вимірювання величини втрати артикуляції приголосних вираженою у відсотках. Метод Alcons широко використовується, особливо в США, для наближеної оцінки розбірливості мови і відображає втрату вокалізованих приголосних, викликану реверберацією і поглинанням звуку в приміщенні.

Використані джерела

1. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962. – 390 с.
2. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – М.: 2000, № 4.
3. К оценке эффективности защиты акустической (речевой) информации. [Електронний ресурс]: - Режим доступу: http://st.ess.ru/publications/articles/tspi/tspi.htm.

Дворецький О.О. - інспектор ВПДО УІАП в Дніпропетровській області;
Калюга Р.І. - інспектор СІП Новомосковського ВП ГУНП в Дніпропетровській області;
Паштета О.М. - старший інспектор СІП Новомосковського ВП ГУНП в Дніпропетровській області;
Рижков Е. В. - завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету, кандидат юридичних наук, доцент

ОПТИМІЗАЦІЯ ДЕЯКИХ ПІДСИСТЕМ ІПС ОВС ТА ІТС НПУ ТА ІНШІ ПИТАННЯ В ДІЯЛЬНОСТІ ПРАЦІВНИКІВ ІАП ГУНП

В процесі реформування діяльності органів Національної поліції Департаментом інформаційно-аналітичної підтримки поступово реалізується запровадження нової концепції діяльності структурних підрозділів. Централізація та оптимізація доступу до баз даних, питання безпеки - є пріоритетними. Саме тому, проблемні питання діяльності інформаційно-аналітичних підрозділів, які існують на сьогодні, повинні бути враховані при вдосконаленні цього виду діяльності в Національній поліції.

Традиційно, працівник ІАП працює з кількома службовими базами, які різняться процедурами ідентифікації. Тому не було б зайвим створення комплексу програмного забезпечення типу автоматизованого робочого місця з єдиним протоколом ідентифікації що б об’єднував та здійснював одночасний вхід до систем. Це б також позитивно позначилось на можливому подальшому електронному документообігу з УІАП в областях та їх структурними підрозділами (зокрема за допомогою включених засобів обміну інформацією).

Актуальним є також питання матеріально-технічного та програмного забезпечення підрозділів ІАП. Однією з проблем роботи є незадовільне забезпечення комп’ютерним обладнанням, багатьом комп’ютерам у

відділеннях по 10-15 років, що унеможливлює встановити на них відповідні програми, тому як операційна система не відповідає вимогам оновлених програм.

Наступною проблемою є незадовільний доступ до всесвітньої мережі «Інтернет», це виявляється у низькій швидкості, обмеженому доступі ,що в свою чергу не надає можливості коректно та швидко переглядати та вводити інформацію в системах ІІПС «Армор» та ІТС «Цунамі».

Критичною також залишається ситуація зі штатною чисельність ІАП. СІП за штатним розписом передбачені лише у відділах поліції, які включають в себе 4-5 відділень. Разом з тим у відділеннях поліції здебільшого є можливість закріплення лише по одному працівнику СІП, а це в свою чергу унеможливлює якісну роботу по всім напрямкам службової діяльності, зокрема під час перебування даного працівника у відпустці, відрядженні тощо.

Практичний досвід роботи з ІІПС ОВС «Армор» (далі ІІПС), ІТС НПУ «Цунамі» (далі ІТС НПУ) дозволив виявити низку проблемних питань, які потребують свого потенційного вирішення. Тому автори висловлюють ряд порад, побажань, спрямованих на оптимізацію роботи їх підсистем.

Інформаційна підсистема «Єдиний облік» ІТС НПУ. Одна з найголовніших підсистем ІТС НПУ. Суть її роботи полягає у реєстрації заяви (повідомлення), введення інформації щодо суті події, місця, дати, часу, заявника чи потерпілого, кваліфікації тощо. На інформацію, введену до ІП «ЄО» спирається безліч інших підсистем, тому від своєчасного, повного та об'єктивного внесення даних до електронних контурів – запорука розкриття злочину. Так, ІП «ЄО» містить вкладку «Речі», для заповнення в т.ч. на випадок крадіжки, добровільної здачі, знахідки тощо речей, які можна ідентифікувати за зовнішніми ознаками (як правило номером). Разом з тим ІТС НПУ містить ряд окремих підсистем, для роботи з окремими їхніми групами (ІП «Номерна річ», «ТЗ, що розшукується», «Кримінальна зброя», «Добровільно здана, знайдена зброя» і т.д.). Їх функціонування мотивується також і необхідністю співпраці з іншими, в т.ч. зовнішніми базами та системами (наприклад, ІП «ТЗ, що розшукуються»). Джерелом для заповнення підсистем є, як правило, інформація, внесена до вкладки «Речі» ІТС НПУ. Тобто, на сьогоднішній день ми маємо проблему дублювання інформації у вкладці «Речі» ІП «ЄО» та у відповідній підсистемі (введення чи корегування однієї і тієї ж інформації до двох підсистем), що призводить до виникнення розбіжностей та, найголовніше, втрачається дорогоцінний час, знижується оперативність розкриття злочинів. Як приклад: інспектор-черговий ОНП реєструє крадіжку мобільного телефону та вносить інформацію щодо нього до вкладки «Речі» ІП «ЄО». Відповідальним за введенням інформації до ІП «Номерна річ» начальником ОНП визначено оперуповноваженого СКП (по аналогії з Інструкцією ІІПС ОВС). У випадку подібної організації роботи в ОНП втрачається час для розкриття злочину, знижується оперативність, нераціонально використовуються ресурси (в т.ч. шляхом визначення окремого працівника, надання чи корегування йому

відповідного доступу тощо). На теперішній час більш-менш нормативно врегульоване питання роботи з ІП «Транспортні засоби, що розшукується», так як в методичних рекомендаціях 2018 року обов'язок введення до неї інформації та підтримання її в актуальному стані належить до компетенції інспектора-чергового органу поліції.

ШЛЯХИ ВИРІШЕННЯ. 1. Програмний – внесення змін до ІТС НПУ при яких у випадках коли об'єктом злочину виступає предмет щодо якого передбачена окрема підсистема – дані з вкладки «Речі» ІП «ЄО» автоматично експортувалися до відповідної підсистеми. Також необхідно передбачити можливість перевірки актуальності даних та автоматичного оновлення стану (наприклад, знаття з обліку в обох підсистемах одночасно). У даному випадку відсутня також необхідність надання (корегування) доступу до цих підсистем наприклад, працівникам чергової служби ОНП. В разі ж виникнення необхідності введення інформації про певний об'єкт джерелом якого виступає не реєстрація у ІП «ЄО» - дані вносяться до підсистеми окремо працівником СІП. 2. Нормативний – на рівні ДІАП (УІАП) розпорядчим документом визначити окремі служби, працівники яких будуть відповідальними за формування певних підсистем (по аналогії з ІІПС).

Пропонуємо також надати старшому інспектору–черговому територіального підрозділу поліції більше можливостей по корегуванню карток, які надходять по даній лінії, в т.ч. їх об'єднання. Наприклад, може одна людина по одному і тому ж факту дзвонити на лінію «102» по декілька раз в окремих випадках - до 10-ти) і весь час приходять нові картки, що в свою чергу призводить до збільшення кількості реєстрацій. Також, на нашу думку, було б доцільним не реєстрація або одночасне списання до справи повідомлень, які не містять ознак кримінального чи адміністративного правопорушення та виключають випадки необхідності надання поліцейських послуг без направлення картки «102» до територіального підрозділу (наприклад, щодо надання контактних телефонів працівників, служб, «інформація незрозумілого змісту», коли заявник «верзе нісенітницю» та ін). Це в свою чергу сприятиме зменшенню кількості реєстрацій та виключення випадків висміювання фабул подій в т.ч. в мережі Інтернет.

Вкладка «Рішення» ІП «ЄО» унеможливлює складання висновку про списання матеріалів «до справи» деякими працівниками в т.ч. працівниками ДС, заступником начальника тощо. Хоча ці працівники досить часто складають подібні висновки, наприклад, при добровільній здачі зброї чи після проведення перевірки по факту несвоєчасного прибуття ГРПП чи СОГ.

ШЛЯХИ ВИРІШЕННЯ. 1. Внесення змін до програмного коду ІТС НПУ. У випадку проставлення у ІП «ЄО» рішення «внесено до ЄРДР» доцільно б було експортувати наявну інформацію до ІП «Кримінальна статистика» (далі ІП «КС»), а саме: орган, місце скоєння, кваліфікація, заявник і т.д. Внесення ж іншої інформації – проводилась би працівником СІП після отримання від слідчого картки Ф. 1. Разом з тим актуальним залишається питання кваліфікації злочинів, а саме відповідність інформації в ІП «ЄО», ІП «КС» та ЄРДР. Саме тому необхідно передбачити автоматичну

зміну кваліфікації після корегування відповідного поля в одній з систем. Це б у свою чергу підтримувало статистичні дані в актуальному стані та значно зменшило б час на внесення інформації до електронних контурів.

Значно б полегшало роботу працівників ІАП і інтегрування ЄРДР до ІП «КС», чи хоча б можливість доступу до ЄРДР через відомчу мережу НПУ.

Інформаційна підсистема «Особа» ІТС НПУ. На сьогоднішній день маємо проблемну ситуацію в вигляді наявності в даній підсистемі електронних карток фактично однієї і тієї ж особи проте з незначними розбіжностями (наприклад, у вигляді місця народження – населеного пункту чи району, дати тощо), які розпізнаються підсистемою як різні. Це пов'язано зокрема із значною кількістю структурних підсистем, багатьма користувачами з можливістю введення відповідної інформації. Як приклад, інспектор-черговий (помічник чергового) отримавши повідомлення вносить до ІП «ЄО» першочергові дані щодо особи заявника з його слів, крім того нерідко трапляються випадки відсутності чи неповідомлення такої інформації. Цей факт негативно впливає зокрема на час обробки інформації, адже необхідно переглянути інформацію всіх карток, часто виникають помилки кваліфікації адміністративних правопорушень, як наслідок повернення судом матеріалів адміністративних правопорушень на доопрацювання, закриття адміністративних правопорушень, уникнення потенційного правопорушника від відповідальності.

ШЛЯХИ ВИРІШЕННЯ. 1. Надання окремій особі територіального підрозділу поліції (наприклад, працівникові ІАП) право на об'єднання карток осіб за наявності обґрунтованих підстав (наприклад, при внесення даних до ІП «Адмінпрактика» маються дані про документ, що посвідчує особу).

У зв'язку зі службовою діяльністю досить часто виникає необхідність прикріплення фото особи до її електронної картки ІП «Особа». Проте програмно це можливо лише, наприклад, у випадах перебування особи на відповідних профілактичних обліках, доставляння чи затримання особи тощо та при наявності чітко визначених законодавчих підстав, які не відповідають потребам служби. Адже існує категорія громадян, які представляють чи можуть представляти оперативний чи службовий інтерес (особи ромської національності, без постійного місця проживання, особи, які часто залишають місце постійного проживання чи навчання (підпадають під категорію безвісно зниклих), психічно хворі, правопорушники тощо). Наявність фотокартки осіб даних категорій значно полегшив би процес ідентифікації, позитивно сприяв би оперативності здійснення розшукових заходів тощо.

ШЛЯХИ ВИРІШЕННЯ. 1. Законодавчий – на нормативному рівні розширення кола підстав для здійснення фотографування особи. 2. Програмний – поповнення інших підсистем ІТС НПУ можливістю прикріплення фотокартки особи.

Інформаційна підсистема «Адмінпрактика». Дана інформаційна підсистема ІТС НПУ призначена для введення інформації щодо складених поліцейськими протоколів про адміністративні правопорушення, накладення

та виконання стягнень. Згідно КУпАП підставою для визначення повторності є «вчинені повторно протягом року після застосування заходів адміністративного стягнення» як і ст. 39 КУпАП: «якщо особа, піддана адміністративному стягненню, протягом року з дня закінчення виконання стягнення не вчинила нового адміністративного правопорушення, то ця особа вважається такою, що не була піддана адміністративному стягненню». Ключовим моментом у цій ситуації виступає необхідність висвітлення у відомчих підсистемах (ІП «Адмінпрактика») виду накладення адміністративного стягнення та, що найголовніше, відмітку його виконання та дату виконання. Проте КУпАП передбачено кілька суб'єктів розгляду та прийняття рішення за адміністративними матеріалами, проте КУпАП не містить жодних законодавчо визначених підстав надання цими суб'єктами інформації до поліції для її внесення до підсистеми. Надсилання відповідних запитів з метою отримання такої інформації як правило займає досить багато часу чи взагалі безрезультатно. Як наслідок – неправильна кваліфікація дій правопорушника з подальшим поверненням матеріалів чи закриття провадження та уникнення особи від відповідальності.

ШЛЯХИ ВИРІШЕННЯ. 1. Законодавчий – визначення у нормативній базі (наприклад, КУПАП) обов'язку суб'єкта прийняття рішення повідомити про це до орган, посадова особа якого склала протокол протягом певного строку (наприклад, 1 робочого дня). 2. Програмний – на сьогоднішній день маємо Інтернет-ресурс судових рішень, в т.ч. за адміністративними матеріалами. Саме тому було б доцільно інтегрувати автоматичний експорт цих рішень до відомчих підсистем та, зокрема, до вкладки про прийняте рішення кожної електронної картки протоколу. 3. Глобальний – створення єдиної об'єднаної системи на базі Інтернет-ресурсів, що об'єднувала б інформацію з усіх суб'єктів розгляду адміністративних матеріалів, ДВС, секторів пробації Міністерства дстиції з подальшим інтегруванням її до ІП ІТС НПУ (для ідентифікації можливе використання ЕЦП, так як його отримують більшість посадовий осіб даних установ і які являються суб'єктами декларування). Крім того у ІП «Адмінпрактика» передбачена можливість автоматичного експорту інформації щодо сплати штрафу правопорушниками проте лише по лінії безпеки дорожнього руху. Цей факт потребує оптимізації в вигляді застосування подібного експорту і до інших адміністративних протоколів. Це в свою чергу значно зменшить паперовий документообіг, забезпечить отримання інформації про сплату без повторного візиту до органу поліції та надання підтверджуючих документів (квитанції, чеку тощо).

На прикладі зазначених проблемних питань маємо ситуацію, яка потребує свого вирішення як мінімум адміністративно-нормативним шляхом, особливо в умовах, коли керівництвом Департаменту інформаційно-аналітичної підтримки та керівництвом Національної поліції у найближчий час буде реалізовуватися стратегія On-line інформаційно-аналітичного супроводу діяльності органів Національної поліції, в т.ч. оперативних підрозділів, слідства, патрульної поліції тощо, що, у сою чергу, є безумовно

перспективним форматом діяльності сучасного правоохоронного органу держави.

Демидов З.Г. - науковий співробітник;
Ницюк С.П. - старший науковий співробітник (Науково-дослідна лабораторія захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ)

КОМП'ЮТЕРНІ ВІРУСИ, ЯК ЗАСІБ ЗАРОБІТКУ

Найскладніше в специфіці хакеру не зламати чийсь комп'ютер або сервер, а залишитися непоміченим або анонімним при цьому. На призначених для користувача (домашніх) машинах, немає нормального захисту від вірусів. Ні військових суперпотужних серверів з хардварними фаєрволами, як в Пентагоні, які, до речі, теж зламуються хакерами. Ні відділу безпеки або навіть системного адміністратора, який хоч щось може протиставити злому. Від провайдера ми максимум отримуємо ізоляційну стрічку на кабелі))), основна наша надія на антивіруси з того ж інтернету, звідки до нас приходять віруси. Багато хто вважає, що віруси в їх комп'ютерах тільки гальмують систему і витрачають нерви користувача. Насправді хтось заробляє на них величезні гроші без вашого відома. Все, що відбувається в цьому світі, кому-то вигідно. З вірусами та ж історія [1].

Є 5 основних методів заробітку на вірусах:

1) Шантаж

Найпростіший метод, в нього потрапляють віруси-шифратори і "вінлокери". Суть проста - вірус при попаданні на комп'ютер шифрує всі дані на ньому або повністю блокує роботу комп'ютера. Для відновлення роботи зловмисник вимагає гроші за антивірус або програму-дешифратор. Звичайно ж, після отримання "викупу" ніхто нічого не надсилає і не розблокує. Вирішити проблему в принципі можна в сервісному центрі, або якщо є знайомий сисадмін. А в разі вірусу-шифратора можна сподіватися тільки на те, що дешифратор вже написаний. В іншому випадку доведеться відформатувати жорсткий диск і позбутися всієї інформації, яка там була ...

2) Прямий злом

Тут мова йде про крадіжку особистих даних. Користувач може і не здогадуватися, що зламаний, поки не спливе факт використання його особистих даних деінде. Вірус потрапляє на комп'ютер і знімає всю особисту інформацію користувача, висилаючи її на сервер зловмисника. Це інформація про паролі, логіни, номери банківських карток, рахунків і т.п. Зазвичай це робиться вірусом класу "кейлоггер".

3) Прихований злом

Тут зовсім інша система ... Користувач взагалі не повинен здогадатися