УДК 65.012.8

О.В. Манжай

*Харківський національний університет внутрішніх справ, Харків*

# ВИКОРИСТАННЯ ЗАМКІВ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

*Досліджено роль замків у побудові системи захисту інформації, проаналізовано нормативно-правову базу у сфері використання замків, надано класифікацію замків за різним критеріями, запропоновано правила використання замків на об'єктах інформаційної діяльності, надано рекомендації щодо встановлення замків на різних класах об'єктів.*

***Ключові слова:*** *система захисту інформації, об'єкт інформаційної діяльності, нормативно-правова база, замки, класифікація замків, правила використання замків.*

## Вступ

**Постановка проблеми.** Важливим аспектом побудови системи захисту інформації на об'єкті інформаційної діяльності (ОІД) є правильний вибір та встановлення запірних пристроїв, зокрема, замків. Встановлення належних типів таких пристроїв є завданням не лише побудови системи технічної охорони об'єкту, але й системи захисту інформації. Таким чином, воно має комплексний характер і спрямоване на забезпечення технічної реалізації обмеження несанкціонованого доступу до об'єкту, особливо, коли мова йде про виділені або режимні приміщення.

Необхідно зауважити, що, 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 літератури.** Дослідження нормативно-правових актів у сфері захисту інформації та технічної охорони об'єктів засвідчив, що питанню вибору та поводження із замковими пристроями відведено другорядну роль у більшості з них.

Найбільшу кількість нормативних документів, у яких хоча б опосередковано згадується вимога щодо обладнання об'єктів замковими пристроями, створено за участю Міністерства внутрішніх справ. Причому, здебільшого мова йде про обмеження пересування осіб або охорону майна. Охороні за допомогою замків об'єктів інформаційної діяльності уваги приділено вкрай мало і здебільшого мова йде про банківські установи.

Наведемо декілька прикладів. Так, у [1, п. 3.4] вказується, що вхідні двері мають бути виготовлені за діючими стандартами, мати не менше *двох урізних замків* (що не замикаються самі) із встановленням їх на відстані не менше 300 мм між центрами ригелів … . З метою захисту двостулкових дверей можуть використовуватись спеціальні двосторонні шпінгалетні запори, що у разі замикання можуть фіксуватися *врізними або навісними замками* …Можуть бути використані металеві двері, виготовлені з кутника 40 мм х 40 мм х 4 мм за ГОСТ 8509 та листа металу товщиною не менше 2 мм, обладнані *двома внутрішніми замками*.

У [2, п. 2.1] зазначається, що вхідні двері сховищ повинні бути справні, добре підігнані під дверну коробку, металеві або дерев'яні повнотілі, товщиною не менше 40 мм, мати не менше *двох врізаних не самозамикальних замків*.

У [3, п. 11.5, 11.7] сказано, що відомча зброя, бойові припаси до неї, пристрої та зазначені патрони повинні зберігатися у спеціально обладнаному сховищі, яке повинно мати двоє дверей з міцними і *надійними замками* … Зовнішні двері повинні зачинятися на *два внутрішні замки* і опечатуватися або опломбовуватися. Внутрішні гратчасті двері зачиняються на *внутрішній або навісний замок* ... Допускається зберігання вогнепальної зброї у важких сейфах, які мають *внутрішні замки* …

У [4, п. 2.6] визначається, що *дверні замки* палат повинні бути накладними, тюремного типу і зачинятися на перший оберт автоматично, а потім – на два оберти ключем.

Двері кімнати для затриманих та доставлених обладнуються накладним замком «камерного типу» та двома металевими засувами, розташованими напроти петель дверей, повинні бути навішані з лівого боку відносно входу з таким розрахунком, щоб у відчиненому положенні їх неможливо було зняти з петель, та відчинятися у бік коридору. При замиканні дверей вручну замки повинні замикатися ключем на три оберти, а в разі автоматичного зачинення

дверей – автоматично на один оберт [5, п. 7.1.4]. Питанню обладнання об'єктів інформаційної діяльності ОІД присвячено низку нормативних документів Національного банку України.

Зокрема, організація зобов'язана розмістити автоматизоване робоче місце з програмними та апаратними засобами захисту інформації, яке призначене для роботи в системі електронних платежів у спеціально виділеному для цього приміщенні з обмеженим доступом, двері якого повинні бути оснащені *кодовим або автоматичним замком* і місцем для опечатування або системою доступу, яка забезпечуватиме персоніфіковану реєстрацію входу/виходу осіб у спеціальному електронному журналі [6, п. 3.2].

У вимогах до Центру ініціалізації та системної персоналізації карток вказується, що Приміщення повинно мати сейф з двома відділеннями, що закриваються на різні замки… [7, п. 4.4]

Наведені приклади є лише частиною проаналізованої нормативно-правової бази з досліджуваного питання, проте навіть в них можна побачити, що у нормативних документах багато уваги приділяється обладнанню дверей, грат, але аж ніяк не видам встановлюваних замків та їх розміщенню, таким чином, по суті *не забороняється встановлювати на важливі ОІД дешеві замки низького класу стійкості*, що суттєвим чином впливає на стан захищеності об'єкту.

Виходячи з наведеного, вважаємо за необхідне розробити нормативний документ щодо оснащення об'єктів інформаційної діяльності 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 відповідними замками та процедури поводження з вказаним пристроями.

## Основний матеріал дослідження

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 [8, п. 3.1].

Замок – виріб складений, як мінімум, із корпуса, запірного механізму, засува, планки запірної, ключа або іншого носія коду (секрету) і призначений для ідентифікації введеного носія коду (секрету) з запрограмованим кодом (секретом) замка, з метою розфіксування засува і введення (виведення) його в запірну планку або деталь, що її заміняє [8, п. 4.1].

Несанкціоноване відмикання замка – це відмикання замка за допомогою сторонніх предметів без видимого пошкодження конструкції [8, п. 3.15].

Опірність замка несанкціонованому відмиканню – можливість замка протистояти несанкціонованому відмиканню протягом певного часу [8, п. 3.17].

Класифікацію замків можна представити як на рис. 1.


Рис. 1. Класифікація замків

Під час проведених досліджень було виявлено, що кодові замки з поворотним тумблером є більш надійними, ніж замки з ключем, оскільки передбачають більш високий ступінь захисту до зломів. Наявність шпарини для ключа робить замки з механічним ключем вразливими до використання маніпуляційних технік, як-от класичне використання відмичок або бампінг, або, навіть, підбирання ключа.

Хоча кодові замки, зазвичай, вважаються більш надійними, проте і в них є певні вразливі місця, основними серед яких є такі:

1. Зняття **відбитків пальців** для встановлення коду. Для захисту від цього типу атак можна використовувати спеціальні маски для циферблату замка.

2. **Заміна внутрішніх частин** замка. Вказана вразливість з'являється, коли зловмисник має доступ до внутрішньої частини замка. Для запобігання такій вразливості слід одразу після отримання замка змінити настройки виробника, забезпечити обмеження кола осіб, які мають доступ до замка, на замках мають бути відсутніми позначки про їх внутрішню структуру, обслуговування замка має здійснюватися лише авторизованим персоналом, корпус замка має бути опломбовано.

3. **Рентгенографія**, полягає у використанні спеціального пристрою для з'ясування настройок коду шляхом вивчення рентгенівського зображення внутрішніх частин замкового пристрою. Захист від цього витонченого методу злому полягає у забезпеченні обмеження близького доступу осіб до основної частини замка, аж до просторового рознесення циферблату і решти блоків замка.

Проаналізувавши нормативні документи Великобританії [9], Німеччини [10] та США [11] 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 замків, відповідність кожного класу об'єкту інформаційної діяльності у залежності від важливості інформації, яка циркулює в його межах.

2. **Порядок надходження замків**. У цьому розділі мають міститися відомості про постачальників замків, забезпечення гарантій безпеки замків від неавторизованого доступу та гарантії зломостійкості.

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

4. **Порядок встановлення та експлуатації замків.** Інформує персонал про кількість і якість замкових пристроїв для кожного об'єкту інформаційної діяльності, їх розташування на дверних полотнах та вимоги до конструкцій дверей, 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 замкових пристроїв.

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

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

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

До першого розділу вказаних Правил пропонуємо включити таблицю 1 з умовним розділенням приміщень на чотири рівні безпеки, наприклад, відповідно до існуючих категорій об'єктів. Це дозволить унормувати та формально закріпити неможливість встановлення «слабких» замкових пристроїв на важливі ОІД.

Таблиця 1

Рекомендації по встановленню замків

| **Рівень безпеки приміщення** | **Рекомендовані замки** | **Рекомендовані додаткові методи і способи захисту** | **Рівень захисту ОІД** |
|---|---|---|---|
| Перший рівень | Замки 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 | Броньовані накладки, броньовані двері, штифтові накладки підвищеної секретності, накладки проти злому циліндра, камери спостереження, сигналізація, профілактика замка кожні 2 місяці | Дуже високий |
| Другий рівень | Замки 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 замках | Накладки проти злому циліндра, броньовані накладки, сигналізація, профілактика замка кожні 4 місяці | Високий |
| Третій рівень | Безпечні замки, які є стійкими до атак обізнаної особи, із мінімальними засобами | Накладки проти злому циліндра, невелика кількість додаткових ключів, профілактика замка кожні 6 місяців | Середній |
| Четвертий рівень | Якісні замки з помірною стійкістю до неавторизованого відкриття | Металева накладка. Додаткові способи на власний розсуд | Низький |

## Висновки

Підсумовуючи наведене слід зазначити, що жоден замок 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.

## Список літератури

*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 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.*

*9. The Defence Manual of Security Volumes 1, 2 and 3 Issue 2. – October, 2001.*

*10. 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/Shared Docs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=publicationFile.*

*11. Executive Order 12958 Classified National Security Information, April 20, 1995 (amended by Executive Order 13292 Further Amendment to Executive Order No. 12958, as Amended, Classified National Security Information of March 25, 2003).*

*Надійшла до редколегії 37.03.2012*

**Рецензент:** д-р техн. наук, доц. К.Е. Петров, Харківський національний університет внутрішніх справ, Харків.

### ИСПОЛЬЗОВАНИЕ ЗАМКОВ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

А.В. Манжай

*Исследована роль замков в построении системы защиты информации, проанализирована нормативно-правовая база в сфере использования замков, дана классификация замков по разным критериям, предложены правила использования замков на объектах информационной деятельности, даны рекомендации по установлению замков на разных классах объектов..*

***Ключевые слова:*** *система защиты информации, объект информационной деятельности, замки, классификация замков ,правила использования замков.*

### THE LOCKS USE IN INFORMATION ACTIVITY OBJECTS PROTECTION

O.V. Manzhai

*The role of locks in the information security system is probed, a legislation is analysed in the field of the locks use, classification of locks is given on different criteria, the rules of the use of locks are offered on the objects of information activity, recommendations on locks installation on the different classes of objects are proposed.*

***Keywords:*** *information security system, object of information activity, locks, classification of locks, locks using rules.*