**УДК 004.056.53**

# АНАЛІЗ ВИМОГ ТА РЕКОМЕНДАЦІЙ ІСАО ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖІ ATN

***Олексій Голубничий***

*Розроблення та впровадження в експлуатацію мережі авіаційного електрозв'язку, яка використовує стандарти та протоколи пакету протоколів Інтернет, супроводжуються вимогами та рекомендаціями ІСАО щодо забезпечення захисту зв'язку від несанкціонованого доступу. Ці вимоги, з одного боку, мають концептуальний характер, який визначає рівні захисту відповідно до класифікації OSI/ISO, загальну методологію захисту, а з іншого боку – імперативний характер, який визначає конкретні способи та технічні рішення захисту інформаційних ресурсів. Проблема полягає в інтеграції різних технічних рішень захисту з урахуванням їх можливої девіантності там, де це дозволяється концептуальним характером вимог, а також забезпеченні при цьому необхідного рівня захисту. Процедури захисту інформаційних ресурсів при здійсненні сеансів цифрового зв'язку «земля–земля» та «повітря–земля» в мережі ATN/IPS, які рекомендовані нормативними документами ІСАО, повинні реалізовуватися на мережному, транспортному та прикладному рівнях систем цифрового авіаційного зв'язку. При цьому чітко не зазначаються жорсткі критерії необхідного (гарантованого) рівня захисту (критерії оцінки захищеності інформації від несанкціонованого доступу) і в той же час регламентуються до використання заходи із захисту інформації на основі IPsec, IKEv2 та ESP. Тому розроблення моделей загроз та визначення функціональних профілів захищеності для автоматизованих систем (АС) авіаційного призначення може ґрунтуватися на досвіді розроблення моделей загроз та визначення функціональних профілів захищеності для АС класу «2» та класу «3», функціонування яких базується на стандартних телекомунікаційних каналах, що використовують стандарти та протоколи пакету протоколів Інтернет.*

***Ключові слова:*** *інформаційна безпека, авіаційний електрозв'язок, мережа авіаційного електрозв'язку ATN, захист Інтернет-протоколів, протоколи обміну ключами в Інтернет.*

**Вступ.** Розроблення та впровадження в експлуатацію мережі авіаційного електрозв'язку (ATN), яка використовує стандарти та протоколи пакету протоколів Інтернет (IPS), а також відповідних ліній передавання даних VDL, HFDL та AMSS супроводжуються вимогами ІСАО щодо забезпечення захисту зв'язку від несанкціонованого доступу. Ці вимоги, з одного боку, мають концептуальний характер, який визначає рівні захисту відповідно до класифікації OSI/ISO, загальну методологію захисту, а з іншого боку – імперативний характер, який визначає конкретні способи та технічні (програмно-апаратні) рішення захисту інформаційних ресурсів. Проблема полягає в інтеграції різних технічних рішень захисту з урахуванням їх можливої девіантності там, де це дозволяється концептуальним характером вимог, а також забезпеченні при цьому необхідного (гарантованого) рівня захисту.

**Постановка завдання.** Метою статті є систематизація вимог, рекомендацій та заходів щодо забезпечення інформаційної безпеки, які регламентовані нормативними документами ІСАО для сеансів зв'язку «земля-земля» та «повітря-земля» в мережі ATN.

**Аналіз заходів захисту зв'язку «земля–земля».** Захист IP-рівня при проведенні сеансів зв'язку «земля–земля» в об'єднаній мережі ATN/IPS відповідно до вимог та рекомендацій ІСАО [1] здійснюється за допомогою протоколу захисту мережного трафіка IPsec та протоколу обміну ключами в Інтернет, версія 2 (IKEv2).

*Використання IPsec для захисту зв'язку «земля–земля».* Базовою для безпеки цифрового зв'язку «земля–земля» є вимога забезпечення захисту на мережному рівні в об'єднаній мережі ATN/IPS, яка реалізується за допомогою IPsec. IPsec створює границю між незахищеними та захищеними інтерфейсами. IPsec як правило використовується для формування віртуальної приватної мережі VPN між шлюзами [2]. Шлюзом може бути маршрутизатор або інший засіб захисту, наприклад брандмауер. В такому контексті іншими засобами захисту вважаються вузли ATN/IPS. Модель «від шлюзу до шлюзу» захищає зв'язок по мережах ATN/IPS між регіонами або між державами або організаціями в конкретному регіоні. IPsec може також використовуватися в режимі «від хоста до шлюзу» зазвичай для того, щоб дозволити хостам у незахищеній мережі отримати доступ до захищених ресурсів. IPsec також може використовуватися в конфігурації «від хоста до хоста» коли надається захист застосувань в режимі передавання даних між кінцевими системами.

Заходами забезпечення функціональної взаємодії в межах об'єднаної мережі ATN/IPS рекомендації ІСАО розглядають підтримку архітектури безпеки IPsec, протокол інкапсуляції захищених

даних ESP та використання єдиного набору криптографічних алгоритмів. Їх архітектура описана в [15]. Питання ESP розглядаються в [13], а криптографічні алгоритми, які можуть використовуватися, проаналізовані в [4]. Документ ICAO по ATN/IPS [1] додатково уточнює, що кодування за допомогою ESP є факультативним, однак автентифікація виконується завжди.

Цей же документ визначає, що вузли ATN/IPS при роботі в режимі «земля–земля» можуть використовувати протокол автентифікації заголовка IP (AH) (відповідно до вказівок [12]). При цьому зазначається, що AH може використовуватися в окремих виробах, однак все рідше застосовується в IPsec. В [15] зазначається: «Статус положення про підтримку протоколу AH понижений до "MAY" (факультативного), оскільки досвід показує, що лише в дуже обмеженій кількості випадків ESP не може надати необхідних заходів захисту. Слід мати на увазі, що ESP можна використовувати для забезпечення лише цілісності (без конфіденційності), так що він співставний з AH у більшості контекстів».

*Використання IKEv2 для захисту зв'язку «земля–земля».* Архітектура IPsec [15] пропонує підтримку як ручного, так і автоматизованого управління ключами. Тенденція розвитку ATN/IPS показує, що частота ручного управління ключами буде зменшуватися. Тому в рекомендаціях ICAO зазначається, що вузли в умовах зв'язку «земля-земля» реалізовують протокол обміну ключами в Інтернет, версія 2 (IKEv2), який обумовлено в [9], для автоматизованого управління ключами. IKEv2 є останньою версією цього протоколу. Специфікації IKEv2 не такі складні як в першій версії протоколу, що повинно сприяти кращій функціональній сумісності різних схем реалізації.

Як і у випадку з ESP, протокол IKEv2 потребує використання набору обов'язкових алгоритмів для забезпечення сумісності. Даний протокол передбачає використання вузлами при здійсненні зв'язку «земля-земля» криптографічних алгоритмів, які визначені у [3].

*Процедури використання IPsec/IKEv2 для захисту зв'язку «земля–земля».* Процедури використання IPsec/IKEv2 при проведенні сеансів зв'язку «земля–земля» полягають у дотриманні таких правил:

1) IPS-вузли дотримуються вимог архітектури захисту для Інтернет-протоколу (вказані у [15]);

2) IPS-вузли використовують IP-протокол інкапсуляції захищених даних ESP (відповідно до вказівок [13]);

3) IPS-вузли можуть використовувати IP-протокол заголовка автентифікації AH (відповідно до вказівок [12]);

4) IPS-вузли використовують протокол обміну ключами в мережі Інтернет, версія 2 (IKEv2) (відповідно до вказівок [9]);

5) IPS-вузли дотримуються вимог по використанню криптографічних алгоритмів для ESP та AH, якщо використовуються AH (відповідно до вказівок [4]);

6) IPS-вузли використовують нульовий алгоритм шифрування (відповідно до вказівок [4]), але не нульовий алгоритм автентифікації при встановленні асоціацій протоколу захисту мережного трафіка IPsec;

7) IPS-вузли використовують криптографічні алгоритми, що призначені для використання в протоколі IKEv2 (відповідно до вказівок [3]) при узгодженні алгоритмів для обміну ключами;

8) IPS-вузли повинні використовувати профіль сертифіката інфраструктури відкритих ключів в форматі Інтернет X.509 та списку відкликаних сертифікатів CRL (вказаний у [10]), якщо для автентифікації IKEv2 використовується цифровий підпис;

9) IPS-вузли повинні використовувати визначені стандартом Інтернет X.509 політику в галузі сертифікатів інфраструктури відкритих ключів та практику сертифікатів (відповідно до вказівок [11]), якщо для автентифікації IKEv2 використовується цифровий підпис.

Робоча група з безпеки цифрового зв'язку (DSWG) Асоціації повітряного транспорту (ATA) розробила політику в галузі сертифікатів (специфікація 42 ATA) для використання авіаційним співтовариством. Специфікація 42 ATA містить профілі сертифікатів та CRL, які придатні для використання в авіації та функціональною взаємодією з використовуваним аерокосмічною галуззю мостом до інфраструктури відкритих ключів PKI. Ці профілі більш конкретні, ніж у [10], але не протирічать вимогам та рекомендаціям, викладеним у документі ICAO [1].

*Альтернативи IPsec/IKEv2 для захисту зв'язку «земля–земля».* За певних обставин може бути прийнятним використання альтернативних заходів мережної безпеки. Альтернативи IPsec можуть застосовуватися на канальному, транспортному або прикладному рівнях. Документ [2] визначає основні альтернативи, характеризує сильні та слабкі сторони цих альтернатив та наводить ситуації, в яких вони можуть використовуватися.

**Аналіз заходів захисту зв'язку «повітря–земля».** Захист при проведенні сеансів зв'язку «повітря–земля», так же як і при проведенні сеансів зв'язку «земля–земля», в своїй основі передбачає використання протоколу захисту мережного трафіка IPsec та протоколу обміну ключами в Інтернет, версія 2 (IKEv2).

*Використання IPsec для захисту зв'язку «повітря–земля».* Як і при проведенні сеансів зв'язку «земля–земля», для забезпечення функціональної сумісності при проведенні сеансів зв'язку «повітря–земля» документ [1] рекомендує, щоб вузли ATN/IPS підтримували архітектуру безпеки IPsec та протокол ESP. Як і для наземного зв'язку, архітектура відповідає положенням [15], а ESP – вимогам [4]. Однак, замість того, щоб використовувати всі криптографічні алгоритми, які ідентифіковані у [4], вказуються спеціальні алгоритми за замовчуванням для автентифікації, а також для кодування та автентифікації. Це робиться з урахуванням обмеженої ширини смуги каналів зв'язку «повітря–земля», а також для запобігання виникненню невикористаних кодів на платформі авіоніки.

Алгоритмом автентифікації, який обирається для використання, якщо також не обрана функція конфіденційності, є AUTH_HMAC_SHA2_256-128, який вказаний у [20]. Цей алгоритм використовує 256-бітовий ключ для розрахунку хеш-коду автентифікації повідомлень (HMAC) за допомогою хеш-функції SHA-256. Тег є усіченим до 128 біт. Цей же алгоритм використовується для забезпечення цілісності в IKEv2.

Для шифрування ESP нормативна документація ICAO рекомендує використовувати стандарт криптографічного захисту AES в режимі Galois/Counter Mode (GCM). AES-GCM використовується з 8-октетним значенням контролю цілісності (ICV) та довжиною ключа 128 (відповідно до вказівок [19]). AES-GCM є алгоритмом «комбінованого режиму», який дозволяє в рамках однієї операції забезпечувати як конфіденційність, так і автентифікацію. Алгоритми комбінованого режиму характеризуються вищою ефективністю в порівнянні з методом послідовного застосування шифрування та автентифікації. При використанні AES-GCM ICV складається виключно з тега автентифікації AES-GCM, а окремий тег HMAC не застосовується.

*Використання IKEv2 для захисту зв'язку «повітря–земля».* У зв'язку з тим, що при веденні зв'язку «повітря–земля» ручне управління ключами є непрактичним, нормативні документи ICAO рекомендують, щоб вузли ATN/IPS використовували протокол обміну ключами в Інтернет-2 (IKEv2), зазначений у [9]. Як і у випадку з ESP, враховуючи обмеження ширини смуги частот, а також небажаність невикористаних кодів на платформі авіоніки, рекомендується використовувати набір алгоритмів за замовчуванням для використання в IKEv2. При виборі перетворювача слід, наскільки це можливо, враховувати рекомендації Асоціації повітряного транспорту (ATA), Робочої групи з захисту цифрового зв'язку (DSWG), Комітету авіакомпанії з електронної інженерії (AEEC) та Робочої групи з захисту ліній передачі даних (DSEC), проте в рекомендаціях, які зазначені в [1] вказуються лише ті перетворювачі, які зареєстровані в IANA.

IKEv2 використовує п'ять перетворювачів.

1) Псевдовипадкова функція (PRF), яка використовується в IKEv2 для генерування матеріалу ключів і для автентифікації асоціації захисту IKE. У документах ICAO є рекомендації по використанню в якості PRF функції PRF_HMAC _SHA_256, яка зазначена в [20].

2) IKEv2 використовує протокол обміну ключами Дифі-Хелмана для учасників обміну інформацією з обмеженим доступом. Метод Дифі-Хелмана потребує розрахунку дискретного логарифма з використанням арифметики кінцевого поля або еліптичних кривих. При використанні криптографії на еліптичних кривих зазвичай обирають криві основних характеристик або двійкові криві. У нормативних документах ICAO зроблено вибір на користь кривої основних характеристик і рекомендується використовувати 233-бітову випадкову групу ECP відповідно до [5].

3) Якщо для автентифікації об'єкта в IKEv2 використовуються сертифікати відкритих ключів, певні дані при обміні IKEv2 повинні бути підписані. Нормативні документи ICAO рекомендують для цього алгоритм еліптичної кривої для створення цифрового підпису (ECDSA) з використанням SHA-256 в якості хеш-алгоритму на 256-бітовій кривій основних характеристик (відповідно до вказівок [8]).

4) Автентифікаційний обмін по IKEv2 має корисне навантаження, яке шифрується з захистом цілісності. Нормативні документи ICAO рекомендують використовувати в якості криптографічного перетворювача IKEv2 AES-CBC з 128-бітовими ключами (відповідно до вказівок [17]).

5) Нормативні документи ICAO рекомендують використовувати для захисту цілісності зашифрованої корисної інформації MAC-SHA-256-128 як це передбачено в [20].

Згаданий вище пакет алгоритмів разом з AES-GCM, який використовується для ESP-шифрування, становить комплект «Suite-B-GCM-128», використання якого регламентовано у [16]. Очікується, що цей комплект надійде в комерційне серійне виробництво (COTS) і забезпечуватиме адекватний криптографічний захист на період до 2030 року та наступні роки. Додаткові рекомендації з вибору криптографічних алгоритмів і розмірів ключів також надаються в NIST SP 800-57.

Разом з перевагами серійного комерційного виробництва, гнучкості у виборі алгоритмів зв'язку, механізмів автентифікації і інших параметрів, використання протоколу IKEv2 призводить до збільшення кількості службових повідомлень у порівнянні зі стандартним обсягом при застосуванні в авіації. IKEv2 вимагає обміну принаймні чотирма повідомленнями для встановлення сеансового ключа для зв'язку «повітря–земля». Крім того, алгоритми шифрування в IKEv2 і ESP вимагають збільшення розміру повідомлень. Це збільшення, можливо, не дуже помітно у великих повідомленнях, проте для коротких повідомлень воно становить істотну частку. Це є важливим аспектом стосовно ліній передачі даних з обмеженнями по діапазону, проте очікується, що дана проблема буде менш гострою після переходу до високошвидкісних ліній передачі даних для передачі повідомлень, пов'язаних з безпекою польотів.

*Базові процедури захисту при зв'язку «повітря–земля».* Мобільні IPS-вузли використовують заходи захисту мережі доступу, які забезпечують безпеку мережі доступу. Процедури використання IPsec/IKEv2 при проведенні сеансів зв'язку «повітря–земля» полягають у дотриманні таких правил:

1) IPS-вузли дотримуються вимог архітектури захисту протоколу Інтернет (вказані у [15]);

2) IPS-вузли використовують IP-протокол ESP (відповідно до вказівок [13]);

3) IPS-вузли використовують AUTH_HMAC_SHA2_256-128 як алгоритм цілісності для автентифікації ESP (відповідно до вказівок [20]) при встановленні асоціацій захисту IPsec;

4) IPS-вузли при проведенні сеансів зв'язку «повітря–земля» з шифруванням використовують AES-GCM с 8-октетним значенням контролю цілісності ICV та атрибутом довжини ключа 128 біт для шифрування та автентифікації ESP (відповідно до вказівок [19]);

5) IPS-вузли використовують протокол IKEv2 (відповідно до вказівок [9]);

6) IPS-вузли використовують протокол IKEv2 з такими перетвореннями:

а) PRF_HMAC_SHA_256 для псевдовипадкової функції (відповідно до вказівок [20]);

б) 256-бітова випадкова група протоколу управління шифруванням ECP для значень обміну ключами відповідно до алгоритму Дифі-Хелмана (Diffie-Hellman key exchange) (відповідно до вказівок [5]);

в) ECDSA з SHA-256 на кривій P-256 як метод автентифікації (відповідно до вказівок [8]);

г) AES-CBC з 128-бітовими ключами як перетворення у шифруванні IKEv2 (відповідно до вказівок [17]);

д) HMAC_SHA_256-128 як перетворення цілісності IKEv2 (відповідно до вказівок [20]);

7) IPS-вузли повинні використовувати встановлений стандартом Інтернет X.509 профіль сертифіката інфраструктури відкритих ключів та списку відкликаних сертифікатів CRL (відповідно до вказівок [10]), якщо для автентифікації IKEv2 використовується цифровий підпис;

8) IPS-вузли повинні використовувати таку, що відповідає стандарту Інтернет X.509 політику в галузі сертифікатів інфраструктури відкритих ключів і практику сертифікатів (відповідно до вказівок [11]), якщо для автентифікації IKEv2 використовується цифровий підпис; як і для випадку здійснення процедур використання IPsec/IKEv2 при проведенні сеансів зв'язку «земля–земля» Робоча група з безпеки цифрового зв'язку (DSWG) Асоціації повітряного транспорту (ATA) розробила політику в галузі сертифікатів (специфікація 42 ATA) для використання авіаційним співтовариством; специфікація 42 ATA містить профілі сертифікатів та CRL, які придатні для використання в авіації та функціональною взаємодією з використовуваним аерокосмічною галуззю мостом до інфраструктури відкритих ключів PKI; ці профілі більш конкретні, ніж у [10], але не протирічать вимогам та рекомендаціям викладеним у документі ICAO [1];

9) IPS-вузли використовують мобільний протокол Ipv6 з IKEv2 та переглянуту архітектуру IPsec (відповідно до вказівок [14]).

*Захист транспортного рівня при зв'язку «повітря–земля».* Мобільні IPS-вузли та вузли-кореспонденти можуть використовувати протокол захищеного передавання даних TLS (відповідно до вказівок [18]), а також використовують пакет шифрування TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (відповідно до вказівок [6]) при використанні TLS.

*Захист прикладного рівня при зв'язку «повітря–земля».* Мобільні IPS-вузли та вузли-кореспонденти можуть використовувати заходи захисту прикладного рівня на межі діалогового обслуговування IPS, які визначені в [1]. Вони також додають у кінці повідомлень хеш-код автентифікації повідомлень HMAC (відповідно до вказівок [7]), використовуючи SHA-256 як криптографічну хеш-функцію, якщо застосовуються заходи захисту прикладного рівня.

Тег HMAC, вкорочений до 32 бітів, передається поверх даних користувача разом з 32-бітовим порядковим номером пакета (який направляється) для захисту повторного передавання, якщо використовуються заходи захисту прикладного рівня.

IKEv2 використовується для введення в дію ключа, якщо використовуються заходи захисту прикладного рівня.

**Висновки.**

Результати дослідження показують, що процедури захисту інформаційних ресурсів при здійсненні сеансів цифрового зв'язку «земля–земля» та «повітря–земля» в мережі ATN/IPS, які рекомендовані нормативними документами ICAO, повинні реалізовуватися на мережному, транспортному та прикладному рівнях систем цифрового авіаційного зв'язку. При цьому чітко не зазначаються жорсткі критерії необхідного (гарантованого) рівня захисту (критерії оцінки захищеності інформації від несанкціонованого доступу) і в той же час регламентуються до використання заходи із захисту інформації на основі IPsec, IKEv2 та ESP.

Пропонується розроблення моделей загроз та визначення функціональних профілів захищеності для автоматизованих систем (АС) авіаційного призначення (функціонування яких базується на авіаційному цифровому зв'язку «земля–земля» або «повітря–земля») виконувати з урахуванням досвіду розроблення моделей загроз та визначення функціональних профілів захищеності для АС класу «2» та класу «3», функціонування яких базується на стандартних телекомунікаційних каналах, що використовують стандарти та протоколи пакету протоколів Інтернет (IPS).

Враховуючи концепцію впровадження у перспективні системи цифрового авіаційного зв'язку способів передавання, що використовують багатопозиційні методи модуляції та широкосмугові технології, також пропонується підвищувати ступінь захищеності таких систем зв'язку на їх фізичному рівні (використовуючи властивість прихованості складних сигнально-кодових конструкцій).

## ЛІТЕРАТУРА


[1]. Руководство по сети авиационной электросвязи (ATN), использующей стандарты и протоколы пакета протоколов Интернет (IPS): Doc 9896 AN/469. – Издание первое. – Международная организация гражданской авиации (ICAO), 2010. – 112 с.

[2]. Computer security. Guide to IPsec VPNs: NIST SP 800-77. – National Institute of Standards and Technology (NIST), 2005. – 126 pp.

[3]. Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2): RFC 4307. – Internet Engineering Task Force (IETF), 2005. – 6 pp.

[4]. Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH): RFC 4835. – Internet Engineering Task Force (IETF), 2007. – 11 pp.

[5]. ECP Groups for IKE and IKEv2: RFC 4753. – Internet Engineering Task Force (IETF), 2007. – 16 pp.

[6]. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS): RFC 4492. – Internet Engineering Task Force (IETF), 2006. – 35 pp.

[7]. HMAC: Keyed-Hashing for Message Authentication: RFC 2104. – Internet Engineering Task Force (IETF), 1997. – 11 pp.

[8]. IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA): RFC 4754. – Internet Engineering Task Force (IETF), 2007. – 15 pp.

[9]. Internet Key Exchange (IKEv2) Protocol: RFC 4306. – Internet Engineering Task Force (IETF), 2005. – 99 pp.

[10]. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: RFC 5280. – Internet Engineering Task Force (IETF), 2008. – 151 pp.

[11]. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework: RFC 3647. – Internet Engineering Task Force (IETF), 2003. – 94 pp.

[12]. IP Authentication Header: RFC 4302. – Internet Engineering Task Force (IETF), 2005. – 34 pp.

[13]. IP Encapsulating Security Payload (ESP): RFC 4303. – Internet Engineering Task Force (IETF), 2005. – 44 pp.

[14]. Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture: RFC 4877. – Internet Engineering Task Force (IETF), 2007. – 26 pp.

[15]. Security Architecture for the Internet Protocol: RFC 4301. – Internet Engineering Task Force (IETF), 2005. – 101 pp.

[16]. Suite B Cryptographic Suites for IPsec: RFC 4869. – Internet Engineering Task Force (IETF), 2007. – 9 pp.

[17]. The AES-CBC Cipher Algorithm and Its Use with IPsec: RFC 3602. – Internet Engineering Task Force (IETF), 2003. – 15 pp.

[18]. The Transport Layer Security (TLS) Protocol Version 1.2: RFC 5246. – Internet Engineering Task Force (IETF), 2008. – 104 pp.

[19]. The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP): RFC 4106. – Internet Engineering Task Force (IETF), 2005. – 11 pp.
[20]. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec: RFC 4868. – Internet Engineering Task Force (IETF), 2007. – 21 pp.

## REFERENCES

[1]. International Civil Aviation Organization (ICAO) (2010), Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, 1st ed.
[2]. National Institute of Standards and Technology (2005), NIST SP 800-77: Guide to IPsec VPNs.
[3]. Internet Engineering Task Force (IETF) (2005), RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).
[4]. Internet Engineering Task Force (IETF) (2007), RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).
[5]. Internet Engineering Task Force (IETF) (2007), RFC 4753: ECP Groups for IKE and IKEv2.
[6]. Internet Engineering Task Force (IETF) (2006), RFC 4492: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).
[7]. Internet Engineering Task Force (IETF) (1997), RFC 2104: HMAC: Keyed-Hashing for Message Authentication.
[8]. Internet Engineering Task Force (IETF) (2007), RFC 4754: IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA).
[9]. Internet Engineering Task Force (IETF) (2005), RFC 4306: Internet Key Exchange (IKEv2) Protocol.
[10]. Internet Engineering Task Force (IETF) (2008), RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[11]. Internet Engineering Task Force (IETF) (2003), RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
[12]. Internet Engineering Task Force (IETF) (2005), RFC 4302: IP Authentication Header.
[13]. Internet Engineering Task Force (IETF) (2005), RFC 4303: IP Encapsulating Security Payload (ESP).
[14]. Internet Engineering Task Force (IETF) (2007), RFC 4877: Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.
[15]. Internet Engineering Task Force (IETF) (2005), RFC 4301: Security Architecture for the Internet Protocol.
[16]. Internet Engineering Task Force (IETF) (2007), RFC 4869: Suite B Cryptographic Suites for IPsec.
[17]. Internet Engineering Task Force (IETF) (2003), RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec.
[18]. Internet Engineering Task Force (IETF) (2008), RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2.
[19]. Internet Engineering Task Force (IETF) (2005), RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP).
[20]. Internet Engineering Task Force (IETF) (2007), RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec.

## АНАЛИЗ ТРЕБОВАНИЙ И РЕКОМЕНДАЦИЙ ICAO ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ ATN

Разработка и введение в эксплуатацию сети авиационной электросвязи, использующей стандарты и протоколы пакета протоколов Интернет, сопровождаются требованиями и рекомендациями ICAO по обеспечению защиты связи от несанкционированного доступа. Эти требования, с одной стороны, имеют концептуальный характер, определяющий уровни защиты в соответствии с классификацией OSI/ISO, общую методологию защиты, а с другой стороны – императивный характер, определяющий конкретные способы и технические решения защиты информационных ресурсов. Проблема заключается в интеграции разных технических решений защиты с учётом их возможной девиантности там, где это допускается концептуальным характером требований, а также обеспечении при этом необходимого уровня защиты. Процедуры защиты информационных ресурсов при осуществлении сеансов цифровой связи «земля–земля» и «воздух–земля» в сети ATN/IPS, рекомендованные нормативными документами ICAO, должны реализовываться на сетевом, транспортном и прикладном уровнях систем цифровой авиационной связи. При этом чётко не указываются жёсткие критерии необходимого (гарантированного) уровня защиты (критерии оценки защищённости информации от несанкционированного доступа) и в то же время регламентируются к использованию меры по защите информации на основе IPsec, IKEv2 и ESP. Поэтому разработка моделей угроз и определение функциональных профилей защищённости для автоматизированных систем (АС) авиационного назначения могут быть основаны на опыте разработки моделей угроз и определения функциональных профилей защищённости для АС класса «2» и класса «3», функционирование которых базируется на стандартных телекоммуникационных каналах, использующих стандарты и протоколы пакета протоколов Интернет.

**Ключевые слова:** информационная безопасность, авиационная электросвязь, сеть авиационной электросвязи ATN, защита Интернет-протоколов, протоколы обмена ключами в Интернет.

## AN ANALYSIS OF ICAO REQUIREMENTS AND RECOMMENDATIONS FOR INFORMATION SECURITY OF THE ATN

Development and commissioning of the Aeronautical Telecommunication Network using standards and protocols for Internet Protocol Suite accompanied by the ICAO requirements and recommendations for the protection of communications against unauthorized access. These requirements, on the one hand, are conceptual in nature determining the levels of protection in accordance with the classification of the OSI/ISO, the general methodology of protection, on the other hand, have mandatory defining specific processes and technical solutions protect information resources. The problem boils down to the integration of various technical security solutions considering their possible deviance, where permitted by the conceptual nature of the requirements, and at the same time ensuring the necessary level of protection. Procedures for the protection of information resources in the implementation of digital communication sessions "ground-to-ground" and "air-to-ground" in the network ATN/IPS, recommended by the regulations of the ICAO, should be implemented in the network, transport, and application layers of digital aeronautical communications. There is not clearly specified strict criteria for the required (guaranteed) level of protection (evaluation criteria for information security from unauthorized access) and at the same time regulates the use of measures to protect the information based on IPsec, IKEv2 and ESP. Therefore the development of threat models and the definition of the functional profile of security for automated systems (AS) of aviation applications can be based on the experience of the development of threat models and definitions of functional profiles of protection for AS of the class "2" and class "3", the operation of which is based on standard telecommunication channels using the standards and protocols of the Internet protocol Suite.

**Keywords:** information security, aeronautical telecommunications, Aeronautical Telecommunication Network, protection of Internet protocols, Internet Key Exchange protocol.

**Голубничий Олексій Георгійович**, кадидат технічних наук, доцент, докторант Національного авіаційного університету.
E-mail: a.holubnychyi@nau.edu.ua
**Голубничий Алексей Георгиевич**, кандидат технических наук, доцент, докторант Национального авиационного университета.
**Holubnychyi Alexei**, PhD in Eng., Docent, Doctoral Student of the National Aviation University.

**УДК 004.658.2**

## ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ МЕТОДОМ МАСКИРОВАНИЯ

***Михаил Коломыцев, Анатолий Южаков***

*Согласно закону о защите персональных данных, владельцы баз персональных данных обязаны обеспечить их защиту. Основным видом хранилища для персональных данных в информационной системе является база данных. Практика разработки информационных систем показывает, что, кроме производственной (основной) базы данных, возникает задача создания ее копий, непроизводственных (тестовых) баз данных. Использовать в тестовых базах данных такой универсальный механизм, как криптография, для защиты персональных данных не всегда представляется возможным. Причина тому не только известные законодательные ограничения, но и то, что тестовые базы данных должны быть функционально эквивалентными производственной базе данных. Это означает, что защищаемая информация должна быть представлена в виде, не нарушающем целостность базы данных (как целостность по ссылкам, так и по принадлежности данных к определенному домену). Для защиты персональных данных в такой ситуации можно использовать подход, который называется маскирование данных. В данной статье раскрывается суть данного метода, его актуальность, требования к реализации. Авторы предлагают разработанную ими в виде программного кода методику защиты персональных данных в среде MS SQL Server.*

***Ключевые слова**: база данных, персональные данные, защита персональных данных, маскирование данных, конфиденциальные данные, информационная система.*

**Актуальность задачи маскирования данных.** Согласно закону о защите персональных данных [1], владельцы баз персональных данных (ПД) обязаны обеспечить их защиту. Особенно важно защищать данные, идентифицирующие конкретную личность. К таким данным можно отнести индивидуальный налоговый номер (ИНН), серию и номер паспорта, ФИО, почтовые адреса, телефоны, номера банковских карточек и другие.

Основным видом хранилища для персональных данных в информационной системе является