РЕАЛІЗАЦІЯ СЕРЕДОВИЩА АУДИТУ ТА МОНІТОРИНГУ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Анна Чунарьова

Національний авіаційний університет, Україна

ЧУНАРЬОВА Анна Вадимівна, к.т.н., доцент

Рік та місце народження: 1987 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: доцент кафедри комп'ютеризованих систем захисту інформації кафедри з 2012 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 93 наукові публікації, серед яких наукові статті, патенти на корисні моделі та навчально-методичні роботи.
E-mail: chunariova@gmail.com

Анотація. *У даній статті сформовано систему вимог та основних правил, щодо процесів моніторингу й управління доступом до інформаційних мереж. Виділено переваги та недоліки застосування комплексу засобів захисту на базі методів аудиту та контролю. Сформовані правила та рекомендації дозволили виділити етапи реалізації системи аудиту та моніторингу.*

Ключові слова: *захист інформації, моніторинг, системний журнал, інформаційно-комунікаційна система та мережа, система захисту.*

Вступ

На сьогоднішній день організації мають розгалужені інформаційно-комунікаційні системи та мережі і тому на перше місце виходить завдання управління, як і інформаційними потоками та безліччю різноманітних захисних механізмів у таких корпоративних мережах. Складність мережної інфраструктури, різноманіття даних та програм призводять до того, що при реалізації системи інформаційної безпеки необхідне здійснення регулярного аудиту та постійного моніторингу безпеки інформаційних потоків та структури інформаційно-комунікаційної системи та мережі (ІКСМ). Моніторинг ІКСМ є невід'ємною частиною забезпечення інформаційної безпеки корпоративної мережі з точки зору забезпечення цілісності, конфіденційності та доступності.

Виконання завдань моніторингу неможливе без відображення поточного стану захищеності ІКСМ на основі існуючих критеріїв оцінки захищеності інформації від несанкціонованого доступу. Нормативним документом з цих питань виступає НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Функціональними критеріями за документом є: конфіденційність; цілісність; доступність; спостереженість [1].

Постановка задачі

Для вирішення більшої частини проблем, які виникають при функціонуванні корпоративних мереж, застосовують системи моніторингу й управління мережею. Цей клас рішень забезпечує інвентаризацію й розширену діагностику комп'ютерних мереж; постійний контроль функціонування використовуваного мережного устаткування, прикладних систем і мережних сервісів; збір статистики й візуалізацію ключових показників продуктивності й операційних параметрів мережної інфраструктури; оптимізацію навантаження на мережне устаткування й сервери; фіксацію інцидентів; аналіз впливу ризиків на бізнес-процеси і критично важливі додатки; локалізацію причин інциденту і його автоматичне усунення, або повідомлення відповідальних за його усунення осіб. Використання подібних систем дозволяє організації здійснювати активний моніторинг доступності, стану й продуктивності компонентів корпоративної мережі передачі даних, аналізувати й оптимізувати їхнє завантаження, а також прогнозувати виникнення позаштатних ситуацій.

Метою даної статті є розробка рекомендацій щодо функціонування сучасних засобів реалізації методів аудиту та моніторингу функціональних елементів автоматизованої інформаційної системи у рамках створення комплексної системи захисту інформації. Використання даних рекомендацій дозволить підвищити рівень захищеності даних, що зберігаються у БД Oracle, засобами аудиту і завдяки методу активного налаштування та дозволить централізовано обробляти дані щодо процедур аудиту зі всіх сегментів ІКСМ.

Під ***моніторингом доступу й використання системи*** будемо розуміти *процес виявлення відхилень*

від реалізації політики управління доступом до інформаційних ресурсів та мережних послуг з метою фіксації неавторизованих дій.

Необхідно проводити моніторинг системи, щоб виявляти відхилення від політики управління доступом і записувати контрольовані події, а також забезпечувати доказ у випадку інцидентів, що стосуються безпеки інформаційної мережі та її ресурсів. Моніторинг системи дає змогу перевіряти ефективність прийнятих засобів управління й підтверджувати відповідність моделі системи політиці доступу.

Варто створювати журнали аудиту для запису подій, пов'язаних з безпекою інформаційних ресурсів та мережних послуг, і зберігати їх протягом погодженого періоду, з метою надання допомоги в майбутніх розслідуваннях і моніторингу управління доступом.

Необхідно встановлювати стандартизовані процедури для моніторингу використання засобів обробки інформації. Такі процедури необхідні для забезпечення впевненості в тім, що користувачі виконують тільки ті дії, на які вони були явно авторизовані. Рівень моніторингу, необхідного для окремих засобів, варто визначати за допомогою оцінки ризику.

В попередніх роботах було проведено класифікацію та аналіз існуючих методів аудиту та моніторингу інформаційних потоків ІКСМ, що дозволило формувати критерії оцінки якості систем моніторингу. Також було проведено тестування поширених інструментів моніторингу та аудиту за наступними характеристиками: підтримка різних операційних систем; можливість аудиту та контролю різних за призначенням серверів; можливість аудиту та контролю СУБД; виявлення відхилень функціонування мережі від норми (поява незареєстрованих вузлів, втрата зв'язку з окремими вузлами, втрата пакетів, перенавантаження комунікаційних пристроїв); підтримка графічних інтерфейсів для перегляду звітів, можливості конфігурування параметрів налаштувань [2, 3].

Формування вимог для створення комплексу засобу захисту (КЗЗ) на базі методів аудиту та контролю

Основною вимогою до середовища КЗЗ є його відповідність функціональному профілю захищеності, тому необхідно щодо кожного критерію визначити перелік дій, що потребують реалізації (таблиця 1).

Критерій оцінки захищеності КЗЗ на базі методів аудиту та контролю Таблиця 1

Критерій оцінки захищенності	Шлях реалізації
КД-3 «. Повна довірча конфіденційність»	Застосування LDAP – серверу для опису облікових записів, політики доступу до ресурсів.
КА-3 «. Повна адміністративна конфіденційність»	Підтримка авторизації через LDAP.
КВ-3 «Повна конфіденційність при обміні»	Підтримка LDAP – функціональності на Active Directory.
ДР-3 «Пріоритетність використання ресурсів»	Застосування механізму пріоритезації виконуваних процесів; штучне обмеження пропускної здатності мережі працівників.
НР -4 «Детальна реєстрація»	Застосування прикладних протоколів (Netflow, SNMP) реєстрації стану апаратного забезпечення; розміщення централізованого колектору syslog для накопичення записів подій з елементів ІКСМ;
НЦ-3 «КЗЗ з функціями диспетчера доступу»	Підтримка LDAP – авторизації на всіх можливих елементах ІКСМ; Застосування детального аудиту серверу баз даних (fine-grained audit - FGA) в сукупності з контекстами додатків для контролю доступу до об'єктів БД.
НТ-2 «Самотестування при старті»	Створення інструментів, що виконують запити на отримання даних щодо життєво – важливих показників апаратного забезпечення ІКСМ.

КЗЗ, що реалізовує аудит та моніторинг стану ІКСМ, складається з багатьох окремих програмних компонентів та прикладних протоколів взаємодії у Front та Back частинах мережної інфраструктури організації «Процес - сервіс» :

− LDAP – технологія зберігання та доступу до даних користувачів мережі;

− SNMP – протокол керування програмними та апаратними компонентами комп'ютерної мережі;

− Syslog – системний журнал, подібний колектору записів подій, який є базовою складовою процедури моніторингу.

− Сервіс трансляції записів подій типу Windows Event у події стандарту syslog.

Окремим етапом аудиту та моніторингу є аудит баз даних Oracle.

Далі при розробці рекомендацій найбільшу увагу слід приділити реалізації таких критеріїв оцінки захищеності, як НР-4, НЦ-3, НТ-2. Розглянемо питання реалізації даних критеріїв при розробці КЗЗ на базі методів аудиту та контролю більш детально.

НР–4 «Детальна реєстрація»

Використання процедури реєстрації дозволяє

контролювати небезпечні для ІКСМ дії. КЗЗ, яка основана на даному критерії, здатна контролювати одиничні або повторювані реєстраційні події та негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій [1].

Компоненти, що реалізовують даний критерій, мають забезпечувати:

1. Реєстрацію подій, що мають пряме чи опосередковане відношення до безпеки інформації, компонентів ІКСМ;

2. Централізоване накопичення записів подій на колекторі типу syslog, з можливістю, швидкої вибірки, ротації логів, попередження перевищення квот пам'яті, зайнятої записами, сортуванню за типом подій.

3. Налаштування тригерів, що відправлятимуть повідомлення для випадку перевищення порогів значень.

4. Аудит доступу до баз даних з підтримкою можливості реєстрації ідентифікаторів доступу користувачів у разі наявності проміжного елементу – серверу додатків.

Практична реалізація даного критерію вимагає вивчення теоретичної частини створення, використання та підтримки журналів подій.

Ведення журналів подій

До сфери відповідальності адміністраторів організації «Процес - сервіс» входить аналіз подій, що сталися в масштабах організації. Аналіз можна виконати шляхом використання можливості програмного забезпечення, встановленого на вузлах ІКСМ, генерування записів подій. Задача налаштування процесу ведення журналу подій є неординарною через необхідність знаходження «золотої» середини між детальністю записів подій та об'ємом постійної пам'яті, що при цьому буде використовуватися.

Типи записів подій ІКСМ у системному журналі:

1. Запис у текстовому файлі – кожний запис представлений окремим рядком у текстовому файлі.

2. Запис у вигляді декількох рядків у файлі. Зазвичай до такого типу відносять логи у форматі xml, та подібних. Даний тип запису потребує спеціального програмного забезпечення (ПЗ) для зчитування, але дозволяє формалізувати запис події.

3. Бінарний запис подій. Є непридатним для читання у необробленому вигляді. Для роботи за такими логами необхідне ПЗ для перетворення двійкових даних у придатну для читання інформацію.

4. Запис подій у бази даних. Даний тип запису є досить зручним з точки зору виконання запитів на вибірку необхідної інформації, але може вплинути на загальну продуктивність системи [4-8].

З точки зору зручності та адекватності використання ПЗ з ведення журналу подій найбільш важливою функцією ПЗ є критерій заміни логів (ротація). Файли логів з часом стають занадто великими, що може вплинути на продуктивність системи, тому необхідне забезпечення наступного:

− Кожного дня (тижня, місяця) система створює новий лог – файл. При цьому в імені файлу повинна фігурувати дата та час створення файлу. Файли зі старішими записами зберігаються до певного моменту, можливе їх архівування.

− Створення нового файлу виконується при досягненні певного розміру поточним файлом. Ім'я файлу повинне мати хоча б унікальний ідентифікатор, що збільшується на одне значення при кожному створенні нового файлу.

− Зміна файлу виконується одночасно з перезавантаженням служби, яка відповідає за ведення журналу. У даному випадку можлива ситуація зі зниженням продуктивності системи через тривале функціонування служби.

− Періодичність запису даних у файл. Даний параметр дозволяє визначити об'єм накопичених у оперативній пам'яті записів, при досягненні якого виконується їх запис у файл. При грамотному налаштуванні це дозволяє зменшити кількість звернень служби ведення журналу подій до накопичувача [8].

− Фільтрація подій дає можливість вибору тих подій, що дійсно необхідні, дозволяє оптимізувати роботу системи накопичення записів подій, полегшити завдання аналізу операторам та спеціалістам з моніторингу, адміністраторам, знизити навантаження на сервіси та системи, що відсилають записи подій.

НЦ-3 «КЗЗ з функціями диспетчера доступу»

Використання даного критерію визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Реалізований КЗЗ гарантує, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Компоненти, що реалізовують даний критерій, мають забезпечувати:

1. Централізоване керування обліковими записами кадрового складу, корпоративних та фізичних клієнтів організації, використовуючи LDAP – сервер.

2. Підтримку можливості авторизації на всіх можливих компонентах ІКСМ через LDAP – сервер.

3. Застосування аудиту в цілому та методу облікових записів як необхідної складової діяльності аудиту СУБД.

В масштабах КЗЗ використання аудиту СУБД є важливою процедурою. Його наявність дозволяє реєструвати будь-які потенційно небезпечні та підозрілі дії осіб, що отримали доступ до БД, надсилати повідомлення адміністратору безпеки щодо виникнення нештатних ситуацій з метою здійснення несанкціонованого доступу [9].

Стандартні налаштування аудиту СУБД Oracle дозволяють контролювати системні та об'єктні привілеї доступу до таблиць. Існує 2 варіанти застосування баз даних для збереження та маніпулювання даними:

1. Безпосереднє підключення до БД одним з клієнтських додатків від Oracle, або інших виробників програмного забезпечення. При цьому, кожний користувач використовує унікальний ідентифікатор для доступу до бази даних. За наявного увімкненого аудиту, даний ідентифікатор однозначно вказуватиме на особу у звітах з аудиту [10-13].

2. У якості проміжного елементу між користувачем та БД використовується сервер додатків, який є середовищем виконання певного серверного додатку. Взаємодія користувача з БД відбувається неявно. За таких обставин користувач взаємодіючи з додатком, неявно виконує запити до БД на отримання, зміну або видалення даних. Для забезпечення доступу адміністратор СУБД заздалегідь створює облікові записи. Кожний з користувачів має власний ідентифікатор, за яким його можна буде ідентифікувати в захищеній ІКСМ, наприклад, у звітах з аудиту, всі вони взаємодіють з об'єктами БД через користувача App_user.

За існування другого варіанту, у звітах з аудиту будуть відсутні ідентифікатори, за якими можна було б визначити реальну особу, що здійснила певні дії з об'єктами БД.

Застосування методу облікових записів дозволить підвищити рівень надійності даних аудиту у звітах та використати механізм, який знижує ймовірність взаємодії з даними, що перевищує привілеї для конкретної особи.

У таблиці продемонстровано прототип таблиці аудиту, за умови використання методу облікових записів. Поле client_id є унікальним. Саме воно відповідає за збереження ідентифікатора користувача.

Таблиця аудиту — Таблиця 2

Timestamp	Object_ name	Policy_name	Sql_text	**Client_id**
21-04-2013 15:44:10	Table1	Audit rule1	Select field1, field2 from Table1 when field>N	**Id1111**
23-05-2013 16:44:10	Table1	Audit rule2	Update Table1 set field1 = N when field1=M	**Id1222**

Теоретичне підґрунтя методу облікових записів

Основним підґрунтям створення даного методу є наявність у СУБД Oracle такого поняття, як контекст. Поняття контексту можна пояснити абстрактною структурою даних, кожний запис якої має значення, та унікальний ключ, за яким можна отримати значення. У межах СУБД у контексті можуть знаходитися навіть посилання на дані з таблиць та інших об'єктів для пришвидшення доступу до них.

Контекст є тим місцем зберігання даних, що дозволить вирішити задачу ідентифікації користувачів та створення необхідних політик безпеки по відношенню до об'єктів БД. У рамках кожної сесії з'єднання можна створити унікальний контекст з даними, до яких існуватиме доступ лише в межах поточної сесії [10-16].

За замовчуванням, кожної нової сесії з'єднання створюється контекст USERENV, значення якого доступні лише для прочитання. За його допомогою можна дізнатися про:

− дані щодо механізму автентифікації для поточної сесії;

− клієнтський ідентифікатор.

− регіональні дані, дійсні для поточної сесії;

− IP – адресу та назву хосту, з якого виконується з'єднання.

Обов'язковою складовою даного методу є Fine – grained audit (Деталізований аудит), застосування якого дає можливість динамічно змінювати запит користувача перед його виконанням в залежності від певних чинників. Такими чинниками можуть бути джерело запиту, автор запиту, значення змінних, що знаходяться у контексті. Прикладом деталізованого контролю доступу може бути політика безпеки, яка визначає, які записи можуть бути доступними для читання різним групам користувачів. Дана політика формує предикат, зміст якого залежить від того, який користувач виконує запит. Наприклад, оригінальний запит має вигляд "select * from table". Його обробка існуючою політикою може призвести до наступного вигляду : "Select * from (select * from table1 where approved_user = N)".

Переваги та недоліки застосування методу КЗЗ на базі методів аудиту та контролю

Перевагами застосування даного методу є:

− заборона на з'єднання з БД від імені генералізованих облікових записів. З'єднання може бути встановлене лише у випадку, коли користувач надав власний унікальний ідентифікатор;

− спрощення розробки додатків;

− гарантування повного захисту інформації БД та безперервного захисту незалежно від того, яким чином відбувається з'єднання з БД;

− спрощення підтримки об'єктів БД. Зменшується загальна кількість об'єктів БД, які необхідні для підтримки додатку.

Недоліком даного методу є складність виявлення помилок у PL-SQL скриптах, що відповідають за підтримку політики безпеки, через те, що вони виконуються у фоновому режимі. Для відлагодження рекомендується використовувати пакет debug.

НТ-2 «Самотестування при старті»

Компоненти, що реалізовують даний критерій, мають забезпечувати:

1. Опитування програмних та апаратних компонентів при їх старті, задля отримання значень основних життєво-важливих параметрів.

2. Періодичне опитування програмних та апаратних компонентів.

3. Побудова графічної схеми, що демонструє стан ІКСМ на даний момент часу.

Етапи реалізації системи аудиту та моніторингу. В процесі побудови КЗЗ, що базується на засобах аудиту та моніторингу, необхідно забезпечити виконання наступних етапів:

1. Створення реєстру апаратного та програмного забезпечення з класифікацією за можливістю моніторингу його, наявності налаштувань для інтеграції його у загальну систему моніторингу, можливості передачі інформації захищеними каналами (протоколами).

2. Створення реєстру відповідальних осіб за програмно-апаратне забезпечення, з можливістю запису контактних даних до параметрів одиниці забезпечення (SNMP).

3. Визначення переліку параметрів, за якими буде проводитися аудит та моніторинг для кожної одиниці інфраструктури організації.

4. Створення конфігурації системних журналів на всіх можливих одиницях інфраструктури мережі для забезпечення генерації оптимальної кількості записів подій та можливості їх трансляції на центральний колектор логів.

5. Уведення в експлуатацію програмних сервісів, які забезпечуватимуть перетворення записів подій формату Windows Event Log у формат syslog з можливістю подальшої їх передачі на центральний колектор логів.

6. Редагування Адміністративної Бази даних агентів SNMP, встановлених на елементах інфраструктури мережі для отримання можливості аудиту та моніторингу за встановленим раніше переліком параметрів.

7. Планування політики розмежування доступу працівників та клієнтів організації до інформаційних об'єктів мережі та вибір моделі розподілу доступу до інформації.

8. Планування політики розмежування доступу працівників організації до об'єктів СУБД Oracle.

9. Створення пакету та скриптів SQL генерації службових таблиць у СУБД Oracle для отримання можливості впровадження методу облікових записів.

Висновок

Можна відзначити, що моніторинг відомчих мереж є перспективним напрямком розвитку інформаційної інфраструктури та гарантованості надання послуг. Незважаючи на низку проблем, які виникають при його впровадженні, використання подібних рішень забезпечить значний ріст ефективності використання апаратного й програмного забезпечення та знизить кількість критичних збоїв у системах, що особливо важливо для сучасних підприємств.

Сформовано систему вимог та основних правил, щодо процесів моніторингу й управління доступом до інформаційної мереж.

Література

[1] Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

[2] Чунарьова А.В. Підсистеми моніторингу функціонування корпоративних мереж / А.В. Чунарьова, О.К. Юдін // Захист інформаційно-комунікаційних систем: науково-практична конференція, 26-28 травня 2009, Київ. – К.: НАУ, 2009. – С. 59-60.

[3] Чунарьова А.В. Сучасні засоби моніторингу інформаційних потоків ІКСМ / А.В. Чунарьова, А.В. Чунарьов, К.П. Сластенко // Wyksztalcenie i nauka bez granic-2012: Materialy VIII Miedzynarodowej naukowo-praktycznej konferencji, 07-15 grudnia 2012, Polska. – Przemysl: Nauka i studia, 2012. – Vol. 34. – P. 74-77.

[4] Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques / A. Cecil // Computer Systems Analysis. – 2006. – P. 4–7.

[5] Lowekamp B. Using passive traces of application traffic in a network monitoring systems / B.B. Lowekamp, M. Zangrilli. – IEEE Computer Society, 2004. – P. 73 – 75.

[6] Internetworking Technology Handbook : User manual / Jackson C. – Massachusets : Cisco Systems, 2011. – P. 56 -67.

[7] Jackson C. Network Security Auditing / C. Jackson. – Indianapolis : Cisco Press, 2010. – P. 112 – 118, 136.

[8] Fry C. Security Monitoring / C. Fry, M. Nystrom – Sebastopol : O'Reily Media, 2009. – P. 40–56, 163–170.

[9] Davis C. IT Auditing. Using controls to protect information assets / C. Davis, M. Schiller, K. Wheeler. – Chicago : McGraw – Hill Companies, 2011. – P. 119–135, 145–150, 171–180.

[10] Rajvaidya P. A Router – based technique for monitoring the next generation of Internet multicast protocols / P. Rajvaidya, K. C. Almeroth // Symposium On Cryptography and Information Security. – 2001. – №3. – P. 2–4.

[11] Della Maggiora P. Performance and fault management. / P. L. Della Maggiora, C. E. Elliott, R. L. Pavone, K. J. Phelps, J. M. Thompson. - Indianapolis : Cisco Press, 2003. – P. 135–143.

[12] Strassner J.C. Policy – based network management. / J. Strassner. – Colorado : Morgan Kaufmann Publishers, 2004. – P. 28–33.

[13] Уилсон Э. Мониторинг и анализ сетей / Э. Уилсон. – Москва : Лори, 2002. – С. 211–215, 267–271.

[14] Нанда А. Oracle PL/SQL для администраторов баз данных / А. Нанда, С. Фейерштейн. – Москва : O'Reily Media, 2008. – С. 25–28, 74–81.

[15] Price J. Oracle Database 11G SQL / J. Price. – McGraw – Hill Osborne Media, 2007. – P. 210–217.

[16] Zeltserman D. Practical Guide to SNMPv3 and network management / D. Zetserman. – Colorado : Prentice Hall PT, 1999. – P. 184–192, 207–211.

УДК 004.056.53 (045)

Чунарева А.В. Реализация среды аудита и мониторинга современных информационно-коммуникационных систем и сетей
Аннотация. *В данной статье сформирована система требований и основных правил, относительно процессов мониторинга и управления доступом к информационной сети. Выделены преимущества и недостатки применения комплекса средств защиты на базе методов аудита и контроля. Сформированные правила и рекомендации позволили выделить этапы реализации системы аудита и мониторинга.*
Ключевые слова: *защита информации, мониторинг, системный журнал, информационно-коммуникационная система и сеть, система защиты.*

Chunariova A.V. Implementation of audit & monitoring environment of modern information and communication systems and networks
Abstract. *In this article the system requirements and the basic rules on processes to monitor and control access to network information. Highlighted the advantages and disadvantages of the use of remedies against on the basis of auditing and control. Formed rules and recommendations possible to identify the stages of implementation of audit and monitoring.*
Keywords: *information security, monitoring, system log, information and communication system and network protection.*

Отримано *13 травня 2013 року*, затверджено редколегією *5 червня 2013 року*

СКОРОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ В КВАНТОВОМ КАНАЛЕ С ДЕПОЛЯРИЗАЦИЕЙ ПРИ КОДИРОВАНИИ СИМВОЛОВ ОРТОГОНАЛЬНЫМИ КВАНТОВЫМИ СОСТОЯНИЯМИ

Евгений Василиу[1], Иван Гулаков[2], Андрей Зеневич[2], Александр Тимофеев[2], Сергей Николаенко[1]

[1] Одесская национальная академия связи им. А.С. Попова, Украина
[2]Учреждение образования «Высший государственный колледж связи», Беларусь

ВАСИЛИУ Евгений Викторович, д. т. н., доцент

Год и место рождения: 1966, Ялта, Крым, Украина.
Образование: Одесский государственный университет имени И. И. Мечникова, 1990.
Должность: директор Учебно-научного института «Радио, телевидения, электроники» с 2013 года.
Научные интересы: квантовая криптография, квантовые протоколы распределения ключей, квантовые протоколы прямой безопасной связи, помехоустойчивое кодирование для протоколов квантовой криптографии, квантовая стеганография.
Публикации: более 100 научных публикаций, среди которых 3 монографии, научные статьи, материалы конференций, патенты.
E-mail: vasiliu@ua.fm

ГУЛАКОВ Иван Романович, д. ф.-м. н., профессор

Год и место рождения: 1946, д. Костеничи, Мглинский р-н, Брянской обл., Российская Федерация.
Образование: Учреждение образования «Высший государственный колледж связи».
Должность: профессор кафедры математики и физики с 2006 года.
Научные интересы: фотоэлектронные процессы в фотоприемниках при одноквантовой регистрации, методы и техника регистрации сверхслабых оптических потоков.
Публикации: больше 150 научных публикаций, среди которых монографии, учебные пособия, научные статьи, патенты на изобретения.
E-mail: gulakov@bsu.by