УДК 65.012.8

Манжай О.В.
к.ю.н., доцент, доцент кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ
Манжай І.А.
викладач кафедри фінансів, обліку і аудиту Харківського економіко-правового університету

Аналіз нормативно-методичної урегульованості питання протидії несанкціонованому проникненню на об'єкти інформаційної діяльності

Анотація: в статті досліджено роль охоронної сигналізації та замків у побудові системи захисту інформації, проаналізовано нормативно-правову базу у сфері використання замків та охоронної сигналізації, надано класифікацію замків за різним критеріями, запропоновано правила використання замків та охоронної сигналізації на об'єктах інформаційної діяльності, надано рекомендації щодо встановлення замків та охоронної сигналізації на різних класах об'єктів.

Ключові слова: система захисту інформації, об'єкт інформаційної діяльності, нормативно-правова база, замки, охоронна сигналізація.

Аннотация: в статье исследована роль замков и охранной сигнализации в построении системы защиты информации, проанализирована нормативно-правовая база в сфере использования замков и охранной сигнализации, дана классификация замков по разным критериям, предложены правила использования замков и охранной сигнализации на объектах информационной деятельности, даны рекомендации по установлению замков и охранной сигнализации на разных классах объектов.

Ключевые слова: система защиты информации, объект информационной деятельности, нормативно-правовая база, замки, охранная сигнализация.

Summary: In the article analysed the role of locks and intruder alarm in the information security system is probed, a legislation is analysed in the

field of the locks and intruder alarm use, classification of locks is given on different criteria, the rules of the use of locks and intruder alarm are offered on the objects of information activity, recommendations on locks and intruder alarm installation on the different classes of objects are proposed.

Keywords: information security system, object of information activity, legislation, locks, intruder alarm.

Постановка проблеми. Останніми роками в Україні спостерігається підвищення уваги з боку державних органів до формалізації процесу побудови системи захисту інформації (СЗІ) на об'єктах інформаційної діяльності. Під час практичного вирішення завдання побудови СЗІ нерідко доводиться стикатися з проблемою нормативної невирішеності окремих питань. Зокрема, як співвідносяться між собою система технічного захисту та система технічної охорони (СТО) об'єкту, які вимоги висуваються до сигналізації охоронюваних приміщень та їх обладнання замковими пристроями в рамках побудови СТО та комплексної системи захисту інформації або комплексу технічного захисту інформації тощо?

Окремим важливим аспектом побудови системи захисту інформації на об'єкті інформаційної діяльності (ОІД) є правильний вибір та встановлення запірних пристроїв, зокрема, замків. При цьому, якщо питання використання замків для охорони матеріальних цінностей та обмеження свободи пересування певних категорій осіб вже досить давно та ґрунтовно досліджено, то обладнання замками об'єктів інформаційної діяльності залишається поза увагою більшості науковців у сфері інформаційної безпеки або згадується мимохіть. У чинній нормативно-правовій базі з питань захисту інформації цьому питанню приділено мало уваги, хоча проблема є досить актуальною, особливо в умовах масового доступу через Інтернет до маніпуляційних технік відмикання замків.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Нормативно-методичні питання обладнання об'єктів охоронною сигналізацією та замковими пристроями здебільшого розглядаються науковцями і практиками у сфері захисту інформації та спеціальної техніки. Причому, у досліджуваному контексті можна виділити праці С.С. Єпіфанова, С.М. Кльонова, М.К. Коровіна, В.В. Кулабухова, В.В. Попова, І.Ф. Хараберюша тощо.

Вивчення нормативно-правових актів у сфері захисту інформації та технічної охорони об'єктів засвідчило, що питанню вибору та поводження із охоронною сигналізацією та замковими пристроями відведе-

но другорядну роль у більшості з них. Найбільшу кількість нормативних документів, у яких хоча б опосередковано згадується вимога щодо обладнання об'єктів охоронною сигналізацією та замковими пристроями, створено за участю Міністерства внутрішніх справ. Причому, як правило мова йде про обмеження пересування осіб або охорону майна. Охороні за допомогою замків та сигналізації об'єктів інформаційної діяльності уваги приділено вкрай мало і здебільшого мова йде про банківські установи [1–7]. Вказані джерела є лише частиною проаналізованої нормативно-правової бази з досліджуваного питання, проте навіть в них можна побачити, що у нормативних документах багато уваги приділяється конструктивним особливостям охоронюваних приміщень, але аж ніяк не вимогам до встановлюваної сигналізації та видам використовуваних замків та їх розміщенню.

Виходячи з наведеного, вважаємо за необхідне розробити нормативний документ щодо оснащення об'єктів інформаційної діяльності сигналізацією та замковими пристроями і поводження з ними та внести належні зміни бланкетного характеру до нормативних документів у сфері захисту інформації.

Метою статті є дослідження проблем обладнання об'єктів інформаційної діяльності охоронною сигналізацією, відповідними замками та процедури поводження з вказаними пристроями.

Виклад основного матеріалу дослідження. Питання нормативного врегулювання СТО об'єктів інформаційної діяльності є вельми актуальним при побудові СЗІ, адже під час побудови СТО об'єкта інформаційної діяльності необхідно пройти по суті такі ж етапи, що і при побудові системи технічного захисту інформації [8, п. 3.7]. Так, при складанні окремої моделі загроз необхідно враховувати багато аспектів. Зокрема треба звернути особливу увагу на можливість подолання штатних технічних засобів охорони. Найбільш вразливими елементами сучасних охоронних систем є шлейфи сигналізації (дроти, кабелі) та охоронні датчики.

Для боротьби з загрозами такого типу при створенні СТО необхідно передбачати унеможливлення доступу потенційного порушника до шлейфів та датчиків охоронної сигналізації без спрацювання самої сигналізації, наприклад, застосуванням максимальної кількості пасивних оптичних датчиків руху. Тобто забезпечити деяке резервування системи за рахунок введення надмірності [9].

Для ефективної побудови СТО необхідно мати якісно складену окрему модель загроз, нормативні документи щодо створення якої на

даний час відсутні. Таким чином, вироблення вірних методик створення СТО інформації є одним з ключових при побудові системи захисту інформації в цілому. Адже фізичне проникнення зловмисника на об'єкт інформаційної діяльності фактично нівелює якщо не всю, то багато рубежів системи технічного захисту інформації об'єкту. В той же час доцільним є комплексне використання охоронних систем, зокрема проводової та безпроводової сигналізації (наприклад, на базі GSM/GPRS модему).

Ще одним елементом забезпечення безпеки ОІД є його обладнання належними замковими пристроями. Відповідно до ДСТУ Б А.1.1-74-2004 *виріб замковий* – це виріб, який призначений для запирання дверей, воріт тощо, і замикає (відмикає) об'єкт певним кодом (секретом). Носієм коду (секрету) можуть бути механічні, електронні та інші елементи [10, п. 3.1]. Несанкціоноване відмикання замка – це відмикання замка за допомогою сторонніх предметів без видимого пошкодження конструкції [10, п. 3.15]. Опірність замка несанкціонованому відмиканню – можливість замка протистояти несанкціонованому відмиканню протягом певного часу [10, п. 3.17].

Класифікацію замків можна представити, наприклад, як на рис. 1.

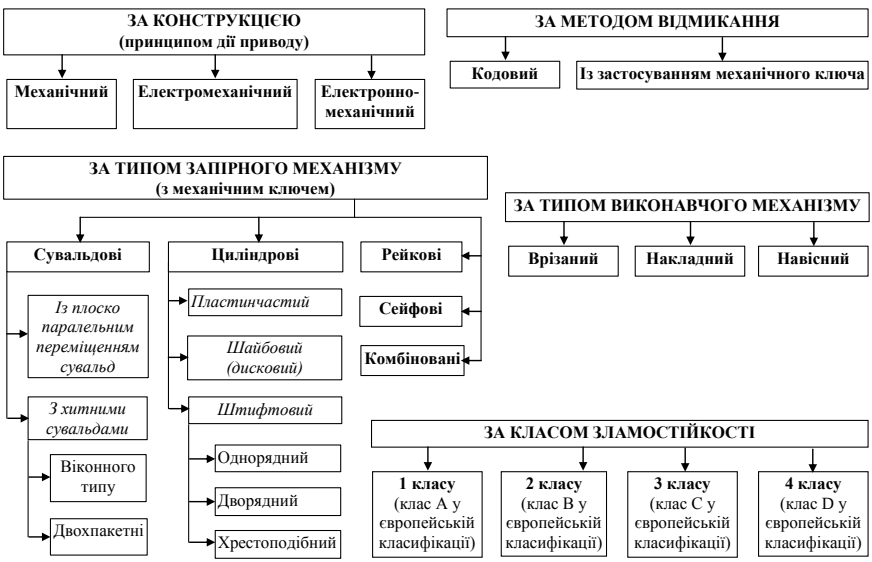

Рис. 1. **Класифікація замків**

Проаналізувавши нормативні документи Великобританії [11], Німеччини [12] та США [13] у сфері забезпечення безпеки ресурсів обмеженого доступу, можна окреслити структуру правил забезпечення безпеки замкових пристроїв на об'єктах інформаційної діяльності (далі Правила).

На нашу думку, Правила мають обов'язково містити наступні розділи:

1. **Загальні відомості,** у яких мають бути наведені класи та принцип дії сигналізації і замків, їх відповідність класу об'єкту інформаційної діяльності у залежності від важливості інформації, яка циркулює в його межах.

2. **Порядок надходження замків та сигналізації**. У цьому розділі мають міститися відомості про постачальників цього обладнання, забезпечення гарантій їх безпеки від неавторизованого доступу та гарантії зламостійкості.

3. **Настройка обладнання** міститиме відомості про порядок та місця зберігання настройок сигналізації та замків (їх зміни), вимоги до кодових комбінацій або ключів.

4. **Порядок встановлення та експлуатації обладнання.** Інформує персонал про кількість і якість сигналізації та замкових пристроїв для кожного об'єкту інформаційної діяльності, їх розташування на дверних полотнах (вікнах, приміщеннях) та вимоги до конструкцій дверей (вікон, приміщень), порядок видачі та зберігання ключів безпеки та їх опис.

5. **Захист від неавторизованого доступу.** Передбачає виклад інформації про виконання захисних дій для запобігання відомим технікам злому та подолання сигналізації та замкових пристроїв.

6. **Ремонт обладнання.** Містить відомості про порядок передачі замків і сигналізації до ремонтних майстерень та вимоги до таких установ.

7. **Дії у разі несправності та компрометації.** Окреслюється порядок дій персоналу на випадок несправності сигналізації та замків або їх компрометації, у тому числі випадки та процедура проведення службової перевірки по фактах компрометації такого обладнання або неавторизованого доступу до нього.

8. **Фінансування заміни обладнання.** Передбачає опис джерел фінансування заміни сигналізації та замків у випадках їх поломки або втрати ключів безпеки.

До першого розділу вказаних Правил пропонуємо включити таб-

лицю 1 з умовним розділенням приміщень на чотири рівні безпеки, наприклад, відповідно до існуючих категорій об'єктів. Це дозволить унормувати та формально закріпити неможливість встановлення «слабкої» сигналізації та замкових пристроїв на важливі ОІД.

Таблиця 1

Рекомендації по встановленню обладнання

Рівень безпеки приміщення	Рекомендоване обладнання	Рівень захисту ОІД
Перший рівень	Замки та сигналізації з високим рівнем безпеки, які мають високий ступінь стійкості до експертних та професійних атак, із застосуванням ексклюзивно розроблених методів та спеціалізованих засобів, недоступних у вільному обігу	Дуже високий
Другий рівень	Замки та сигналізації з середнім рівнем безпеки, які мають високий ступінь стійкості до експертних та професійних атак, із застосуванням методів та засобів, доступних у вільному обігу для спеціалістів по такому обладнанню	Високий
Третій рівень	Безпечні замки та сигналізації, які є стійкими до атак обізнаної особи, із мінімальними засобами	Середній
Четвертий рівень	Якісні замки та сигналізації з помірною стійкістю до неавторизованого відкриття та подолання	Низький

Висновки. Підсумовуючи наведене, слід зазначити, що жодне технічне обладнання не може надати стовідсоткову гарантію убезпечення об'єкту інформаційної діяльності від несанкціонованого проникнення, проте належне використання таких пристроїв за встановленими правилами з чітким дотриманням процедури дозволить максимально ускладнити процес неавторизованого доступу до ОІД, а відтак забезпечити певні гарантії збудованої системи захисту інформації.

Література:

1. Інструкція з організації охорони державних музеїв, історико-культурних заповідників, інших важливих об'єктів культури підрозділами Державної служби охорони при Міністерстві внутрішніх справ України, затверджена спільним наказом МВС України, Міністерства культури і мистецтв України від 30.07.2004 № 846/489 // Офіційний вісник України, 2004, № 34 (10.09.2004), ст. 2297.

2. Про затвердження Вимог до об'єктів і приміщень, призначених для здійснення діяльності з обігу наркотичних засобів, психотропних речовин, прекурсорів та зберігання вилучених з незаконного обігу таких засобів і речовин: наказ МВС

України від 28.08.2009 № 216 // Офіційний вісник України, 2009, № 63 (28.08.2009), ст. 2237.

3. Інструкція про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної і холодної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та зазначених патронів, а також боєприпасів до зброї та вибухових матеріалів, затверджена наказом МВС України від 21.08.1998 №622; [із змінами і доповненнями на 11.10.2011] // Офіційний вісник України, 1998, № 42 (05.11.1998), ст. 1574.

4. Інструкція про порядок організації охорони приміщень і територій відділень судово-психіатричної експертизи та режиму тримання осіб, які перебувають під вартою і направлені на судово-психіатричну експертизу, затверджена спільним наказом МВС та МОЗ України від 04.11.1996 №751/338 [Електронний ресурс] / Ліга: Закон Еліт: Мережна версія.

5. Про організацію діяльності чергових частин органів і підрозділів внутрішніх справ України, направленої на захист інтересів суспільства і держави від протиправних посягань: наказ МВС України від 28.04.2009 №181; [із змінами і доповненнями на 30.11.2011] // Офіційний вісник України, 2009, № 66 (07.09.2009), ст. 2303.

6. Про затвердження Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України: постанова Правління Національного банку України № 112 від 02.06.2007 // Офіційний вісник України, 2007, № 31 (07.05.2007), ст. 1250.

7. Положення про захист інформації в Національній системі масових електронних платежів: постанова Правління Національного банку України від 02.06.2008 № 119 // Законодавчі і нормативні акти з банківської діяльності, 2008. – 07 – № 7.

8. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38883&cat_id=38836.

9. Манжай О.В. Проблемні питання захисту інформації на об'єктах інформаційної діяльності / О.В. Манжай, В.П. Коваль, Ю.М. Онищенко // Системи обробки інформації / Безпека та захист інформації в інформаційних системах. – 2009. – Вип. 7 (79). – С. 69 – 73.

10. ДСТУ Б А.1.1-74-2004. ССНБ. Вироби замкові і скоб'яні. Терміни та визначення понять [Електронний ресурс]. – Режим доступу: http://info-build.com.ua/normativ/detail.php?ID=45811.

11. The Defence Manual of Security Vol. 1, 2 and 3 Issue 2. – October, 2001.

12. Instruction sheet on the Handling of Protectively Marked Information Classified VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED) [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=publicationFile.

13. Executive Order 13526 Classified National Security Information, December 29, 2009 [Електронний ресурс]. – Режим доступу: http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf.