Наприклад для підвищення безпеки різних електронних сервісів альянс FIDO пропонує перехід на двофакторну систему аутентифікації користувачів. Учасники альянсу, до числа яких входять такі компанії, як Infineon, PayPal і Lenovo, відмічають, що сьогодні кіберзлочинці використовують паролі як одне з найбільш вразливих місць електронних систем.

При використанні одноразових паролів слід враховувати, що: використання SMS–повідомлень для доставки одноразових паролів не є абсолютно безпечним, оскільки SMS можуть бути перехоплені; картки одноразових паролів можуть бути вкрадені і скомпрометовані; генератори одноразових паролів також не завжди є безпечними.

Використання одноразових паролів не забезпечує можливість підписання електронних документів для надання їм юридичної значущості, а також не вирішує задачу забезпечення цілісності і конфіденційності даних, переданих по каналу зв'язку.

Для забезпечення цілісності і конфіденційності даних ряд Web-сервісів на додаток до одноразових паролів використовує вбудований у браузери протокол HTTPS з вбудованими криптоалгоритмами. Проте такий підхід не завжди застосовний зважаючи на законодавчі обмеження по обробці персональних даних, банківської таємниці, захисту даних в державних інформаційних системах і в інших випадках, коли потрібний захист конфіденційності даних відповідно до законодавства.

Більше того, нещодавно стало публічно відомо, що деякі спецслужби вже давно уміють читати дані, захищені західними криптоалгоритмами в HTTPS-протоколі стандартних браузерів. А значить не виключено, що це під силу і кіберзлочинцям. У зв'язку з цим використання надійних алгоритмів для шифрування є надійнішим при захисті конфіденційних даних.

Надійна аутентифікація є одним з ключових елементів системи інформаційної безпеки. Не знаючи, хто саме має доступ до конфіденційних даних, і чи являється цей "хтось" тим, за кого себе видає, неможливо побудувати ефективну, прозору і керовану систему захисту інформаційних ресурсів.

Вимоги до надійності, типу, технології і засобів аутентифікації залежать від важливості оброблюваної інформації, прав і повноважень адміністраторів і користувачів системи, вірогідності інциденту і визначаються на основі аналізу ризиків можливого збитку (фінансового, репутаційного, організаційного).

Добре зарекомендувала себе двофакторна аутентифікація, в процесі якої використовуються аутентифікаційні чинники двох типів. Наприклад, користувач повинен надати смарт-карту і ввести пароль. В цьому випадку зловмисник не зможе отримати доступ до даних, оскільки йому доведеться не лише підглянути пароль, але і пред'явити фізичний пристрій, крадіжка якого, на відміну від крадіжки пароля, практично завжди швидко виявляється.

Проте найбільш надійним і безпечним способом упевнитися в тому, що "хтось" є саме тим, за кого себе видає, виступає технологія строгої аутентифікації. При строгій аутентифікації користувач повинен довести, що має заздалегідь отриманим безпечним способом секрет (закритим криптографічним ключем). В процесі доказу сторони в захищеному режимі обмінюються послідовно підписаною інформацією. Строга аутентифікація не допускає підробки або клонування персонального секрету, яким є закритий криптографічний ключ.

Для строгої аутентифікації необхідно використовувати криптографію і інфраструктуру відкритих ключів (Public Key Infrastructure - PKI). Інші методи і технології здатні забезпечити лише просту або посилену аутентифікацію.

У Україні запустили пілотний проект універсальної електронної ідентифікації громадян через банківські дані. Проект вирішуватиме питання верифікації користувача через Інтернет для надання довідок, дозвільних та інших документів в електронному вигляді.

Суть технології проста: банки країни об'єднуються в систему, яка дозволяє проводити видалену ідентифікацію, умовно кажучи, Інтернет-банкінг. Наприклад, щоб отримати довідку на державному порталі, Вам досить ввести пароль Інтернет-банкінгу вашого

банку і, скажімо, SMS-пароль (щось схоже, до речі, дозволяє робити Facebook). При обранні громадянином верифікації особини через BankID достатньо ввести логін та пароль свого Інтернет -банку, пройти через другий етап авторизації шляхом введення SMS-паролю — і отримати доступ до переліку електронних послуг.

Онищенко Ю.М., Минко П.Є.

ОРГАНІЗАЦІЙНІ ТА ПРАВОВІ ОСНОВИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Міжнародні організації визнають і небезпеку кіберзлочинності, і її транскордонний характер, обмеженість одностороннього підходу до вирішення цієї проблеми і необхідність постійної та активної міжнародної співпраці як щодо вжиття необхідних технічних заходів, так і в розробленні міжнародного законодавства. Рада Європи, Європейський Союз, ООН та Інтерпол – усі ці організації відіграють важливу роль у координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами у сфері високих технологій.

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 р. в Будапешті Конвенція Ради Європи про кіберзлочинність. Це один із найважливіших правових актів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі, і поки що єдиний документ такого рівня.

17 липня 2014 р. Кабінет Міністрів України розглянув проект Указу Президента України "Про Стратегію забезпечення кібернетичної безпеки України". Проект Указу був розроблений адміністрацією ДССЗЗІ на виконання рішення РНБО України від 28 квітня 2014 р. "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", уведеного в дію Указом Президента України від 1 травня 2014 р. № 449. Проект Указу був схвалений Урядом та переданий на розгляд РНБО.

Проект Указу був підтриманий та погоджений без зауважень Міністерством внутрішніх справ, Міністерством фінансів України, Державним агентством з питань науки, інновацій та інформатизації України (Держінформнауки) та Державною службою України з питань захисту персональних даних. Частково було враховано зауваження та пропозиції СБУ, Міністерства економічного розвитку і торгівлі та Міністерства юстиції України. Наступним кроком у формуванні національної системи кібербезпеки має стати прийняття Закону України "Про основні засади забезпечення кібербезпеки України".

Проект цього Закону, розроблений адміністрацією ДССЗЗІ, вже пройшов обговорення за участю представників громадськості та зацікавлених державних органів. Сьогодні він перебуває на етапі остаточного погодження та найближчим часом буде поданий на розгляд Кабінету Міністрів України. Ця робота здійснювалась з урахуванням основних принципів забезпечення кібербезпеки України, покладених в основу проекту Стратегії.

Порівняльний аналіз досліджень зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до збільшення. Однією з умов її зростання є ускладнення технічних систем глобального зв'язку (телефонної, радіо, супутникової) та спрощення доступу до використання комп'ютерних технологій широкого кола користувачів через персональні комп'ютери.

Дослідження проблем боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні й технологічні засоби забезпечення інформаційної безпеки (технічного захисту інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху. Парадокс полягає в тому, що чим складніше стає комп'ютерне програмно-математичне забезпечення, тим більш вразливими виявляються традиційні організаційні заходи і засоби інженерно-технічного захисту інформації в автоматизованих (комп'ютерних) системах, зокрема відносно несанкціонованого доступу.

Проблемою наступного порядку також є і те, що з розвитком сучасних електронних засобів інформації розвиваються технічні засоби перехоплення й доступу до інформації, що обробляється й передається в електронних системах зв'язку. Доступ до цих засобів не створює проблеми для злочинних формувань.

Найбільшу небезпеку для суспільства, держави становить транскордонна організована кіберзлочинність: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з комп'ютеризованих баз даних і порушення права інтелектуальної власності на комп'ютерні програми; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин.

Питаннями вдосконалення правового регулювання, визначення й організації реалізації державної політики у сфері інформаційних стосунків займаються також Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомча робоча група з розроблення й узгодження Концепції легалізації програмних продуктів і боротьби з їх нелегальним використанням.

Аналіз емпіричного матеріалу дозволяє зробити прогноз, що в разі невирішення проблем боротьби з організованою кіберзлочинністю, особливо у сфері міжнародних економічних відносин, на Україну з боку міжнародного співтовариства посилюватиметься інформаційний, політичний та економічний тиск.

Правові основи протидії комп'ютерній злочинності на національному рівні визначено у Кримінальному Кодексі України. Окремі види комп'ютерних злочинів (кіберзлочинів) виділено в окремий розділ XVI Особливої частини – "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж" (ст. 361, 361, 363).

За скоєння злочинів проти основ національної безпеки (конституційного ладу України): проти життєво важливих інтересів особи, суспільства держави, громадської безпеки. або скоєння інших злочинів, передбачених чинним ККУ, з використанням функціональних можливостей (технологій) комп'ютерних мереж, комп'ютерних систем, комп'ютерних інформаційних ресурсів та інших електронних інформаційних технологій, покарання призначається за статтями Особливої частини, у яких передбачається відповідальність за такий злочин.

Такий правовий захід дозволить забезпечити здійснення організаційних та інших заходів, у тому числі об'єктивного моніторингу і статистику комп'ютерних злочинів і комп'ютерної злочинності в Україні.

Серед інших організаційних заходів в Україні на урядовому рівні створено багато робочих груп, що розробляють проекти законодавчих і підзаконних актів у сфері громадських інформаційних стосунків, які прямо або побічно відбивають питання протидії та запобігання кіберзлочинності і взаємодію з різними транснаціональними організаційними структурами.

Аналіз різних ініціатив зі створення проектів нормативно-правових актів свідчить, що між вказаними та іншими державними структурами немає взаємодії, координації діяльності. На законодавчому рівні лобіюються суперечливі антидержавні потреби та інтереси на тлі сповідання ідей правового нігілізму з чинним законодавством, що провокує масовий правовий хаос, у тому числі у правотворчій діяльності. Сьогодні у сфері інформаційного законодавства створено умови, що дозволяють злочинцям "законно" уникати відповідальності, використовуючи конфлікти різних юридичних норм. Вказаний чинник можна розглядати як додаткову ознаку латентності кіберзлочинності.

Колісник Т.П.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ОСВІТНЬОМУ ПРОЦЕСІ МАЙБУТНІХ ОФІЦЕРІВ ПОЛІЦІЇ

Впровадження інформаційних технологій у освітній процес забезпечує розвиток особистості, майбутнє професійне становлення. При використанні інформаційних технологій викладачеві необхідно створювати умови для реалізації всебічного розвитку особистості: пізнавального інтересу, творчого мислення, комунікативних вмінь, естетичного аспекту.

Використання інформаційних технологій в освітньому процесі є ефективним, за умови що викладач має високу професійну компетентність у області інформаційних технологій і вміння: застосовувати дані технології в підготовці, аналізі, коригуванні освітнього процесу, управлінні освітнім процесом і навчально-пізнавальною діяльністю курсантів; добирати найраціональніші методи і засоби навчання, враховуючи індивідуальні особливості курсантів, їх нахили і здібності; ефективно поєднувати традиційні методичні системи навчання із новими інформаційними технологіями.

Основними шляхами застосування інформаційних технологій в освіті є:

- створення інформаційних середовищ навчальних закладів;
- створення педагогічних програмних засобів;
- застосування інформаційно-комунікаційних технологій під час здійснення проективного і дослідницького навчання;
- застосування мультимедійних засобів навчання;
- розробка дистанційних курсів;
- застосування інформаційних технологій в управлінні навчальним закладом;
- використання засобів Інтернет з метою пошуку інформації, розробки програмно-методичного забезпечення навчальних закладів, професійного і психологічного консультування;
- створення Web-сайтів навчальних закладів;
- здійснення профорієнтаційної роботи в закладах освіти тощо.

У освітньому процесі використовують навчальні, моделюючі, імітаційні, діагностичні, тренувальні програми, інструментальні програмні засоби.

Посилення самостійної аудиторної та позааудиторної роботи з використанням інформаційних технологій, забезпечує здатність самостійно здобувати і розвивати знання та творчо їх використовувати.

Для оптимізації процесу підготовки майбутніх офіцерів поліції все більшої уваги приділяється використанню інформаційних технологій. Акцентується увага на їх ефективності в управлінні процесом навчання, організації самостійної роботи над вивченням нового матеріалу та розвитку пізнавальної діяльності курсантів. Інформаційно-навчальне середовище використовує дидактичні засоби, засновані на високотехнологічних комп'ютерних, мультимедійних й комунікаційних технологіях.

Інформативна підготовки курсантів здійснюється навчальними дисциплінами, визначеними нормативними документами. У змісті навчання цих дисциплін сформульовані вимоги до рівня професійної підготовки працівників поліції. Основною задачею вибіркових дисциплін кафедри інформаційної та економічної безпеки є формування знань, умінь та навичок, необхідних для використання сучасних інформаційних технологій в практичній діяльності та ознайомлення з напрямами застосування інформаційних технологій в професійній діяльності.

Для вирішення проблем якісної підготовки майбутніх офіцерів поліції з використанням інформаційних комп'ютерних технологій необхідно створити у вищому