УДК 004.0:056.00 DOI: 10.46972/2076-1546.2020.18.11

О. В. Самчишин, Д. В. Перевізна

АНАЛІЗ ВИДІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ТА ПЕРЕВАГИ АТРИБУТНОЇ ІДЕНТИФІКАЦІЇ ЗА QR-КОДОМ

Поява нових та модернізація сучасних інформаційних технологій, розвиток інформаційно-телекомунікаційних систем обробки та зберігання інформації зумовили необхідність зростання ефективності захисту інформації разом зі складністю архітектури зберігання даних. Захист інформації від несанкціонованого доступу є вкрай необхідним заходом для запобігання матеріального та нематеріального збитку її власника, тому дуже важливо досліджувати ефективність роботи підсистеми управління доступом та захисту даних задля збереження безпеки певної системи інформаційної інфраструктури.

Загроза витоку інформації зробила засоби забезпечення інформаційної та кібербезпеки однією із обов'язкових характеристик інформаційно-телекомунікаційних систем, а захист інформації став невід'ємною складовою професійної діяльності.

В умовах гібридної війни Російської Федерації проти України значно збільшилася кількість кібернетичних атак на інформаційно-телекомунікаційні системи військового призначення. Водночас зросла їх технологічна складність. Даний процес обумовлює необхідність удосконалення систем захисту інформації та процесу надання доступу до них з використанням сучасних видів ідентифікації користувачів.

Ефективним методом захисту інформації є управління доступом. Він регулює використання ресурсів інформаційних систем. Важливим та невід'ємним елементом системи управління доступом є ідентифікація користувачів.

У статті проаналізовано сучасні види ідентифікації користувачів. Розглянуто технологію QR-коду: принцип формування, види кодування, структуру елементів, переваги його використання. Встановлено взаємозв'язок між його складовими. Перспективою подальших досліджень є розроблення алгоритму та програмного додатка ідентифікації користувачів для надання доступу за QR-кодом в інформаційно-телекомунікаційні системи військового призначення.

Ключові слова: *інформаційно-телекомунікаційна система; доступ; користувач; атрибутна ідентифікація*; *QR-код.*

Постановка проблеми в загальному вигляді. В умовах тривалого геополітичного протистояння інформаційна політика Російської Федерації (РФ) набула агресивного характеру. Протягом періоду ведення гібридної війни РФ проти України було здійснено велику кількість кібернетичних атак на інформаційно-телекомунікаційні системи (ІТС) військового призначення, що обумовлює необхідність удосконалення систем захисту інформації та процесу надання доступу до них [1].

Аналіз останніх досліджень і публікацій. Питаннями дослідження, розробки та впровадження сучасних видів ідентифікації користувачів займається велике коло вчених, зокрема, В. Бурячок, В. Толубко, В. Хорошко, М. Грайворонський та багато інших

вітчизняних і зарубіжних науковців [1–4]. Але в даних роботах не розглянуто аспект використання атрибутної ідентифікації користувачів на основі використання QR-коду саме для ІТС військового призначення. Тому це питання потребує додаткового дослідження.

Формулювання завдання дослідження. Метою статті є детальний аналіз сучасних видів ідентифікації користувачів для надання доступу до ІТС та дослідження одного зі способів атрибутної ідентифікації – QR-коду, а саме розгляд принципу його технології, будови, виду кодування, способу та переваг використання.

Виклад основного матеріалу. Ідентифікація дозволяє суб'єктові (користувачу, процесу, який діє від імені певного користувача) повідомити своє ім'я за допомогою унікального параметра — ідентифікатора, який є відомим іншій стороні. Під час ідентифікації здійснюється порівняння заявленого суб'єктом параметра на відповідність відомому іншій стороні. У разі успішної ідентифікації відбувається автентифікація. У такий спосіб інша сторона переконується, що суб'єкт є саме тим, за кого себе видає. Наступним етапом є авторизація. Її суть полягає в наділенні користувача певними правами.

На сьогодні є декілька видів ідентифікації користувачів: парольна, атрибутна, біометрична. Кожна з них має свої переваги і недоліки, що визначає сферу їх використання [2].

Парольна ідентифікація. База даних користувачів парольної системи містить облікові записи всіх її користувачів. Під парольною системою розумітимемо програмно-апаратний комплекс, що реалізовує системи ідентифікації та автентифікації користувачів ІТС на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати низку додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів.

Парольна система є “переднім краєм оборони” всієї системи безпеки. Деякі її елементи (зокрема ті, що реалізують інтерфейс користувача) можуть бути розташовані в ділянках, відкритих для доступу потенційному зловмиснику. Тому парольна система стає одним із перших об'єктів атаки в разі вторгнення зловмисника в захищену систему [2].

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів у базі даних облікових записів. Можливі такі варіанти зберігання паролів:

у відкритому вигляді;

у вигляді згорток (хешування);

зашифрованими за деяким ключем.

Хешування (використання незворотної хеш-функції для будь-якої інформації перетворює її на унікальний код) не забезпечує захисту від підбору паролів за словником у разі отримання бази даних зловмисником. У ході вибору алгоритму хешування, який буде використано для розрахунку згорток паролів, необхідно гарантувати незбіг значень згорток, отриманих на основі різних паролів користувачів (відсутність колізій). Крім того, слід передбачити механізм, що забезпечує унікальність згорток у разі, якщо два користувачі обирають однакові паролі. Для шифрування паролів особливе значення має спосіб генерації та зберігання ключа шифрування в базі даних облікових записів. Перерахуємо деякі можливі варіанти:

ключ генерується програмно та зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження;

ключ генерується програмно та зберігається на зовнішньому носії, з якого він зчитується під час кожного запуску;

ключ генерується на основі обраного адміністратором пароля та вводиться в систему щоразу під час запуску.

Найбільш безпечне зберігання паролів забезпечується в разі їх хешування та подальшого шифрування отриманих згорток, тобто за комбінації другого і третього способів. Враховуючи, що користувачі нерідко обирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого мережею значення згортки пароля становлять серйозну загрозу безпеці парольної системи. У більшості випадків автентифікація відбувається в розподілених системах і пов'язана з передачею мережею інформації про параметри облікових записів користувачів. Якщо інформація, що передається мережею в процесі автентифікації, не захищена належним чином, то виникає загроза її перехоплення зловмисником і використання для порушення захисту парольної системи. Відомо, що багато комп'ютерних систем дозволяють програмно перемикати мережевий адаптер у режим прослуховування мережевого трафіка, адресованого іншим одержувачам у мережі, що ґрунтується на передачі пакетів даних.

Суть парольної ідентифікації зводиться до такого алгоритму: кожен зареєстрований користувач певної системи одержує набір персональних реквізитів (зазвичай використовуються пари логін-пароль). Далі щоразу для входу користувач повинен вказати ці реквізити. Оскільки пара логін-пароль унікальна для кожного користувача, то на її підставі відбувається його ідентифікація в системі.

Головна перевага парольної ідентифікації – це простота реалізації та використання. Крім того, вона не вимагає значних витрат: даний процес реалізований у всіх програмних продуктах, що є в продажу. Отже, система захисту інформації є гранично простою і доступною.

Її недоліком є значна залежність надійності ідентифікації від самих користувачів, тобто від обраних ними паролів. Це зумовлено тим, що більшість користувачів застосовують нестійкі ключові слова, які легко підбираються. До них належать занадто короткі паролі та ті, які складаються тільки з одного виду символів [3].

Атрибутна ідентифікація ґрунтується на визначенні особистості користувача за певним предметом, що перебуває в його персональному користуванні, – спеціальним електронним ключем. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння із собою. На даний момент найбільшого поширення набули два типи пристроїв. До першого належать так звані “токени”, що мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT). Іншим типом ключів, які можуть використовуватися для апаратної ідентифікації, є різноманітні ідентифікаційні карти.

Основною перевагою застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які зловмисникам не вдасться. Крім того, у них реалізовані різні варіанти захисних механізмів. Вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати інші корисні функції [4].

Недоліком апаратної ідентифікації є можливість втрати електронних ключів зареєстрованими користувачами. Під втратою розуміється викрадення, передача іншій особі, дублікат. Крім того, недоліком є також вартість. Для введення в експлуатацію системи атрибутної ідентифікації зареєстрованого користувача потрібно забезпечити ключем. Також згодом деякі типи ключів потребують заміни через зношеність, факт втрати тощо, тобто апаратна ідентифікація вимагає певних експлуатаційних витрат [5].

Біометрична ідентифікація. Біометрія − це ідентифікація людини за унікальними, властивими тільки їй, біологічними ознаками. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки як основу для ідентифікації користувача й ухвалення рішення про можливість доступу до ресурсів комп’ютерних систем.

Серед біометричних механізмів ідентифікації можна виділити такі:

за статичними ознаками – тими, які практично не змінюється з часом, починаючи з народження людини (фізіологічні характеристики);

за динамічними ознаками – поведінковими характеристиками, які ґрунтуються на особливостях, притаманних для підсвідомих рухів у процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів у завданнях ідентифікації користувача комп’ютерних систем використовуються такі:

ідентифікація за відбитком пальця: в основі цього методу лежить унікальність малюнка папілярних візерунків на пальцях. Ідентифікація побудована таким чином: за допомогою сканера одержують зображення відбитка, потім це зображення певним алгоритмом перетворюється на спеціальний цифровий код, який далі порівнюється з еталоном, що зберігається в базі даних;

ідентифікація за розташуванням вен на долоні: приладом, який зчитує інформацію в цьому разі, є інфрачервона камера. У результаті на вході програми для формування цифрового коду з'являється малюнок вен на руці. Не потребує контакту людини з пристроєм для сканування;

ідентифікація за сітківкою ока: сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. Зрозуміло, що цей малюнок спостерігається тільки за певних умов: для сканування людина дивиться на віддалене світлове джерело і спеціальна камера сканує її очне дно, що, у свою чергу, може викликати дискомфортні відчуття;

ідентифікація за райдужною оболонкою ока: малюнок райдужної оболонки ока – унікальний для кожної людини. Для застосування цього методу важлива не тільки спеціальна камера, а й надійне програмне забезпечення (ПЗ), адже саме за його допомогою із зображення виділяється малюнок потрібної райдужної оболонки;

ідентифікація за формою кисті руки: цей метод ґрунтується на розпізнаванні геометричних особливостей кінцівки. Спеціальний сканер формує тривимірний малюнок кисті, у ході його аналізу здійснюються вимірювання, за допомогою яких формується відповідний цифровий код;

ідентифікація за формою обличчя: на практиці використовують як двовимірне, так і тривимірне зображення, причому перше на сьогоднішній день є одним із найменш ефективних методів біометрії, тому має обмежене коло застосування або

використовується тільки в сукупності з іншими методами. Розпізнавання за тривимірним зображенням обличчя схоже на метод ідентифікації за формою кисті руки, оскільки так само будується тривимірний образ. Спеціалізоване ПЗ виділяє з цього образу контури очей, губ й інших частин обличчя. Далі проводяться точні вимірювання між заданими контурами. Саме за цими даними будується цифровий код.

Серед динамічних методів, які використовуються для біометричної ідентифікації особи користувача, можна назвати такі:

ідентифікація за голосом: на сьогодні є велика кількість подібних програм розпізнавання. У методі ідентифікації за голосом важливі його частотні характеристики, оскільки саме за ними будується цифрова модель;

ідентифікація за почерком: досліджується підпис людини. Перевіряються такі динамічні характеристики, як: графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. На основі цих характеристик будується цифровий код;

ідентифікація за клавіатурним почерком: даний метод аналогічний методу ідентифікації за почерком, але замість того, щоб нанести підпис, людині необхідно надрукувати кодове слово. Цифровий код будується за динамікою набору певного слова або фрази.

Попри все теоретичне різноманіття можливих біометричних методів, тих, що застосовуються на практиці, небагато. В основному використовуються розпізнавання за відбитком пальця, за зображенням особи (двомірним або тривимірним), за райдужною оболонкою та за сітківкою ока. Це обумовлено технічною складністю реалізації програмно-апаратних засобів.

Головна перевага біометричних технологій − висока надійність. Оскільки біометричні характеристики кожної людини індивідуальні, то ймовірність зламу системи з використанням біометричної ідентифікації суттєво знижується.

Основним недоліком біометричної ідентифікації є вартість устаткування. З підвищенням його ціни збільшується термін його використання, значно зменшується відсоток помилок іншого роду (наприклад, відмова в доступі зареєстрованому користувачеві).

Отже, було розглянуто три види однофакторної ідентифікації користувачів ІТС. Також на сьогодні набуває поширення комплексна або багатофакторна ідентифікація, коли для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів. Комбінуватися вони можуть у довільному порядку. Утім сьогодні в переважній більшості випадків використовується пара ідентифікаторів − парольний захист і токен. Це унеможливлює підбір пароля користувача зловмисником (без електронного ключа він працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Проте в деяких системах застосовуються процедури ідентифікації, у яких одночасно використовуються паролі, токени та біометричні характеристики людини [6].

Принципово новим та найменш поширеним в ІТС військового призначення є метод атрибутної ідентифікації користувачів на основі технології QR-коду.

QR-код – це різновид двомірного штрих-коду, у який закладається певний контент. Він складається з певного набору міток і пікселів, які становлять собою закодоване повідомлення, збережене в ньому.

Принцип використання QR-кодів полягає в тому, що роздрукований або в електронному вигляді код може бути зчитаний і розшифрований за допомогою пристрою, який має функціональну камеру і встановлене ПЗ для декодування.

Закодувати інформацію в QR-код можна кількома способами, вибір конкретного з них залежить від того, які символи використовуються. Якщо беруть лише цифри від 0 до 9, то можна застосувати цифрове кодування, якщо крім цифр необхідно зашифрувати букви латинського алфавіту, пробіл і спецсимволи, то використовується буквено-цифрове кодування. Ще відоме кодування кандзі, яке застосовують для шифрування китайських і японських ієрогліфів, а також побайтове кодування, коли перед кожним сеансом кодування створюється порожня послідовність біт, яка потім заповнюється.

Цифрове кодування вимагає 10 біт на 3 символи. Уся їх послідовність розбивається на групи по 3 цифри, кожна група (тризначне число) переводиться в 10-бітове двійкове число і додається до послідовності біт. Якщо загальна кількість символів не кратна 3, тобто в кінці залишається 2 символи, то отримане двозначне число кодується 7 бітами, а якщо 1 символ – 0–4 бітами.

Для *буквено-цифрового кодування* 2 символів потрібно 11 біт інформації. Послідовність символів розбивається на групи по 2, у групі кожен символ кодується згідно з таблицею ASCII. Значення першого символа множиться на 45, потім до цього добутку додається значення другого символа. Отримане число переводиться в 11-бітове двійкове число і додається до послідовності біт. Якщо в останній групі залишається один символ, то його значення кодується 6-бітовим числом.

Байтовим кодуванням можна закодувати будь-які символи. Їх вхідний потік кодується в будь-якому кодуванні (рекомендовано в UTF-8), переводиться в двійковий вигляд та об'єднується в один потік бітів.

В основі кодування ієрогліфів (як й інших символів) *кандзі* лежить візуально сприйнятна таблиця або список зображень ієрогліфів з їх кодами. Така таблиця називається “Character set”. Для японської мови основне значення мають дві таблиці символів: JIS 0208:1997 [7] і JIS 0212:1990 [8]. Друга з них є доповненням до першої. JIS 0208:1997 складається з 94 сторінок по 94 символи.

QR-код складається з певного набору міток і пікселів, які становлять собою закодоване повідомлення, збережене в QR-коді (рис. 1).

На будь-якому QR-коді обов'язково повинні бути 6 видів міток [9]:

позиціонування (область, необхідна для детектування коду);

номер версії (визначає, яка версія коду використовується (від 1 до 40));

синхронізація (дублюються у двох напрямках і дозволяють знизити ймовірність виникнення помилок у разі зчитування, системної інформації (наприклад, версія, тип даних тощо));

формат (необхідні для визначення типу даних, закодованих у коді);

вирівнювання (використовуються для кращого позиціонування коду під час обробки (для версії QR-коду вище 1));

рівень виправлення помилки (дозволяють визначити, який рівень перешкодозахищеності був використаний на етапі кодування для правильного вибору способу виявлення можливих помилок у коді).

Рис. 1. Будова QR-коду

Переваги використання QR-коду:

1) дозволяє кодувати більше інформації, ніж лінійні штрих-коди (порівняння об'єму даних, що можуть міститися в QR-коді та штрих-коді, наведено в табл. 1);

2) легко розпізнається сканувальним обладнанням (за допомогою структурних елементів, що містить QR-код, камера без ускладнень фокусується на ньому та відбувається декодування інформації, що в ньому міститься);

3) може бути зчитаний навіть у разі пошкоджень (QR-код має здатність відновлення інформації, що міститься в ньому, навіть якщо певна частина символів на зображенні QR-коду була пошкоджена або не розпізнана. Максимальна кількість кодових слів, що може бути відновлена, становить до 30%).

Таблиця 1

Порівняння об'єму даних у штрих-коді та QR-коді

Тип даних	**QR-код**	**Штрих-код**
Числові дані, символів	7089	1230
Символьні дані, символів	4296	70
Бінарна інформація, байт	2953	516

Дані переваги та новизна QR-коду як атрибута ідентифікації користувачів обумовлюють доцільність додаткового аналізу й досліджень, а також розробки алгоритму та ПЗ ідентифікації користувачів для надання доступу за QR-кодом в ІТС військового призначення.

Висновки. На основі аналізу сучасних методів ідентифікації користувачів було визначено, що на сьогодні найбільш поширеним є парольний захист, оскільки є найпростішим у реалізації. Його недолік полягає у великій кількості методів підбору паролів, що зумовлює високу вірогідність зламу систем парольної ідентифікації. Решта розглянутих видів ідентифікації користувачів також не в змозі в повному обсязі забезпечити захист інформації, цілком унеможлививши ризик несанкціонованого доступу, або мають високу вартість розробки та технологічну складність реалізації. Було досліджено технологію QR-кодів. Перспектива подальших досліджень полягає в розробленні алгоритму та програмного додатка ідентифікації користувачів для надання доступу за QR-кодом в ІТС військового призначення.

СПИСОК ЛІТЕРАТУРИ

1. Косогов О. М., Сірик А. О. Основні проблемні питання та напрямки підвищення ефективності державної інформаційної політики України в умовах гібридної війни. Київ : НУОУ ім. І. Черняховського, 2017. 104 с.
2. Інформаційна та кібербезпека: соціотехнічний аспект : навч. посіб. / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Київ : ДУТ, 2015. 288 с.
3. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій : навч. посіб. Харків : ХНУ ім. В. Н. Каразіна, 2013. 632 с.
4. Грайворонський М. В., Новіков О. М. Безпека інформаційно-телекомунікаційних систем : підруч. Київ : ВНУ, 2009. 608 с.
5. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29 березня 2006 р. (зі змінами) № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006 (дата звернення: 14.11.2020).
6. Самчишин О. В., Перевізна Д. В. Програмний додаток надання доступу на основі атрибутної ідентифікації // Тези доповідей ІІІ Всеукр. наук.-техн. конф. «Комп'ютерні технології: інновації, проблеми, рішення». Житомир : Житомирська політехніка, 2020. С. 11–13.
7. Таблиця символів: JIS 0212: 1990. URL: https://www.normadoc.com/english/jis-z-0212-1998-r2013.html (дата звернення: 16.11.2020).
8. Таблиця символів: JIS 0208: 1997. URL: https://www.normadoc.com/english/jis-x-0208-1997-r2007.html (дата звернення: 16.11.2020).
9. ISO/IEC 18004:2006. URL: https://www.iso.org/ru/standard/43655.html (дата звернення: 17.11.2020).

Подано 17.11.2020

REFERENCES

1. Kosohov, O. M., & Siryk, A. O. (2017). *Osnovni problemni pytannia ta napriamky pidvyshchennia efektyvnosti derzhavnoi informatsiinoi polityky Ukrainy v umovakh hibrydnoi viiny [The main problematic issues and directions of increasing the efficiency of the state information policy of Ukraine in the conditions of hybrid war]*. Kyiv: NDU of Ukraine named

after Ivan Cherniakhovskyi [in Ukrainian].
2. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and cybersecurity: socio-technical aspect]*. Kyiv: SUT [in Ukrainian].
3. Yesin, V. I., Kuznetsov, O. O., & Soroka, L. S. (2013). *Bezpeka informatsiinykh system i tekhnolohii [Security of information systems and technologies]*. Kharkiv: V. N. Karazin KhNU [in Ukrainian].
4. Hraivoronskyi, M. V., & Novikov, O. M. (2009). *Bezpeka informatsiino-telekomunikatsiinykh system [Security of information and telecommunication systems]*. Kyiv: VNU [in Ukrainian].
5. Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh : postanova Kabinetu Ministriv Ukrainy vid 29 bereznia 2006 r. (zi zminamy) № 373. [On approval of the Rules for ensuring information protection in information, telecommunication and information-telecommunication systems: Resolution of the Cabinet of Ministers of Ukraine from March 29, 2006 (as amended) № 373]. (2006). Retrieved from https://zakon.rada.gov.ua/laws/show/373-2006 [in Ukrainian].
6. Samchyshyn, O. V., & Perevizna, D. V. (2020). Prohramnyi dodatok nadannia dostupu na osnovi atrybutnoi identyfikatsii [Software application for providing access based on attribute identification]. In *Tezy dopovidei III Vseukr. nauk.-tekhn. konf. «Komp'iuterni tekhnolohii: innovatsii, problemy, rishennia» [Abstracts of reports III All-Ukrainian scientific and technical conf. "Computer technologies: innovations, problems, solutions"]*. (pp. 11–13). Zhytomyr: Zhytomyr Polytechnic State University [in Ukrainian].
7. Tablytsia symvoliv [Character table]: JIS 0212: 1990. (1990). Retrieved from https://www.normadoc.com/english/jis-z-0212-1998-r2013.html [in Ukrainian].
8. Tablytsia symvoliv [Character table]: JIS 0208: 1997. (1997). Retrieved from https://www.normadoc.com/english/jis-x-0208-1997-r2007.html [in Ukrainian].
9. ISO/IEC 18004:2006. (2006). Retrieved from https://www.iso.org/ru/standard/43655.html.

O. V. Samchyshyn, D. V. Perevizna

ANALYSIS OF TYPES OF USER'S IDENTIFICATION AND ADVANTAGES OF USER'S ATRIBUTE IDENTIFICATION BY QR-CODE

Emergence of new technologies and modernization of existing information technologies, development of information and telecommunication processing and storage systems have increase the level of information security, necessitating an increase of information security's effectiveness with the complexity of data storage architecture. Security of information from unauthorized access is an essential measure to prevent material and non-material damage to its owner. So it is very important to take into account the efficiency of the subsystem of access control and data security in order to ensure security of some information system.

Accordingly the threat of information leakage has made the means of information security and cyber security one of the mandatory characteristics of information and telecommunication systems and information security has become an integral part of professional function.

Under conditions of the hybrid war of the Russian Federation against Ukraine? the number of cyber attacks on military information and telecommunication systems has increased. At the

same time their technological complexity has increased too. This process necessitates the improvement of information security systems and the process of providing access to them by using modern types of users identification.

Access control is an effective method of information security. It regulates the use of information system resources. User's identification is an important and integral element of access control system.

An analysis of modern types of users identification is presented in the paper. The technology of QR-code is considered: the principle of formation, the types of coding, the structure of elements, the advantages of its usage. The interconnection between its components was established. Prospects for further research are the development of an algorithm and software application for user identification to provide access by QR-code to information and telecommunication systems for military purposes.

Keywords: *information and telecommunication system; access; user; attribute identification; QR-code.*