ПРОЕКТИРОВАНИЕ И ПРИМЕНЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056:004.057.2

ФУНКЦІОНАЛЬНІ ВИМОГИ АНАЛІЗУ ЗАХИЩЕНОСТІ ЕЛЕКТРОННИХ ПРОЇЗНИХ ДОКУМЕНТІВ

Ю.І. ГОРБЕНКО, Д.В. ПОВТАРЄВ, О.С. ТОЦЬКИЙ

Розглядаються задачі проведення комплексного аналізу механізмів та внесення рекомендацій щодо усунення недоліків та протидії загрозам безпеці інформації електронних проїзних документів.

Ключові слова: електронний паспорт, функціональні вимоги захищеності, додатковий контроль доступу (SAC), PACE, автентифікація.

ВСТУП

Одним з важливих напрямів досліджень, що пов'язаний з удосконаленням електронного біометричного паспорту особи та інших електронних документів, є аналіз їх захищеності від існуючих загроз. Механізми, що реалізуються в концепції електронного паспорту, можуть бути успішно реалізовані в різних сферах діяльності. Разом з тим, реалізація проекту впровадження електронних цифрових паспортів для використання в будь-якій сфері, зіштовхується з рядом проблемних питань, які поки що не вирішені в Україні. Першим з них є питання про те, як обрати необхідні параметри захисту так, щоб вони з одного боку забезпечували відповідний рівень захисту, а з іншого були економічно доцільними та прийнятними власниками таких паспортів. Тому визначення функціональних вимог аналізу якості національних електронних проїзних документів є нагальним завданням. Для цього доцільно провести аналіз міжнародних нормативних вимог та найбільш поширених зразків електронних паспортів. Об'єктом аналізу є безконтактна інтегральна схема машино читальних проїзних документів(чип МЧПД), запрограмована згідно з логічною структурою даних описаною в документі ICAO 9303 [1] та використовує механізми базового та розширеного контролю доступу, опис яких наведено в нормативному документі BSI TR-03110 [2]. Об'єкт аналізу включає в себе принаймні такі елементи

- схема чипа МЧПД(інтегральна схема),
- спеціалізоване програмне забезпечення інтегральної схеми, яке включає в себе спеціалізоване програмне забезпечення тестування і підтримки,
- вбудоване програмним забезпеченням інтегральної схеми(операційна система),
- додатки МЧПД,
- відповідні керівні документи.

Електронні проїзні документи мають ряд загроз, які описані та обґрунтовані в документі BSI-CC-PP-0056 [3] і від яких необхідно комплексно захистити користувачів цієї технології. До цих загроз відносяться:

- Читання даних чутливих біометричних посилань;
- Підробка даних на чипі МЧПД;
- Підробка чипу МЧПД;
- Зловживання функціональністю;
- Витік інформації з чипу МЧПД;
- Фізичні підробки;
- Несправність у зв'язку з дією оточуючого середовища.

Об'єкт оцінки повинен відповідати наступним правилам організаційної політики безпеки, яка регулює правила безпеки, процедури, керівні вказівки, які організують його діяльність:

- Виконання вимог профілю захисту базового контролю доступу;
- Захист чутливих біометричних даних посилань;
- Виконання вимог безпеки під час виготовлення чипа МЧПД;
- Виконання вимог безпеки під час процедури персоналізації, яку проводить виключно держава видачі чи відповідна організація.

Опишемо цілі безпеки для об'єкту оцінки, що звертають увагу на відомі загрози, для захисту від яких використовується об'єкт аналізу та організаційна політика безпека об'єкту аналізу.

1) OT.AC_Pers «Контроль доступом для персоналізації логічної MRTD»

Об'єкт оцінки повинен гарантувати, що логічні дані МЧПД в групах даних з EF.DG1 до EF.DG16, документ об'єкту безпеки у відповідності до логічної структури даних і дані TSF можуть бути записані виключно авторизованим агентом персоналізації. Логічні дані МЧПД в групах даних з EF.DG1 до EF.DG16 і дані TSF можуть бути записані лише протягом процесу персоналізації і не можуть бути змінені після закінчення цього процесу. Документ об'єкту безпеки може бути оновлений агентом персоналізації, якщо були додані дані в групи даних з EF.DG3 до

EF.DG16. OT.AC_Pers має на увазі, що дані груп логічної структури даних, що були записані протягом процесу персоналізації для власника МЧПД(хоча б EF.DG1 та EF.DG2) не можуть бути змінені за допомогою доступу з правом запису після персоналізації. Крім того, агент персоналізації може додавати(заповнювати) дані в ще не записані групи логічної структури даних та оновлювати та підписувати документ об'єкту безпеки. Підтримка у додаванні даних на фазі «Операційне використовування» не є обов'язковим.

2) OT.Data_Int «Цілісність персональних даних»

Об'єкт оцінки повинен гарантувати цілісність логічної складової МЧПД, яка зберігається у чипі МЧПД проти фізичних маніпуляцій і не авторизованого запису. Об'єкт оцінки повинен гарантувати цілісність логічних даних МЧПД під час їх передачі до системи перевірки після виконання протоколу автентифікації чипу.

3) OT.Sense_Data_Conf «Конфіденційність посилань на чутливі біометричні дані»

Об'єкт оцінки повинен гарантувати конфіденційність чутливих біометричних даних посилань (EF.DG3 та EF.DG4) шляхом надання доступу на читання тільки уповноваженим розширеним інспекційним системам. Авторизація інспекційної системи здійснюється на основі сертифікату інспекційної системи, який використовується для успішної автентифікації та повинен знаходитися у не строгій підмножині авторизації, що визначається сертифікатом сторони, яка перевіряє документ в ланцюжку сертифікатів до центру сертифікації країни, що проводить перевірку країни. Об'єкт оцінки повинен гарантувати конфіденційність логічних даних МЧПД під час їх передачі до розширеної системи перевірки. Конфіденційність чутливих біометричних даних посилань повинна бути захищена від атак з високим потенціалом.

4) OT.Identification «Ідентифікація і автентифікація об'єкту оцінки»

Об'єкт оцінки повинен забезпечувати засоби для зберігання даних ідентифікації інтегральної схеми та даних попередньої персоналізації в своїй енергонезалежній пам'яті. Дані ідентифікації інтегральної схеми повинні забезпечувати однозначну ідентифікацію інтегральної схеми під час фази 2 "Виробництво " і фази 3 "Персоналізація МЧПД". Зберігання даних попередньої персоналізації включає в себе запис ключа(-ів) агенту персоналізації.

5) OT.Chip_Auth_Proof «Доведення автентичності чипа MRTD»

Об'єкт оцінки повинен підтримувати загальні інспекційні системи для перевірки автентичності і достовірності чипу МЧПД, як такого, що є випущеним відповідною країною чи організацією. Це забезпечується за допомогою протоколу автентифікації чипу. Доказ автентичності, що надається чипом МЧПД, повинен бути захищеним від атак з високим потенціалом. OT.Chip_Auth_Proof має на увазі, що чип МЧПД має номер документа МЧПД в якості унікального ідентифікатора; знання таємниці, щоб ідентифікувати себе, наприклад, закритого ключ автентифікації в якості даних TSF. Об'єкт оцінки повинен захистити ці дані TSF для запобігання їх неправильного використання. Термінал повинен мати довідкові дані для перевірки автентичності спроба чипа МЧПД, наприклад, це може бути сертифікат для відкритого ключа протоколу автентифікації чипа, який відповідає закритому ключу чипа МЧПД. Цей сертифікат забезпечується відкритим ключем протоколу автентифікації чипа (EF.DG14) в логічній структурі даних та його підписаним геш значенням в документі об'єкту безпеки.

6) OT.Prot_Abuse-Func «Захист від зловживання функціональності»

Після доставки об'єкту оцінки до користувача МЧПД, об'єкт оцінки повинен запобігти зловживанням функціями тестування і підтримки, які можуть бути використані зловмисниками для розкриття критичних даних користувача, маніпулювання критичними даними користувача з вбудованого програмне забезпечення інтегральної схеми, маніпулювання само кодованим вбудованим програмним забезпеченням інтегральної схеми або з ціллю обійти, відключити, змінити або дослідити функції безпеки або функції об'єкту оцінки.

7) OT.Prot_Inf_Leak «Захист від витоку інформації»

Об'єкт оцінки повинен забезпечити захист від розголошення конфіденційних даних TSF, які зберігаються та / або обробляються в чипі МЧПД

- шляхом вимірювання та аналізу форми і амплітуди сигналів або часу між подіями, що знайдені шляхом вимірювання сигналів електромагнітного поля, споживання потужності, годиннику, або ліній вводу / виводу і
- шляхом примусового виникнення несправності об'єкту аналізу та / або
- фізичною маніпуляцією з об'єктом оцінки.

8) OT.Prot_Phys-Tamper «Захист від фізичних втручань»

Об'єкт оцінки повинен забезпечити захист конфіденційності і цілісності даних користувача, даних TSF, і вбудованого програмного забезпечення МЧПД. Це включає захист від нападів з високим потенціалом за допомогою

- вимір через гальванічні контакти, які піддаються прямому фізичному дослідженню на поверхні чипів, крім місць склеювання (з використанням стандартних інструментів для вимірювання напруги і струму) або
- вимір, який не використовує гальванічних контактів, але має інші види фізичної взаємодії між зарядами (за допомогою інструментів, що використовуються в твердо тільних фізичних дослідженнях та аналізу відмов інтегральної схеми)

• маніпуляції над обладнанням та його функціями безпеки, а також

• контрольовані маніпуляції вмісту пам'яті (призначених для даних користувача та даних TSF)

з пріоритетом

• використання отриманих даних в декількох напрямках для того, щоб зрозуміти конструкцію, властивості і функції.

9) OT.Prot_Malfunction «Захист від несправностей»

Об'єкт оцінки повинен забезпечити свою правильну роботу. Об'єкт оцінки повинен запобігти його експлуатацію за межами нормальних умовах експлуатації, де надійність і безпеку роботи не було доведено або перевірено.

Це зроблено для запобігання помилок. Умови навколишнього середовища можуть включати зовнішньої енергетичні поля (особливо електромагнітні) , напруги (від будь-яких контактів), тактову частоту, або температуру.

Виходячи з наведених вище цілей безпеки і знання механізмів захисту, що застосовуються в паспортній системі, оберемо та обґрунтуємо функціональні вимоги безпеки для кожної мети безпеки.

Мета безпеки OT.AC_Pers «Контроль доступом для персоналізації логічної MRTD» розглядає питання контролю доступу до запису логічної складової MRTD. Права запису до логічних даних MRTD визначається за допомогою функціональних вимог безпеки FIA_UID.1, FIA_UAU.1, FDP_ACC.1 та FDP_ACF.1 однаково: лише вдало автентифікованому агенту персоналізації дозволяється писати дані до груп з EF.DG1 до EF.DG16 логічної складової MRTD лише один раз. Функціональна вимога безпеки FMT_SMR.1 має список ролей (включно з агентом персоналізації) та функціональна вимога безпеки FMT_SMF.1має список функції безпеки об'єкту аналізу (включно з персоналізацією). Агентом персоналізації обробляє ключі базового доступу у відповідності до функціональної вимоги безпеки FMT_MTD.1/KEY_WRITE як вхідні дані автентифікації для Базового контролю доступу.

Автентифікація терміналу, як агент персоналізації повинен буди представлений з використанням функцій безпеки об'єкту аналізу у відповідності до FIA_UAU.4 та FIA_UAU.5. Якщо термінал персоналізації прагне автентифікувати себе до об'єкту аналізу за допомогою протоколу автентифікації терміналу(після автентифікації чипу) з ключами агенту персоналізації об'єкту аналізу буде використовувати функцій безпеки у відповідності до FCS_RND.1(для генерації запиту), FCS_CKM.1, FCS_COP.1/SHA(для виведення нових сеансових ключів після автентифікації чипу),таFCS_COP.1/SYMiFCS_COP.1/MAC(для впровадження безпечного обміну повідомленнями ENC_MAC_Mode), FCS_COP.1/SIG_VER (як частина протоколу автентифікації терміналу) і FIA_UAU.6(для повторної автентифікації). Якщо термінал персоналізації прагне автентифікувати себе до об'єкту аналізу за допомогою симетричного механізму автентифікації з ключами агенту персоналізації об'єкту аналізу буде використовувати функцій безпеки у відповідності до FCS_RND.1 (для генерації запиту) та FCS_COP.1/SYM (для перевірки автентичності спроби). Сесійні ключі повинні буди знищенні після використання у відповідності до FCS_CKM.4.

Функціональна вимога безпеки FMT_MTD.1/KEY_READ запобігає доступ на читання до секретного ключа ключів агенту персоналізації та забезпечує разом з функціональною вимогою безпеки FPT_EMSEC.1 конфіденційність цих ключів.

Мета безпеки OT.Data_Int «Цілісність персональних даних» вимагає об'єкту аналізу захистити цілісність логічних даних MRTD, що зберігаються на чипі MRTD від фізичних маніпуляцій та несанкціонованого запису. Права на запис логічних даних MRTD визначені функціональними вимогами безпеки FDP_ACC.1 і FDP_ACF.1 однаково: лише агенту персоналізації дозволяється писати дані до груп з EF.DG1 до EF.DG16 логічної складової MRTD (FDP_ACF.1.2, правило 1), та в той же час терміналам не дозволено змінювати будь-які дані груп з EF.DG1 до EF.DG16(див. FDP_ACF.1.4). Агент персоналізації повинен ідентифікувати і автентифікувати себе у відповідності до FIA_UID.1 і FIA_UAU.1 перед доступом до цих даних. Функціональна вимога безпеки FMT_SMR.1 має список ролей і функціональна вимога безпеки FMT_SMF.1має список функції безпеки об'єкту аналізу.

Об'єкт аналізу підтримує можливість системі перевірки виявити будь-які зміни, що проходять дані логічної MRTD після протоколу автентифікації чипа. Автентифікація терміналу, яку агент персоналізації повинен виконувати як функцію безпеки об'єкту аналізу, повинна бути у відповідності до функціональних вимог безпеки FIA_UAU.4, FIA_UAU.5 і FIA_UAU.6. Функціональні вимоги безпеки FIA_UAU.6 та FDP_UIT.1 вимагають захисту даних, що передаються після автентифікації чипа за допомогою використання механізму безпечного обміну повідомленнями, який має бути реалізований криптографічними функціями у відповідності до FCS_CKM.1(генерація та розділення секрету), FCS_COP.1/SHA(для виведення нових ключів сесії) і FCS_COP.1/SYM та FCS_COP.1/MAC для впровадження безпечного обміну повідомленнями ENC_MAC_Mode. Сесійні ключі повинні бути знищенні після використання у відповідності до FCS_CKM.4.

Функціональні вимоги безпеки FMT_MTD.1/CAPK та FMT_MTD.1/KEY_READ вимагають, щоб ключ протоколу автентифікації чипа не міг бути не санкціоновано записаним або зчитаним потім.

Мета безпеки OT.Sense_Data_Conf «Конфіденційність посилань на чутливі біометричні дані» забезпечується функціональними вимогами безпеки до контролю доступу, що визначається в FDP_ACC.1 та FDP_ACF.1, та дозволяє читання даних з EF.DG3 та EF.DG4 лише вдало автентифікованій розширеній системі перевірки, яка авторизована валідним сертифікатом, що може бути перевірений у відповідності до FCS_COP.1/SIG_VER.

Функціональні вимоги безпеки FIA_UID.1 і FIA_UAU.1 вимагають ідентифікації та автентифікації перевіряючи систем. Функціональна вимога безпеки FIA_UAU.5 вимагає успішного виконання протоколу автентифікації чипу перед будь-якими спробами автентифікації, як їх використовує розширена система перевірки. Під час забезпечення захищеному зв'язку з центром сертифікації повторне використання інформації автентифікації забезпечується FIA_UAU.4. Функціональні вимоги безпеки FIA_UAU.6 і FDP_UCT.1 вимагають захисту конфіденційності даних, що передаються після автентифікації чипа за допомогою механізму безпечного обміну повідомленнями, який має бути реалізований криптографічними функціями у відповідності до FCS_RND.1(для генерації запиту автентифікації терміналу), FCS_CKM.1(для генерації загального секрету), FCS_COP.1/SHA(для виведення нових ключів сесії) і FCS_COP.1/SYM та FCS_COP.1/MAC для впровадження безпечного обміну повідомленнями ENC_MAC_Mode. Сесійні ключі повинні буди знищенні після використання у відповідності до FCS_CKM.4. Функціональні вимоги безпеки FMT_MTD.1/CAPK та FMT_MTD.1/KEY_READ вимагають, щоб ключ протоколу автентифікації чипа не міг бути не санкціоновано записаним або зчитаним потім.

Щоб дозволити перевірку ланцюжка сертифікатів як значиться в FMT_MTD.3 відкритий ключ центру сертифікації країни, що здійснює перевірку та сертифікат, а також поточна дата записуються або уточнюються авторизованими та ідентифікованими ролями як описано в FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD та FMT_MTD.1/DATE.

Мета безпеки OT.Identification «Ідентифікація і автентифікація об'єкту оцінки» розглядає зберігання даних ідентифікації інтегральної схеми, що унікально ідентифікує чип MRTD в його в енергонезалежній пам'яті. Це буде забезпечено за рахунок функцій безпеки об'єкту аналізу у відповідності до функціональної вимоги безпеки FAU_SAS.1.

Функціональні вимоги безпеки FMT_MTD.1/INI_ENA дозволяє лише виробнику писати дані ініціалізації і дані попередньої персоналізації(включаючи ключ агента персоналізації). Функціональні вимоги безпеки FMT_MTD.1/INI_DIS дозволяє агенту персоналізації деактивувати дані ініціалізації, якщо їх використання на 4 фазі «Оперативне використання» порушує мету безпеки OT.Identification.

Мета безпеки OT.Chip_Auth_Proof «Доведення автентичності чипа MRTD» забезпечується протоколом автентифікації чипа, що передбачений FIA_API.1 доводить ідентичність об'єкту аналізу. Протоколом автентифікації чипа визначено в FCS_CKM.1 виконується з використання конфіденційного секретного ключа, який внутрішньо зберігається в об'єкті аналізу, як це вимагається у FMT_MTD.1/CAPK і FMT_MTD.1/KEY_READ. Протоколом автентифікації чипа вимагає додаткових функцій безпеки об'єкту аналізу у відповідності до FCS_COP.1/SHA(для виведення нових ключів сесії) і FCS_COP.1/SYM та FCS_COP.1/MAC (для впровадження безпечного обміну повідомленнями ENC_MAC_Mode).

Мета безпеки OT.Prot_Abuse-Func «Захист від зловживання функціональності» гарантуються функціональними вимогами безпеки FMT_LIM.1 і FMT_LIM.2, які запобігання зловживанням тестування функціональності об'єкту оцінки або інших можливостей, які можуть бути використані після видачі об'єкту аналізу.

Мета безпеки OT.Prot_Inf_Leak «Захист від витоку інформації» вимагає від об'єкту дослідження забезпечення захисту конфіденційної інформації функцій безпеки об'єкту аналізу, яка зберігається або/та обробляється в чипі MRTD щодо розкриття інформації:

- шляхом вимірювання та аналізу форми і амплітуди сигналів або часу між подіями визначається шляхом вимірювання сигналів електромагнітного поля, споживана потужності, годиннику, або ліній вводу / виводу, які розглядається в функціональній вимозі безпеки FPT_EMSEC.1,
- змушуючи виникнення несправностей об'єкту аналізу, що розглядається в функціональних вимогах безпеки FPT_FLS.1 і FPT_TST.1, або/та
- під фізичним впливом на об'єкт аналізу, що розглядається в функціональній вимозі безпеки SFR FPT_PHP.3.

Мета безпеки OT.Prot_Phys-Tamper «Захист від фізичних втручань» покривається функціональною вимогою безпеки FPT_PHP.3.

Мета безпеки OT.Prot_Malfunction «Захист від несправностей» покривається (i) функціональною вимогою безпеки FPT_TST.1, що вимагає само тестування з метою підтвердження правильності роботи і тестування авторизованих користувачів для перевірки цілісність даних та кодів функцій безпеки об'єкту аналізу, і (ii) функціональною вимогою безпеки FPT_FLS.1, яка вимагає безпечного стану у разі виявленої помилки, або якщо умови експлуатації можуть викликати несправності.

У табл. 1 представлений узагальнений огляд з покриття функціональних вимог безпеки, що були обгрунтовані вище.

Таблиця 1

Покриття функціональними вимогами безпеки об'єкту безпеки

Функціональна вимога	Опис функціональної вимоги	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tampe	OT.Prot_Malfuntion
1	2	3	4	5	6	7	8	9	10	11
FAU_SAS.1	Зберігання даних аудиту				x					
FCS_CKM.1	Генерація ключа шифрування	x	x	x		x				
FCS_CKM.4	Знищення ключа шифрування	x	x	x						
FCS_COP.1/SHA	Криптографічна операція – геш для виведення ключа	x	x	x		x				
FCS_COP.1/SYM	Криптографічна операція – симетричне шифрування/розшифрування	x	x	x		x				
FCS_COP.1/MAC	Криптографічна операція –MAC	x	x	x		x				
FCS_COP.1/SIG_VER	Криптографічна операція – перевірка підпису чипом паспорту	x		x						
FCS_RND.1	Якісна метрика для випадкових чисел	x		x						
FIA_UID.1	Синхронізація ідентифікації	x	x	x						
FIA_UAU.1	Синхронізація автентифікації	x	x	x						
FIA_UAU.4	Механізми єдиного використання автентифікації - єдине використання автентифікації терміналу електронним паспортом	x	x	x						
FIA_UAU.5	Механізми численної автентифікації	x	x	x						
FIA_UAU.6	Повторна автентифікація – повторна автентифікація терміналу електронним паспортом	x	x	x						
FIA_API.1	Автентифікаційний доказ тотожності					x				
FDP_ACC.1	Підмножина управління доступом	x	x	x						
FDP_ACF.1	Атрибут безпеки, заснований на управлінні доступом	x	x	x						
FDP_UCT.1	Основна конфіденційність обміну даними			x						
FDP_UIT.1	Цілісність обміну даними		x							
FMT_SMF.1	Специфікація функцій управління	x	x							
FMT_SMR.1	Ролі безпеки	x	x							
FMT_LIM.1	Обмеження можливостей						x			
FMT_LIM.2	Обмеження доступності						x			
FMT_MTD.1/INI_ENA	Управління даними TSF – запис даних ініціалізації і даних попередньої персоналізації				x					
FMT_MTD.1/INI_DIS	Управління даними TSF – деактивування права доступу на читання до даних ініціалізації і даних попередньої персоналізації				x					
FMT_MTD.1/CVCA_INI	Управління даними TSF – ініціалізація сертифікату CVCA і поточної дати			x						
FMT_MTD.1/CVCA_UPD	Управління даними TSF – центр сертифікації країни, що здійснює перевірку			x						
FMT_MTD.1/DATE	Управління даними TSF – поточна дата			x						
FMT_MTD.1/KEY_WRITE	Управління даними TSF – запис ключа	x								
FMT_MTD.1/CAPK	Управління даними TSF – закритий ключ протоколу автентифікації чипу		x	x		x				
FMT_MTD.1/KEY_READ	Управління даними TSF – читання ключа	x	x	x		x				
FMT_MTD.3	Безпека даних TSF			x						
FPT_EMSEC.1	Випромінювання об'єкту дослідження	x						x		
FPT_TST.1	Тестування функцій безпеки на вимогу							x		x
FPT_FLS.1	Помилка зі збереженням безпечного стану							x		x
FPT_PHP.3	Опір фізичному нападу							x	x	

Література

[1] ICAO 9303- : 9303 part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability.

[2] BSI TR-03110, "Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, 2010.

[3] BSI-CC-PP-0056 Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control.

[4] ICAO 9303- 9303 part 1 volume 1, Sixth edition, 2006, Passports with MachineReadable Data Stored in Optical Character Recognition Format.

[5] ICAO NTWG. Technical report. PKI for Machine Readable Travel Documents offering ICC Read-Only Access; Version - 1.1; October 01, 2004.

[6] Common Criteria Protection Profile - Machine Readable Travel Document with„ICAO Application", Basic Access Control, reference : BSI-PP-0017, Version 1.0, 18thAugust 2005, BSI.

[7] Technical Report Supplemental Access Control Technical advisory group on machine readableTravel documents (tag-mrtd) Nineteenth meeting Montrйal, 7 to 9 december 2009.

[8] J. Bender, M. Fishlin, D. Kuegler, "Security Analysis of the PACE Key-Agreement Protocol", Information Security Conference (ISC) 2009, Lecture Notes in Computer Science, Volume 5735, pp. 33-48, Springer-Verlag, 2009.

Надійшла до редколегії 11.05.2011

Горбенко Юрій Іванович, кандидат технічних наук, технічний директор ЗАТ «ІІТ», науковий співробітник НІЦ «Z» каф. БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах.

Повтарєв Дмитро Валерійович, магістрант кафедри БІТ ХНУРЕ. Область наукових інтересів: дослідження механізмів системи електронних цифрових паспортів.

Тоцький Олександр Сергійович, спеціаліст кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах.

УДК 004.056:004.057.2

Функциональные требования анализа защищенности электронных проездных документов / Ю.И. Горбенко, Д.В. Повтарев, А.С. Тоцкий // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 198–203.

Рассматриваются задачи проведения комплексного анализа механизмов и внесение рекомендаций по устранению недостатков и противодействия угрозам безопасности информации электронных проездных документов.

Ключевые слова: электронный паспорт, функциональные требования защищенности, дополнительный контроль доступа, аутентификация.

Табл. 01. Библиогр.: 08назв.

UDC 004.056:004.057.2

Functional requirements of protection analyze of electronic travel documents / Yu.I. Gorbenko, D.V. Povtariev, O. S. Totskiy // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 198–203.

The paper considers problems of performing a complex analysis of mechanisms and offering recommendations on removing shortcomings and opposing information security theats of electronic travel documents.

Keywords: e-passport, functional requirements of security, supplementary access control, authentication.

Tab. 1 Ref.: 8 items.