The content of the direct actions on non-violent power abuse or official position by the employees of the SPSU is: transfer (entry) on the protected area (zone) of prohibited items and/or against the established order like mobile phones, chargers, cigarettes, money (87 %); unauthorized, contrary to the established order permitting the convicted to leave the location in connection with performing certain works by other intended going beyond the limits of penal institutions (13 %).
Abuse of the influence by the employee of the SPSU in most cases is linked to illegal interference in the process of operative management of the property, which is on the balance of the SPSU and is the property of the state. The motivation of these crimes – is lucrative. The decision of their commission is made by the employee of the SPSU according to the appeals of individuals interested in the use of the state property within unlawful conditions. A characteristic feature is the detailed planning of the crime, provision of legal cover in the form of signing contracts, etc.

Keywords: *employee of the State Penitentiary Service, authorities, mechanism, misuse, abuse, crime.*

УДК 004.056

Ю. М. ОНИЩЕНКО,
кандидат наук з державного управління,
доцент кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: http://orcid.org/0000-0002-7755-3071;

К. Е. ПЕТРОВ,
доктор технічних наук, професор,
професор кафедри штучного інтелекту
Харківського національного університету радіоелектроніки;

І. В. КОБЗЕВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і систем управління
Харківського регіонального інституту державного управління
Національної академії державного управління при Президентові України;
ORCID: http://orcid.org/0000-0002-7182-5814

ПРОТИДІЯ ЗЛОЧИНАМ, ЩО ВЧИНЯЮТЬСЯ ЗА ДОПОМОГОЮ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ІНТЕРНЕТІ

Досліджено найбільш поширені алгоритми злочинних дій у мережі Інтернет та визначено проблеми, що виникають під час профілактики та боротьби з кіберзлочинністю. Сформульовано пропозиції щодо протидії використанню різноманітних технік соціальної інженерії для здійснення шахрайських дій у мережі Інтернет.

Ключові слова: *кіберзлочинність, соціальна інженерія, хакери, інтернет-ресурс, фішинг, web-сайт.*

Onyshchenko, Yu.N., Petrov, K.E. and Kobzev, I.V. (2017), "Counteraction crimes committed by the methods of social engineering in the Internet" ["Protydiia zlochynam, shcho vchyniaiutsia za dopomohoiu metodiv sotsialnoi inzhenerii v interneti"], *Pravo i Bezpeka*, No. 1, pp. 63–68.

Постановка проблеми. Сучасне інформаційне суспільство охоплює всі сфери життєдіяльності людини та держави. Однак людство, широко користуючись телекомунікаційними та глобальними комп'ютерними мережами, не змогло передбачити те, які можливості для зловживань створюють ці технології. Сьогодні жертвами злочинців, які орудують у віртуальному просторі, можуть стати не лише люди, й держави. При цьому безпека тисяч користувачів може залежати від дій декількох злочинців. За таких умов особливого значення набуває пошук нових можливостей забезпечення безпеки у зв'язку з появою нової арени боротьби зі злочинністю – кіберпростору. Темпи зростання кількості злочинів, що здійснюються в цій сфері, збільшуються пропорційно кількості користувачів комп'ютерних мереж і, за оцінками Інтерполу, є найшвидшими на планеті [1, с. 1].

Соціальна інженерія – це метод керування діями індивіда без використання технічних засобів, що ґрунтується на використанні слабкостей людського фактора [2]. Найчастіше соціальну інженерію розглядають як незаконний

метод отримання інформації, тому сьогодні її активно використовують в інтернеті для отримання закритої інформації або інформації, що має велику цінність.

Стан дослідження. Проблематика профілактики та боротьби зі злочинністю в кіберпросторі досить часто розглядається фахівцями в наукових статтях, на конференціях і круглих столах, у засобах масової інформації. Деякі аспекти попередження кіберзлочинності вивчали у своїх працях такі відомі вчені, як С. Битко, В. Бутузов, О. Волеводз, Д. Дубов, Н. Дубова, С. Кльоцкін, М. Литвинов, В. Мілашев, В. Мохор, О. Орлов, В. Топчій, Т. Тропіна, В. Хахановський та інші. Однак не вирішених проблем на сьогодні ще досить багато, адже реалією нашого часу є факт стабільного прогресивного зростання кількості злочинів, що вчиняються в кіберпросторі.

Метою статті є дослідження й аналіз найбільш поширених алгоритмів злочинних дій у мережі Інтернет, з виокремлення проблем, що виникають під час профілактики та боротьби з кіберзлочинністю, та надання рекомендацій щодо протидії використанню різноманітних технік соціальної інженерії для здійснення шахрайських дій у мережі Інтернет.

Виклад основного матеріалу. ***Основні техніки соціальної інженерії, що використовуються для реалізації шахрайських схем.*** Згідно зі світовою статистикою, кількість хакерських атак із використанням методів соціальної інженерії неухильно зростає [3], у 2015 році під такі атаки потрапили 37 % фінансових установ світу [4]. Для підвищення ефективності захисту від характерних атак необхідно постійно досліджувати найпоширеніші види шахрайства, аналізувати дії зловмисників, а також вибудовувати відповідну систему безпеки.

Існує декілька поширених технік і видів атак, якими користуються соціальні інженери. Усі вони ґрунтуються на особливостях прийняття людиною рішень, відомих як когнітивні упередження. Ці забобони використовуються в різних комбінаціях з метою створення відповідної стратегії обману в кожному конкретному випадку. Спільною рисою всіх цих методів є введення в оману з метою змусити людину вчинити будь-яку дію, яка не вигідна їй, але потрібна соціальному інженерові. Для досягнення необхідного результату зловмисник використовує низку різноманітних тактик: видає себе за іншу особу, відвертає увагу, нагнічує психологічну напругу тощо. Кінцеві цілі обману також можуть бути дуже різними.

Соціальна інженерія є важливим аспектом у контексті роботи підприємства, установи чи організації, тому що системи захисту створюють для зловмисника бар'єр, який досить складно подолати без спеціальних знань і навичок. У цьому випадку неважливо, якого саме працівника вдалося ввести в оману зловмиснику, тому що результатом є доступ до всіх внутрішніх ресурсів з обминанням бар'єра захисту. Атаки за допомогою методів соціальної інженерії нерідко орієнтуються на працівників, які мають право доступу до конфіденційної інформації. Однією з важливих причин поширення соціальної інженерії як методу атаки є те, що це досить дешевий вид нападу, при цьому зловмисник може не бути фахівцем у сфері інформаційних технологій.

Соціальна інженерія – це метод несанкціонованого доступу до інформаційних ресурсів, що ґрунтується на особливостях психології людини. Головною метою соціальних інженерів, як і інших хакерів та зломщиків, є отримання доступу до захищених систем з метою крадіжки інформації, паролів, даних про кредитні картки тощо. Головною відмінністю від стандартної кібератаки є те, що в цьому випадку на роль об'єкта атаки вибирається не машина, а її оператор. Саме тому всі методи й техніки соціальних інженерів ґрунтуються на використанні слабкостей людського фактора. Зловмисник може отримати інформацію, наприклад, за допомогою звичайної телефонної розмови або шляхом проникнення в організацію під виглядом її співробітника.

Розглянемо відповідні техніки соціальної інженерії, що використовуються для здійснення відповідних злочинних дій, більш детально.

Фішинг – це схема, за якою хакери змушують користувачів передавати конфіденційну інформацію, наприклад, паролі та номери соціального страхування. Зазвичай вона передбачає надсилання користувачеві повідомлення, яке ніби походить із вартого довіри джерела, наприклад із банку (це наживка). У повідомленні міститься посилання на шахрайський web-сайт, що видається за варте довіри джерело (це пастка). Користувач спокійно вводить інформацію, яка цікавить хакерів, вважаючи, що перебуває на безпечному сайті [5]. На сьогодні це найпопулярніша схема соціальної інженерії. Жоден великий витік персональних даних не обходиться без хвилі фішингових розсилок, що йому передують. Опишемо декілька варіантів фішинг-атак.

«Фармінг (Pharming)». Замість того, щоб запрошувати користувача відвідати шахрайський

web-сайт, за допомогою цього методу користувач автоматично перенаправляється на фальшивий сайт.

«Списовий фішинг (Spear phishing)». Якщо звичайний фішинг передбачає надсилання мільйонів згенерованих повідомлень електронної пошти різним користувачам, то цілями списового фішингу є лише конкретні користувачі. Електронні листи, що використовуються для списового фішінгу, налаштовані на конкретних одержувачів із вказівкою на їх імена та особисту інформацію для того, щоб зробити повідомлення більш легітимними та правдоподібними. Оскільки кількість електронних листів, що використовуються в разі списового фішінгу, є значно меншою, ніж у звичайних фішинг-атаках, цей спосіб шахрайства важче виявити.

«Полювання на китів (Whaling)» – один із типів списового фішингу. Замість того, щоб домагатися «дрібних риб», «полювання на китів» орієнтується на «велику рибу», тобто на багатих людей, до банківських рахунків, яких зловмисник бажає отримати доступ. Зосередившись на цій невеликій групі, зловмисник може відвести більше часу на атаку й забезпечити чітке формування повідомлення, щоб досягти успіху з більшою ймовірністю.

Ще одним різновидом фішингу є так званий голосовий фішинг. Сутність його в тому, що зловмисник дзвонить жертві, яка, відповідаючи на дзвінок, чує записане повідомлення начебто з банку про те, що її кредитні картки використовуються в шахрайських схемах або банківський рахунок мав незвичайну активність. Жертві доручають негайно зателефонувати на відповідний номер (заздалегідь створений зловмисником). Коли вона дзвонить, їй на виклик відповідають і за допомогою автоматизованих інструкцій пропонують увести номер кредитної картки, номер банківського рахунку, номер соціального страхування або іншу інформацію за допомогою клавіатури телефона.

Протидіяти фішингу можна за допомогою навчання користувачів визначенню цих типів атак.

Розглянемо деякі ознаки фальшивих повідомлень.

Оманливі web-посилання. Посилання на web-сайт в електронному повідомленні не повинне містити знак «@» посеред адреси. Крім того, фішери полюбляють використовувати варіації справжньої адреси, наприклад, www.ebay_secure.com, www.e-bay.com або www.e-baynet.com. Не можна проходити авторизацію на web-сайті за посиланням у повідомленні електронної пошти, замість цього потрібно відкрити нове вікно браузера й увести справжню адресу.

Логотипи. Зловмисники часто використовують логотип виробника, намагаючись зробити електронний лист схожим на офіційне повідомлення і таким чином переконати одержувача, що повідомлення справжнє. Наявність логотипів не означає, що електронна пошта є законною.

Підроблена адреса відправника. Через те, що адресу відправника можна легко підробити, повідомленню електронної пошти не слід довіряти навіть тоді, коли вона здається коректною (наприклад, tech_support@ebay.com). Знак «@» в адресі відправника – це техніка, яка використовується, щоб приховати справжню адресу.

«Троянський кінь». Це шкідлива програма, що використовується зловмисником для збирання, видалення або модифікації інформації, порушення працездатності комп'ютера або використання ресурсів користувача у своїх цілях. Ця техніка часто експлуатує цікавість або інші емоції жертви. Найчастіше зловмисник відправляє жертві електронне повідомлення, що містить «цікавий» контент, оновлення антивірусу або іншу інформацію, здатну її зацікавити. Відкриваючи прикріплений до листа файл, жертва встановлює собі на комп'ютер шкідливе програмне забезпечення, що дозволяє зловмисникові одержати доступ до конфіденційної інформації.

«Дорожнє яблуко». Ця техніка є адаптацію «троянського коня» та полягає у використанні фізичних носіїв (CD-дисків, флеш-накопичувачів). Зловмисник зазвичай спеціально залишає такий носій у загальнодоступних місцях на території компанії (на парковці, в їдальні, на робочих місцях співробітників, у туалеті). Для того, щоб у працівника виникла цікавість до цього носія, зловмисник може нанести на носій логотип компанії та будь-який надпис, наприклад, «дані про продажі», «зарплата співробітників», «звіт у податкову» тощо.

«Зворотна соціальна інженерія». Цю технологію спрямовано на створення такої ситуації, за якої жертва змушена буде сама звернутися до зловмисника за «допомогою» [2]. Наприклад, зловмисник може надіслати лист із телефонами та контактами «служби підтримки» та через деякий час створити неполадки в комп'ютері жертви. Користувач у такому випадку телефонує або зв'язується за допомогою електронної пошти зі зловмисником, і в процесі «вирішення» проблеми зловмисник може отримати необхідні йому дані.

«Плечовий серфінг». Дає можливість отримати особисту інформацію від жертви шляхом

підглядання за діями користувача через його плече, зокрема спостереження за тим, як людина друкує на клавіатурі свого комп'ютера, щоб виявити й вкрасти її пароль або іншу призначену для користувача інформацію [6]. Цей тип атаки поширений у громадських місцях, таких як кафе, торговельні центри, аеропорти, вокзали, а також у громадському транспорті.

Останніми роками в мережі Інтернет дедалі частіше почали з'являтися сайти, головною функцією яких є негласний доступ до особистої інформації їх відвідувачів: до номерів платіжно-розрахункових карт і PIN-кодів до них, логінів і паролів, адресних книг, історій відвідувань і закладок у браузері, нещодавно збережених документів тощо. Автори таких сайтів-пасток використовують методи соціальної психології, зокрема метод заманювання відвідувачів різноманітними «вигідними» пропозиціями. Попри різноманітність, такі сайти об'єднує обіцянка безумовної вигоди за неадекватно низьких витрат. Принципи дії таких сайтів різний. Наприклад, користувач, працюючи в інтернеті, в разі переходу за посиланням або здійснивши клік «мишкою» по рекламному банеру потрапляє на сторінку, де спеціальна програма, користуючись уразливістю захисту операційної системи та (або) браузера, запускає завантаження програми-вірусу на комп'ютер жертви. Такий «комп'ютер-зомбі» може віддалено контролюватися хазяїном вірусу.

Використання методів соціальної інженерії для попередження злочинів у кіберпросторі. Сайти-пастки можуть також використовуватися для профілактики та боротьби з кіберзлочинністю. Обираються методи дій оперативних працівників залежно від поставлених цілей.

Розглянемо деякі методи роботи оперативних працівників.

Суттю методу *встановлення IP-адреси користувача та подальшого встановлення його особи* є створення сайту будь-якої тематики й виду з розміщенням на ньому програмного коду лічильника відвідувачів із можливістю фіксації IP-адреси та часу відвідування кожним користувачем мережі Інтернет. Стандартним лічильником фіксуються такі дані: IP-адреса комп'ютера користувача, точний час і дата відвідування сайту, деякі відомості про провайдера інтернет-послуг користувача, географічне положення комп'ютера користувача, тип підключення до інтернету, версія браузера (програми для перегляду інтернет-сторінок), версія операційної системи, установки розподільної здатності монітора тощо. Таким чином, зазначену інформацію лічильника відвідувань можна використовувати з метою з'ясування інформації за IP-адресою зловмисника за умови, що він був відвідувачем сторінки, на якій заздалегідь був установлений такий лічильник.

Для реалізації такого методу оперативному працівникові необхідно виконати такі дії: створити шаблон web-сторінки, встановивши на ньому код лічильника, і розмістити цей шаблон в інтернеті; надіслати зловмисникові послання (лист, посилання під час чату тощо) на цю сторінку з пропозицією її переглянути; перевірити статистику відвідувань створеної сторінки з лічильником на сайті з метою встановлення інформації про його IP-адресу; встановити провайдера інтернет-послуг, до мережі якого належить IP-адреса; встановити місцезнаходження комп'ютера, що входив у кіберпростір в указаний час під встановленою IP-адресою. Цей метод виявиться дієвим для встановлення особи, автора анонімних повідомлень злочинного характеру на інтернет-ресурсах, наприклад, оголошень про надання послуг або товарів, заборонених законом.

Наступним методом є *залучення потенційних злочинців до спілкування на спеціально створеному тематичному ресурсі* з метою отримання від них оперативної інформації. Такий метод на практиці можна реалізувати кількома способами: створенням і розвитком інтернет-ресурсу подібного до Dark Market і (або) впровадженням (вербуванням) одного з активних учасників із правами адміністратора порталу.

Метод *дослідження актуальних методик хакерських атак* більше торкається фахівців безпеки інтернет-ресурсів і захисту інформації, оскільки в переважній більшості випадків має дослідницький характер. Суть методу полягає у створенні локальної мережі-приманки, тобто одного з різновидів пастки. Наживкою виступає захищений ресурс, призначення якого – виступати об'єктом зондування атак і зломів з боку хакерів. Із цією метою створюється сайт, на якому не ведеться жодна змістовна діяльність, тобто він не використовується. Це означає, що, якщо кимось в таку пастку передається пакет даних або хтось робить спробу отримати доступ до ресурсу, то, скоріше за все, ці дії є зондуванням, скануванням або атакою. Замість того, щоб генерувати, наприклад, 10 тис. повідомлень на день, як це відбувається в робочих мережах, пастка може генерувати всього лише п'ять або десять таких повідомлень, більшість з яких буде повідомленнями про реальні спроби зондування або атаки.

Незважаючи на те, що сфера застосування таких пасток є досить обмеженою (вони здатні відстежувати лише ті атаки, які спрямовані безпосередньо на пастку), з їх допомогою можна досягти ефективнішого використання вже наявної архітектури системи захисту. Головне призначення таких ресурсів – стати об'єктом атак хакерів. Після кожного зареєстрованого факту атаки зібрана інформація ретельно аналізується.

Таким чином, не зважаючи на сформовану громадську думку про фішинг і соціальну інженерію як методи злочинної діяльності, вони можуть і мають використовуватися, насамперед, для профілактики та боротьби зі злочинністю в інтернеті. Безумовно, їх застосування, як і застосування будь-яких оперативно-розшукових заходів, вимагає попереднього узгодження всіх юридичних аспектів.

Слід зауважити, що сьогодні основним способом захисту від методів соціальної інженерії є здійснення профілактичних заходів, що полягають у навчанні громадян і працівників підприємств, установ та організацій. Користувальницькі облікові дані є власністю компанії (підприємства, установи, організації). Усім працівникам у день прийому на роботу потрібно пояснювати, що логіни і паролі, які вони отримали, не можна використовувати з іншого метою (на сторонніх web-сайтах, для особистої пошти тощо), передавати третім особам або іншим працівникам компанії, які не мають на них права. Наприклад, дуже часто працівник, ідучи у відпустку, передає свої авторизаційні дані своєму колезі для того, щоб той зміг виконати деяку роботу або подивитися певні дані під час його відсутності.

Необхідно проводити вступні та регулярні навчання працівників компанії, спрямовані на підвищення знань з інформаційної безпеки. Такі інструктажі дозволять працівникам мати актуальні дані про сучасні методи соціальної інженерії, а також не забувати головні правила з інформаційної безпеки. Обов'язковою є наявність регламентів з безпеки та інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії працівників у разі виникнення тієї чи іншої ситуації. Наприклад, у регламенті можна прописати, що необхідно робити і до кого звертатися в разі спроби третьої особи запросити конфіденційну інформацію або облікові дані співробітників. Такі дії дозволять швидше визначити зловмисника й не допустити витоку інформації.

Також комп'ютерах працівників завжди повинні бути встановлені актуальне антивірусне програмне забезпечення та брандмауер. У корпоративній мережі компанії необхідно використовувати системи виявлення та запобігання атак, а також системи запобігання витокам конфіденційної інформації. Усе це дозволить знизити ризик виникнення фішингових атак.

Необхідно максимально обмежити права користувача в системі. Наприклад, можна обмежити доступ до web-сайтів і заборонити використовувати з'ємні носії інформації, адже, якщо працівник не зможе потрапити на фішинговий сайт або використати на комп'ютері флешнакопичувач із «троянською програмою», то і втратити особисті дані він також не зможе.

Виходячи з викладеного, можна зробити **висновок,** що протидія кіберзлочинності – це важлива складова захисту національних інтересів держави. Кіберзлочинність уже стала великою проблемою для всього світу, яка потребує негайного вирішення. Правоохоронні органи намагаються перебувати на передньому рубежі боротьби з цими злочинами: формуються спеціальні підрозділи з боротьби з кіберзлочинністю, законодавці ухвалюють нові закони, банківські та фінансові установи в межах своєї компетенції проводять профілактичну роботу з населенням, надаючи відповідні рекомендації для безпечного використання можливостей мережі Інтернет. Однак втрати громадян і збитки держави й приватного сектора від протиправних дій інтернет-шахраїв постійно зростають.

Кіберзлочин, як і будь-який інший злочин, є не лише правовою, й соціальною проблемою. Необхідно створити уніфіковану класифікацію та формальну модель кіберзлочинів, які полегшать і протидію кіберзлочинності, і розслідування кіберзлочинів. Організація системи забезпечення безпеки інформації повинна мати комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків.

Основним способом захисту від методів соціальної інженерії є навчання працівників. Усі працівники компанії мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також про способи запобігання витоку даних.

Список бібліографічних посилань

1. Орлов О. В., Онищенко Ю. М. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління*. 2014. Вип. 1 (44). С. 9–15.

2. Соціальна інженерія // Вікі-знання/Тернопіл. нац. техн. ун-т ім. Івана Пулюя. URL: http://wiki.tstu.edu.ua/Соціальна_інженерія (дата звернення: 10.11.2016).

3. The Social Engineering Infographic // Security trough Education: a free learning resourse/Social-Engineer, Inc. Apr. 28, 2014. URL: http://www.social-engineer.org/social-engineering/social-engineering-infographic/ (дата звернення: 10.11.2016).

4. Gunn J. Social Engineering and How to Win the Battle for Trust // VASCO: blog. Nov. 5, 2015. URL: http://blog.vasco.com/electronic-signature/social-engineering-win-battle-trust-infographic/ (дата звернення: 31.10.2016).

5. Що таке фішинг? // GoDaddy: сайт. URL: https://ua.godaddy.com/help/sho-take-fishing-346 (дата звернення: 10.11.2016).

6. Плечовий серфінг. URL: http://um.co.ua/4/4-5/4-57341.html (дата звернення: 10.11.2016).

Надійшла до редколегії 27.01.2017

ОНИЩЕНКО Ю. Н., ПЕТРОВ К. Э., КОБЗЕВ И. В. ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПОМОЩЬЮ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ИНТЕРНЕТЕ

Исследованы наиболее распространённые алгоритмы преступных действий в сети Интернет и определены проблемы, возникающие при профилактике и борьбе с киберпреступностью. Сформулированы предложения по противодействию использованию различных техник социальной инженерии для осуществления мошенических действий в сети Интернет.

Ключевые слова: *киберпреступность, социальная инженерия, хакеры, интернет-ресурс, фишинг, web-сайт.*

ONYSHCHENKO Yu. N., PETROV K. E., KOBZEV I. V. COUNTERACTION CRIMES COMMITTED BY THE METHODS OF SOCIAL ENGINEERING IN THE INTERNET

The authors have studied the concept of «social engineering», methods and techniques of social engineering, which are used for committing criminal activities in the Internet: Voice phishing, Pharming, Spear phishing, Whaling and others. The authors have determined the main features of the false messages, which are necessary for early detection of phishing attacks like: fake Web-links, logos, sender's addresses of phishing messages. The authors have also considered techniques for obtaining illegal information online, which are used by cybercriminals like: «Trojan Horse», «The road apple», «Reverse social engineering», «shoulder surfing».

Based on the conducted research of the most spread algorithms of criminal acts in the Internet the authors have formulated some recommendations for the protection from social engineering techniques, primarily associated with training employees of companies, institutions, organizations and also ordinary citizens. The problems arising in the prevention and fighting against cybercrime have been defined; propositions (kinds of algorithms of the law enforcement employees' actions) on using the techniques of social engineering to combat fraud in the Internet have been formulated in the paper. Contrary to the formed public opinion about phishing and social engineering as methods of criminal activity, they can and should be used primarily for the prevention and the fight against crime in the Internet.

Keywords: *cybercrime, social engineering, hackers, online-resource, phishing, web-site.*

УДК 343.971

Ю. В. ОРЛОВ,
доктор юридичних наук, доцент,
доцент кафедри кримінального права і кримінології факультету № 1 (слідства)
Харківського національного університету внутрішніх справ;
ORCID: http://orcid.org/0000-0003-1981-0794

КРИМІНОЛОГІЧНИЙ АНАЛІЗ ПРОЕКТУ ЗАКОНУ УКРАЇНИ «ПРО ПЕНІТЕНЦІАРНУ СИСТЕМУ»

У процесі кримінологічному аналізу положень проекту закону України «Про пенітенціарну систему» виявлено дві групи його недоліків – концептуального і техніко-юридичного характеру, надано їх опис та обґрунтування. Визначено шляхи вдосконалення законопроекту через усунення виявлених недоліків. Запропоновано закріпити в цьому законопроекті поняття пенітенціарної системи, під якою можливо розуміти цілісну, керовану систему державних органів та установ, що забезпечують формування і реалізацію державної політики у сфері виконання покарань, здійснення пробації.

Ключові слова: *законопроект, пенітенціарна система, кримінологічна ефективність, кримінологічне моделювання, оперативно-розшукова діяльність, досудове розслідування, системно-правові зв'язки, пенітенціарна послуга.*