питання довіри: третя особа може діяти зловмисно, наприклад, з метою збільшення свого прибутку. Рішення полягає в тому, що метод прийнятий так, для автентифікації потоку, що клієнти можуть перевіряти цілісність і актуальність отриманих від сервера даних. При цьому метод задовольняє вимогам IoT пристроїв, що характеризуються обмеженими ресурсами з точки зору енергоспоживання, обчислювальної потужності і захисту пристроїв.

Проведений аналіз безпеки інтернет речей показує, що поширення послуг IoT вимагає гарантування автентифікації, масштабованості, конфіденційності, сумісності та відповідності протоколам безпеки. Він проливає світло на напрямки досліджень в області поширення IoT.

1. Internet of Things Global Standards Initiative [Електронний ресурс]: – Режим доступу: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

2. S. Paradopulus, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB Journal, 2010, Vol. 19, №1, pp.161-180.

3. Understanding KMS [Електронний ресурс]: – Режим доступу: https://technet.microsoft.com/ru-ru/library/ff793434.aspx.

4. elliptical curve cryptography (ECC) [Електронний ресурс]: – Режим доступу: http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography.

Підготовка фахівців для боротьби з кіберзлочинністю в Україні

Бобик М.В.
курсант групи ПС – 541 факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

В наш час комп'ютерні злочини є поширені оскільки технології розвиваються і люди не сидять на місці. Це залежить від прискореного

розвитку технологій й науки у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Історія навчила нас, що розвиток і прогрес, які приносять людям нові блага та можливості, на жаль, завжди супроводжуються негативними явищами. Також масова комп'ютеризація, і стрімкий розвиток цифрових технологій, які максимально спростили людині всі технологічні та виробничі процеси, полегшили її існування та перевернули уявлення про роботу, кар'єру, дозвілля, фінанси і навіть особисте життя, приховують у собі серйозні небезпеки[1].

Неможливо сьогодення уявити без нових інформаційних технологій ,в потребі яких полягає широке використання комп'ютерної техніки та новітніх засобів комунікації. Більшість функцій суспільства пов'язані з комп'ютерами, інтернет - мережами та комп'ютерною інформацією.

Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Інтернет – це чудовий засіб для зв'язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються, злочини, кіберзлочини. Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем - це далеко не повний перелік подібних злочинів [1].

На сьогодні Україна не стоїть на місці а просувається вперед в підготовці фахівців для боротьби з кіберзлочинністю :

-у березні 2016 року уряд прийняв Стратегію кібербезпеки України, яка має на меті створення національної системи кібербезпеки;

-у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки. Першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки.

-у вересні 2016 року Верховна Рада України у першому читані прийняла закон про основні засади забезпечення кібербезпеки України[3].

- починаючи з 2016 року Харківський національний університет внутрішніх справ здійснює підготовку фахівців з вищою освітою для

підрозділів Національної поліції України, що займаються протидією кіберзлочинності, злочинам у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності [4].

-17 березня 2017 року відбулося підписання Меморандуму про співпрацю між Державною службою інтелектуальної власності (ДСІВ) та Національною академією внутрішніх справ (НАВС). Одним із перспективних напрямів подальшої співпраці сторони вважають реалізацію Проекту з підготовки фахівців по боротьбі з кіберзлочинністю. Створення на базі Національної академії внутрішніх справ курсів з підготовки правоохоронців за спеціалізацією, що спрямована на захист прав інтелектуальної власності, стане платформою для розробки нової освітньої програми, за якою відбуватиметься навчання правників нової генерації, покликаних захистити інноваційний потенціал України.

До підготовки українських спеціалістів вже висловили готовність долучитися міжнародні експерти урядових та громадських структур, які безпосередньо здійснюють боротьбу з кіберзлочинністю. Курси розраховані на правоохоронців системи МВС, СБУ, фіскально-митних органів і Державної служби спеціального зв'язку, в обов'язки яких входить захист прав інтелектуальної власності, боротьба з кіберзлочинністю[2] .

Отже, на нашу думку просування в розвитку в підготовці фахівців для боротьби з кіберзлочинністю є важливою функцією в Україні, так як з кожним роком суспільство рухається в науці, техніці, збільшуються злочини, кіберзлочини прогресують у всіх сферах суспільного життя.

Тож протидія кіберзлочинності та рівень кібербезпеки на сьогодні одним із пріоритетних напрямків в політиці країни. Але для комплексної боротьби з цією проблемою потрібні спільні зусилля держави, громадян та міжнародної спільноти[3].

1.[Електронний ресурс]. - Режим доступу: https://www.science-community.org/ru/node/16132

2.[Електронний ресурс]. - Режим доступу: http://nk.org.ua/ tekhnologii/pidgotovka-fahivtsiv-po-borotbi-z-kiberzlochinnistyu-ta-piratstvom-93239

3.[Електронний ресурс]. - Режим доступу: https://www.gurt.org.ua/ articles/34602

4. [Електронний ресурс]. - Режим доступу: http://univd.edu.ua/dir/ 589/fakultet--4