини, суспільства і держави в Україні : кримінологічний аспект. *Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал ; Міжвід. наук.-досл. центр з проблем б-би з орг. злоч. при РНБО України.* 2010. № 22. С. 215–222.

3. Про кіберзлочинність : Конвенція Ради Європи. *Офіційний вісник України*. 2007. № 65. С. 107. Ст. 2535.