Волков Юрій Михайлович,
викладач кафедри
тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМА ПІДГОТОВКИ ФАХІВЦІВ КІБЕРБЕЗПЕКИ ДЛЯ ОРГАНІВ НАЦІОНАЛЬНОЙ ПОЛІЦІЇ

На сьогоднішній день наше існування неможливе без тісної взаємодії з кібертехнікою, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людей і держави. Але людство, поставивши собі на службу телекомунікації і глобальні комп'ютерні мережі, не передбачало, які можливості для злочинних діянь створюють ці технології. На сьогодні жертвами злочинців, що діють у віртуальному просторі, можуть стати не лише люди, але і цілі країни. При цьому безпека тисяч користувачів інтернет простору залежна від декількох злочинців. Кількість злочинів, що здійснюються в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, за оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет, є найшвидшими на планеті.

Небезпеку кіберзлочинності як для всього світу, так і для України визнають і вітчизняні правоохоронні органи, як найбільш актуальну проблему. Так, на наш погляд, кіберзлочинність (злочинність у сфері високих технологій) в даний час є однією з найбільш серйозних загроз національній безпеці України в інформаційній сфері.

Створення підрозділу з висококваліфікованими працівниками у сфері кібербезпеки є, однією з актуальних проектів, так як дана сфера є найбільш незахищеною і привертає увагу багатьох осіб, які посягають на приватне життя та інші блага пов'язанні з інтернет простором.

Першим кроком, у розвитку безпеки громадян та захисту їх конфіденційної інформації на законодавчому рівні, було затвердження "Стратегії кібербезпеки України" указом президента України станом на 15 березня 2016 року. Даний указ закріплює забезпечення безпеки у кіберпросторі, шляхом застосування сукупності правових, організаційних, інформаційних заходів, що, безпосередньо, базуються на принципах верховенства права і поваги до прав та свобод людини і громадянина, забезпечення національних інтересів України.

Якщо аналізувати даний нормативний документ, а саме у четвертому положенні указу, стає зрозуміло, що майже усі можливі дії та заходи, щодо вдосконалення захисту у сфері кіберпростору, вжиті з боку законодавця, серед яких є:

– розробка та оперативна адаптація державної політики в сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС і НАТО;

– створення національної нормативно-правової та термінологічної основи в цій сфері, гармонізація нормативних актів у сфері електронних кому-

нікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів та стандартів ЄС і НАТО і т.д.[1]

Вищезазначені положення, безумовно, мають чимале значення у гарантуванні безпеки в кіберпросторі, так як стали гарантом діяльності органу кібербезпеки, але впровадження надійного апарату протидії злочинам у кіберпросторі є проблемним, через низький рівень підготовки здобувачів освіти, оскільки дана сфера вимагає знання:

– теоретичних основ кібернетичної безпеки;

– правових та організаційних засад протидії кіберзлочинності;

– методів та засобів протидії кіберзлочинності;

– програмного забезпечення систем кібернетичної безпеки;

– криптографічних механізмів кібернетичної безпеки;

– кібернетичної безпеки підприємств; − основ кібернетичної безпеки держав тощо.

Але у ВНЗ діючих на території України не існує відповідних дисциплін, які, на думку багатьох науковців, могли б надати такий багаж знань. Проте впровадження таких дисциплін, як: "Кібернетичний простір", "Інформаційні технології та системи кібернетичного простору", "Технологія організації збору та добування інформації у кіберпросторі, її обробки аналізу і синтезу", "Основи автоматизації процесів інформаційної діяльності у кібернетичному просторі" – значно змінили б становище майбутніх фахівців, у сфері кібербезпеки. Ввівши вище зазначені дисципліни у ВНЗ зі специфічними умовами навчання системи МВС, здобувачі освіти у цих закладах можуть отримати:

– здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства, застосовувати досягнення інформатики й обчислювальної техніки, проводити цілеспрямований пошук і збір інформації з відкритих, а також її добування з відносно-відкритих і закритих електронних джерел;

– здатність виявляти ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки;

– здатність організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної і кібербезпеки з урахуванням їх правової обґрунтованості, адміністративно-управлінської й технічної реалізуємості й економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації;

– здатність протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;

– здатність організовувати проведення атестації об'єкта на відповідність вимогам державних або корпоративних нормативних документів;

– здатність брати участь у розробці підсистем управління інформаційною і кібербезпекою, здійснювати їх адміністрування й експлуатацію;

– здатність до проведення попереднього техніко-економічного аналізу

й обґрунтування проектних рішень по забезпеченню кібербезпеки;

– здатність оформлювати технічну документацію з урахуванням діючих нормативних і методичних документів в області інформаційної і кібербезпеки [2].

Отже, підготовка фахівців у даній сфері має вагоме значення у гарантованій безпеці кіберпростору, але проблема підготовки, справді, висококваліфікованих кадрів, що підготовленні до усіх реалій у цій сфері й посягань на блага людини та держави, залишається відкритою.

1. Указ Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" від 27 січня 2016 року прийнятий 15 січня 2016 року № 96/2016. – Режим доступу., Електронний ресурс: http://zakon3.rada.gov.ua/laws/show/96/2016;

2. Бурячок В.Л. "Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні"// Кібербезпека та захист критичної інформації інфраструктури., - 2014 р., С. 126-131.

Воронов Ігор Олександрович
д.ю.н., с.н.с., провідний науковий
співробітник Одеського державного
університету внутрішніх справ

ВИКОРИСТАННЯ ПРОГРАМНИХ КОМПЛЕКСІВ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Концепція "інформаційного суспільства" розкрила принципово важливу рису суспільства, відкрила нові властивості інформації та підкреслила її зростаючу роль. Основними рисами, що характеризують інформаційне суспільство, є постійне збільшення ролі інформації і знань, постійний розвиток комунікацій, продуктів та послуг, глобального інформаційного простору.

Поява та розвиток високих інформаційних технологій являє собою масштабний динамічний процес, який має постійний та цілеспрямований характер. Внаслідок цього невпинно удосконалюються і створюються нові засоби та способи обробки інформації.

Важливого значення набувають методи або способи обробки інформації, зокрема її візуального аналізу даних та виявлення прихованих зв'язків.

Одержувані з різноманітних джерел відомості повинні всебічно вивчатися й оцінюватися з погляду їхньої значущості та можливості подальшого використання для забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку.

Реалізація наявного інформаційного матеріалу – наступний етап процесу оперативно-розшукової діяльності. Її успішність визначається насамперед якісним рівнем, на якому перебуває організація збирання й аналізу інформації.

Специфікою сучасних вимог до продуктивної переробки інформації є те, що:

- дані мають значний обсяг;