позапроцесуальних (у порядку оперативно-розшукової діяльності) формах. Досудове слідство здійснюють: слідчі підрозділи (органів Національної поліції, органів безпеки, органів Державного бюро розслідувань); підрозділ детективів, підрозділ внутрішнього контролю Національного антикорупційного бюро України; підрозділи детективів органів Бюро економічної безпеки України.

Отже, організаційне забезпечення правоохоронної діяльності має істотні особливості, чим і пояснюється існування правозахисних та інших структур державних органів, створення правових можливостей для реального та ефективного досягнення мети правоохоронної діяльності – охорони прав людини і громадянина, забезпечення інтересів суспільства і держави, підтримання правопорядку.

Література

1. Ковалів М.В., Єсімов С.С., Лозинський Ю.Р. Правове регулювання правоохоронної діяльності: навч. посіб. Львів: ЛьвДУВС, 2018. 323 с.

2. Судові та правоохоронні органи України: навч.-методич. матеріали. URL: https://arm.naiau.kiev.ua/books/spou_2019/info/lec1.html

УДК 343.9(043.2)

Грекова Л.Ю., асистент,
Національний авіаційний університет, м. Київ, Україна
Греков О.І., Data Management Associate,
J.P. Morgan Poland, Warsaw

КІБЕРЕТИКА ТА УПРАВЛІННЯ ДОСТУПОМ: ПОТЕНЦІЙНІ РИЗИКИ ДЛЯ ЗЛОЧИННИХ ДІЙ В КОРПОРАЦІЇ

Сучасний світ є реальністю комп’ютерних інформаційних технологій, які торкнулися всіх організацій та установ різноманітних галузей людської діяльності. Це призвело до заміни складних операцій, які виконували люди, функціями комп’ютерних систем. Такі перетворення у суспільстві суттєво вплинули на фундаментальні людські цінності, - мораль, політику, соціальну теорію, психологію тощо.

У сфері інформаційних технологій виникли нові етичні проблеми, які потребують безумовного втілення нових етичних стандартів, розробкою яких займається киберетика, яка є складовою забезпечення збалансованості правових та морально-етичних основ регулювання взаємовідносин між комп’ютером та людиною в мережевому просторі [1].

Разом із зручностями від використання комп’ютерних технологій виникають ризики втрати важливої інформації, активного зростання злочинної діяльності, що у значній кількості випадків пов’язані з порушеннями правил комп’ютерної етики.

Для прикладу, використання стандартів кіберетики (КЕ) у банківській сфері схоже на аналогічні дії в будь якій іншій галузі, оскільки кіберетика регулює правила (які є універсальними для всіх галузей) користування інформаційними системами в організаціях. Відрізняє КЕ у фінансових організаціях те, що вірогідним предметом злочинного посягання в таких установах є фінансові продукти, що створює привабливість для потенційного порушення очікуваних поведінкових норм, оскільки неправомірна поведінка може призвести до можливих фінансових вигод навіть більшою мірою, ніж у будь-якій іншій організації.

Одним із наріжних каменів безпеки Банку є управління доступом, що визначає, які користувачі мають відповідний доступ до конкретної програми, додатків або процесів, а також основні дії, на які вони мають право в межах своєї компетенції.

Такими типовими правами є:

– читання – користувач може переглядати та отримувати дані тільки для певних цілей;

– запис – користувач має право створювати записи та, можливо, змінювати дані в додатку. Цей доступ пов’язаний із вищим ризиком, оскільки записами можна маніпулювати в джерелі;

– адміністрування – користувачеві надається повний контроль над програмою з доступом до кожного модуля та можливістю надавати та відкликати доступ іншим користувачам.

Ці права підлягають регулярному перегляду в сенсі мінімізації доступу зазначених вище користувачів до тієї частини інформації, до якої вони у межах своїх службових повноважень не мають доступу.

Тим не менш, є часті випадки, коли співробітники корпорації або втратили свій доступ, або в процесі його оновлення через терміновість або тиск, повинні отримати доступ до необхідного додатку або програми негайно. У таких обставинах те, що найчастіше відбувається, практикується і порушує багато стандартів, - це використання облікових даних іншої особи (наприклад, колеги, яка може бути у відпустці) для швидкого та безпроблемного виконання бізнес-запиту. Однак потрібно розуміти, що з точки зору програми все, що відбувається з такого моменту, записується на особистість відсутнього користувача. Якщо переказ був зроблений за неправильним рахунком, або була заброньована угода з невірним клієнтом, або угода була здійснена з високим ризиком - кожна дія буде зареєстрована, від імені особи, яка була відсутня. Отже, всі можливі негативні наслідки з високою вірогідністю лягатимуть на непоінформованого працівника, включаючи фінансові втрати, штраф або навіть кримінальну відповідальність.

Таким чином, управління доступом є ключовим елементом ІТ-системи банкової або іншої корпорації, яке забезпечує етичне та безпроблемне виконання щоденних завдань і гарантує, що у відповідного персоналу

(тобто навченого персоналу, що мають досвід у тому різновиді бізнес процесів, у яких вони беруть участь) є відповідний доступ до додатку або процесів. Одночасно, управління доступом є і слабкою ланкою, тому що зазвичай отримання доступу – це бюрократичний і тривалий процес, який може перешкоджати швидкому вирішенню поставлених щоденних завдань у встановлений термін. Саме з цієї причини є привабливим обійти бюрократичну процедуру, порушити етичні норми і зробити все можливе задля забезпечення поставлених завдань у галузі, яка керує найважливішим людським ресурсом – грошима.

Література

1. Вікіпедія: Комп'ютерна етика. URL: https://uk.wikipedia.org/wiki/ %D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B5%D1%82%D0%B8%D0%BA%D0%B0 (дата звернення 18.12.2021).

УДК 343.9(043.2)

Гусар Л.В., к.ю.н.,
Чернівецький національний університет ім. Юрія Федьковича,
м. Чернівці, Україна

ДОТРИМАННЯ ПРАВ УВ'ЯЗНЕНИХ В ПЕРІОД ПАНДЕМІЇ

Рада Європи закликала країни-члени організації дотримуватися прав ув'язнених під час пандемії коронавірусу. Про це йдеться у заяві Європейського комітету щодо попередження тортур. Як наголошують експерти, для тих, хто перебуває у місцях позбавлення волі, епідемія може становити особливу небезпеку. На думку представників організації, пандемія коронавірусу поставила перед країнами надзвичайні виклики. «Захисні заходи (для боротьби з коронавірусом) у жодному разі не повинні призводити до нелюдського поводження з особами, позбавленими волі», – зазначає Рада Європи.

Комітет із запобігання катуванням представив зведення принципів поводження з ув'язненими, яким повинні слідувати держави в період пандемії коронавірусу. Влада повинна по можливості пом'якшити вироки, призначені судом, і віддати перевагу УДЗ та іншим альтернативам реальному позбавленню волі. Рада Європи також закликала затримувати мігрантів лише у крайньому випадку.

Мізерні дані про хворих на COVID-19 в пенітенціарній системі не повинні вводити в оману, скоріше за все, хворих значно більше, проте це не виявлено. Тестування в'язнів не передбачено взагалі. Ув'язнених тестують ще до потрапляння в СІЗО. Моніторинг виправних колоній показує, що у багатьох з них, медичні частини забиті засудженими, яких