***Проведено аналіз існуючих методів та підходів до побудови сучасних захищених інформаційно-комунікаційних систем та мереж в комерційних банках. Визначено переваги та недоліки методів, що розглядаються. Запропоновано підхід та методику модернізації існуючих мереж***

***Ключові слова: кібератака, інформаційно-комунікаційна система, комерційний банк, інформаційна безпека***

***Проведен анализ существующих методов и подходов к построению современных защищенных информационно-коммуникационных систем и сетей в коммерческих банках. Определены преимущества и недостатки методов, которые рассматриваются. Предложены подход и методика модернизации существующих сетей***

***Ключевые слова: кибератака, информационно-коммуникационная система, коммерческий банк, информационная безопасность***

УДК 004.05:519.81

# ПРОЕКТ МОДЕРНІЗАЦІЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ КОМЕРЦІЙНОГО БАНКУ НА БАЗІ ТЕХНОЛОГІЇ DYNAMIC MULTIPOINT VPN

**І.А. Пількевич**
Доктор технічних наук, професор, завідувач кафедри*
Контактний тел. (0412) 415-686, 067-397-87-39
E-mail: igor.pilkevich@mail.ru
**Н.М. Лобанчикова**
Кандидат технічних наук, доцент, доцент**
Контактний тел.: 093-652-61-64
E-mail: lobanchikovanm@rambler.ru
**В.І. Котков**
Кандидат технічних наук, доцент, доцент*
Контактний тел. (0412) 22-94-08
E-mail: eko_univer@i.ua
**І.В. Кравченко****
*Кафедра моніторингу навколишнього природного середовища
Житомирський національний агроекологічний університет
бул. Старий, 7, м. Житомир, Україна, 10008
**Кафедра безпеки інформаційних і комунікаційних систем
Житомирський військовий інститут ім. С.П. Корольова
Національного авіаційного університету
пр. Миру, 23, м. Житомир, Україна, 10004

## 1. Вступ. Постановка проблеми

Актуальність проблеми інформаційної безпеки комерційних банків визначається рядом взаємозв'язаних факторів, більшість з яких є наслідком процесу інформатизації сучасного суспільства. Однак, використання інформаційних технологій приховує в собі значні ризики, які потрібно постійно відстежувати та враховувати для мінімізації фінансових втрат. Фактично, дані ризики призводять до втрати конфіденційності, цілісності й доступності інформації, тобто, – до порушення інформаційної безпеки.

В основу інформаційної безпеки комерційного банку має бути покладено заходи та технології захисту інформації в засобах і мережах її передачі, обробки та зберігання. Крім того, необхідним є створення концепції безпеки банку, яка б регулювала порядок доступу, зберігання та використання банківської інформації. Розвиток інформаційних технологій створює передумови для пошуку нових методів та засобів захисту інформації в інформаційно-комунікаційних системах та мережах. Саме модернізації існуючих засобів захисту інформаційно-комунікаційної мережі (ІКМ) і присвячена дана стаття.

## 2. Огляд існуючих рішень

На сьогоднішній день, для забезпечення інформаційної безпеки мережі, використовуються методи тунелювання та шифрування трафіку [1-4]. Тунелювання, як і шифрування, слід розглядати як самостійний сервіс безпеки. Його суть полягає в тому, щоб „упакувати" передану порцію даних, разом зі службовими полями, в новий „конверт". Даний сервіс може застосовуватися для кількох цілей:

– здійснення переходу між мережами з різними протоколами (наприклад, IPv4 і IPv6);

– забезпечення конфіденційності і цілісності всієї переданої порції, включаючи службові поля.

Тунелювання може застосовуватися як на мережевому, так і прикладному рівнях. Комбінація тунелювання і шифрування (з необхідною криптографічного інфраструктурою) на виділених шлюзах дозволяє реалізувати такий важливий метод захисту ІКМ, як віртуальні шифровані мережі „поверх" глобальної мережі Internet. Такі мережі істотно дешевші та набагато безпечніші, ніж власні мережі організації, побудовані на виділених каналах. Сучасні протоколи, спрямовані на підтримку класів обслуговування, допоможуть га-

рантувати для віртуальних приватних мереж задану пропускну здатність, величину затримок тощо, ліквідуючи тим самим єдину, на сьогодні, реальну перевагу власних корпоративних мереж.

Традиційний підхід до побудови подібних мереж за допомогою простого шифрування трафіку методом IPsec в тунельному режимі, в тому числі з використанням технології VPN Site-to-Site, є вкрай неефективним (маються на увазі складності налаштувань, неможливість використання динамічних протоколів маршрутизації та дуже погана масштабованість) [3-5]. Додавання нових „сторін" в таких мережах часто вимагає переналаштувань всіх вузлів мережі, коригування величезного числа ACL, статичних маршрутів.

Збільшення кількості кіберзлочинів підвищує вимоги до захищеності комп'ютерних мереж і систем банку. Тому досить актуальними є знайдення нових методів, засобів та інформаційних технологій для підвищення захищеності інформаційно-комунікаційних систем банків.

*Метою статті* є проведення аналізу методів, засобів та технологій модернізації підсистеми захисту інформаційно-комунікаційної системи комерційного банку.

## 3. Основний частина

Проведений аналіз інформаційно-комунікаційних систем комерційних банків України показав, що особливої уваги та захисту потребує саме підсистема захисту ІКМ.

Також, огляд існуючих традиційних методів та засобів захисту виявив низку недоліків, які повинні бути вирішені розробленим проектом.

Для усунення виявлених недоліків проектом модернізованої ІКМ пропонується використовувати технологію багатоточкової віртуальної приватної мережі (DMVPN – Dynamic Multipoint VPN), що технологія базується на наступних базових принципах:

– використання віртуальної підмережі на базі mGRE-інтерфейсів;

– шифрування GRE трафіку за допомогою IPsec;

– використання протоколу NHRP;

– використання протоколів динамічної маршрутизації.

Multipoint GRE (mGRE) тунель є альтернативою GRE-тунелів „точка-точка", який дозволяє зосередити на собі кілька GRE-тунелів. Тунель mGRE дозволяє одному GRE-інтерфейсу підтримувати кілька IPsec-тунелів і спрощує кількість і складність налаштувань, в порівнянні з GRE-тунелями „точка-точка". Крім того, mGRE-інтерфейс дозволяє використовувати динамічно призначені IP-адреси на spoke-маршрутизаторах. Основна мета побудови мережі на базі віртуальних інтерфейсів GRE – отримати можливість використовувати протоколи динамічної маршрутизації для поширення інформації про маршрути та здійснення відмовостійкості.

Шифрування GRE пакетів, що проходять, реалізовано за допомогою IPsec. Критерій шифрування – присутність GRE заголовка. Особливостями профілю IPSec при налаштуванні багатоточкової віртуальної приватної мережі наступні:

– застосовується на тунельному інтерфейсі;

– після застосування будь-який трафік, що виходить з тунельного інтерфейсу, ініціює створення IPsec-тунелю (немає необхідності використовувати ACL, як у звичайній crypto map);

– source і destination адреси тунельного інтерфейсу використовуються для створення IPsec-тунелю.

Використання багатоточкової віртуальної приватної мережі передбачає функціонування Next Hop Resolution Protocol (NHRP) – клієнт-серверного протоколу перетворення адрес, що дозволяє всім хостам, які знаходяться в NBMA (Non Broadcast Multiple Access)-мережі, динамічно вивчити NBMA-адреси (фізичні адреси) один-одного, звертаючись до next-hop-серверу (NHS). Після цього хости можуть обмінюватися інформацією безпосередньо один з одним.

У модернізованій інформаційно-комунікаційній мережі DMVPN виконуються наступні дії:

1. Hub-маршрутизатор зберігає та обслуговує базу даних NHRP, в якій зберігаються відповідності між фізичними адресами та адресами mGRE-тунелів spoke-маршрутизаторів.

2. Hub-маршрутизатор буде працювати як NHS, а spoke-маршрутизатори будуть клієнтами.

3. На кожному spoke-маршрутизаторі hub-маршрутизатор статично вказаний як NHS, задано відповідність між фізичною адресою та адресою mGRE-тунелю hub-маршрутизатора.

4. При включенні кожен spoke-маршрутизатор реєструється на NHS і, при необхідності, може вимагати у сервера інформацію про адреси інших spoke-маршрутизаторів для побудови spoke-to-spoke тунелів.

В результаті можна виділити наступні переваги технології DMVPN:

– простота та наочність налаштування;

– ефективна масштабованість;

– динамічна відмовостійкість і тонке управління маршрутизацією на базі протоколу динамічної маршрутизації;

– працездатність multicast;

– повноцінна повнозв'язкова топологія з точки зору передачі даних при помірному обсязі службового трафіку;

– spoke-маршрутизатори можуть знаходитися за NAT і мати динамічні IP адреси з private діапазону.

ІКМ було спроектовано у середовищі програмного емулятора GNS3 засобами візуального проектування на базі обладнання Cisco. Вона складається з центрального маршрутизатора (hub-маршрутизатора), трьох spoke-маршрутизаторів, п'яти комутаторів та семи робочих станцій VPCS.

Роль середовища Інтернет виконує Frame Relay switch. Для емуляції було використано образ маршрутизатора „c2691-advipservicesk9-mz.124-15.T6". Схема мережі наведена на рис. 1. Умовно дана частина загальної мережі представляє собою Центральний офіс та 3 регіональні відділення певного комерційного банку „XXX".

Налаштування багатоточкової віртуальної приватної мережі складається з наступних кроків:

– налаштування протоколу IPSec;

– налаштування mGRE-тунелів;

– налаштування протоколу NHRP;

– налаштування динамічної маршрутизації.

Налаштування протоколу IPSec відбувається в два етапи. Перший етап – налаштування IKE, тобто створення політики безпеки isakmp. Другий етап – налаштування IPSec-профілю.

Так як налаштування протоколу IPSec на всіх маршрутизаторах ідентичні, розглянемо команди даних налаштувань на прикладі центрального маршрутизатора R_HUB.

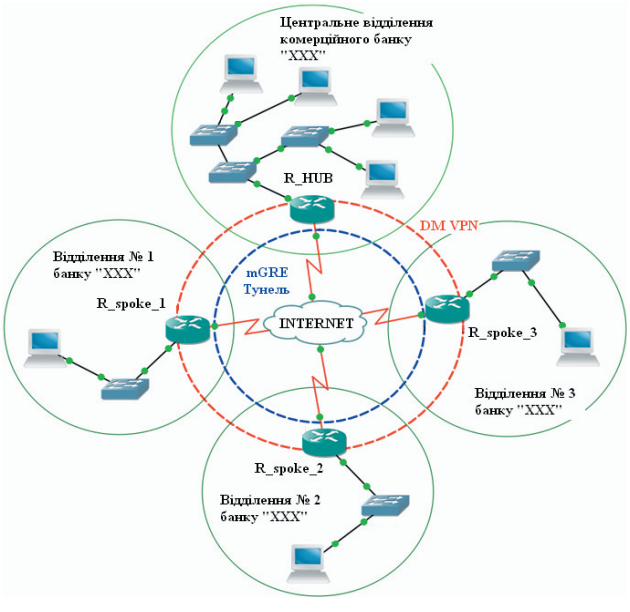


Рис. 1. Схема модернізованої захищеної мережі, побудованої в середовищі GNS3

Налаштування центрального маршрутизатора R_HUB:

*R_HUB(config)#crypto isakmp policy 10* – створення політики isakmp;

*R_HUB(config-isakmp)#encryption aes 192* – вказується, що в якості алгоритму шифрування використовується AES 192 біт;

*R_HUB(config-isakmp)#hash md5* – вказується, що в якості хеш-алгоритму використовується алгоритм MD5 ГОСТ Р 34.11-94 HMAC;

*R_HUB(config-isakmp)#authentication pre-share* – команда для вказівки, що аутентифікація повинна виконуватися по попередньо встановлених ключах;

*R_HUB(config-isakmp)#group 2* – встановлення групи Diffie-Hellman, що буде використовуватися в межах протоколу IKE, рівної 1024 біт;

*R_HUB(config)#crypto isakmp key 0 ISA-KEY address 0.0.0.0 0.0.0.0* – команда, що вказує шаблонну адресу при налаштуванні pre-share key;

*R_HUB(config)#crypto ipsec transform-set DMVPN-TRANS-SET esp-aes 256 esp-md5-hmac* – формування 2 наборів перетворень (комбінацій протоколів захисту та криптографічних алгоритмів) esp-aes-256 (протокол ESP з 256-бітним алгоритмом AES) та esp-md5-hmac (протокол ESP з алгоритмом аутентифікації MD5 ГОСТ Р 34.11-94 HMAC);

*R_HUB(config)#crypto ipsec profile DMVPN-PROFILE* – створення IPSec-профілю;

*R_HUB(config-profile)#set security-association lifetime seconds 120* – встановлення часу життя асоціації захисту (SA) рівної 120 секунд;

*R_HUB(config-profile)#set transform-set DMVPN-TRANS-SET*– призначення сформованих наборів перетворень даному IPSec-профілю.

Переходимо до налаштування mGRE-тунелів. На центральному маршрутизаторі та на spoke-маршрутизаторах mGRE-тунелі налаштовуються аналогічно, тому далі наведено основні команди налаштування та їх коментар на прикладі маршрутизатора R_HUB:

*R_HUB(config)#int tunnel 0* – створення тунельного інтерфейсу;

*R_HUB(config-if)#ip address 11.83.10.1 255.255.255.0* – призначення IP-адреси інтерфейсу;

*R_HUB(config-if)#ip mtu 1440* – збільшення значення MTU до 1440, так як GRE додає додаткові заголовки до IP-пакету;

*R_HUB(config-if)#tunnel source s1/0* – налаштування відповідності між тунельним та фізичним інтерфейсами;

*R_HUB(config-if)#tunnel mode gre multipoint* – включення mGRE тунелю;

*R_HUB(config-if)#tunnel key 0* – задання ключа, який ідентифікує тунель.

Налаштування протоколу NHRP на hub-маршрутизаторі та на spoke-маршрутизаторах мають певні відмінності між собою. Спочатку розглянемо команди налагодження NHRP на прикладі R_ HUB (hub-маршрутизатора):

*R_HUB(config)#int tunnel 0* – перехід на тунельний інтерфейс;

*R_HUB(config-if)#ip nhrp network-id 1* – увімкнення протоколу NHRP шляхом призначення унікального ідентифікатора мережі;

*R_HUB(config-if)#ip nhrp map multicast dynamic* – налаштування автоматичного додавання відповідностей між адресами spoke-маршрутизаторів;

*R_HUB(config-if)#ip nhrp authentication ISA-KEY* – налагодження аутентифікації.

Далі, на прикладі маршрутизатора R_spoke_1, наведемо команди налаштування протоколу NHRP на spoke-маршрутизаторі:

*R_spoke_1(config)#int tunnel 0* – перехід на тунельний інтерфейс;

*R_spoke_1(config-if)#ip nhrp network-id 1* – увімкнення протоколу NHRP шляхом призначення унікального ідентифікатора мережі. Вказується той самий ідентифікатор, що і на hub-маршрутизаторі;

*R_spoke_1(config-if)#ip nhrp map multicast dynamic* – налаштування динамічної побудови карти відповідностей між адресами spoke-маршрутизаторів;

*R_spoke_1(config-if)# ip nhrp map 11.83.10.1 10.83.10.1* – налагодження статичної відповідності між адресою mGRE-тунелю і фізичною адресою hub-маршрутизатора (перша адреса – адреса тунельного інтерфейсу, друга – адреса зовнішнього фізичного інтерфейсу);

*R_spoke_1(config-if)#ip nhrp map multicast 10.83.10.1* – адреса зовнішнього фізичного інтерфейсу hub-маршрутизатора вказується як одержувач multicast-пакетів від локального маршрутизатора;

*R_spoke_1(config-if)# ip nhrp nhs 11.83.10.1* – адреса тунельного інтерфейсу hub-маршрутизатора вказується як next-hop-сервер.

Останнім етапом налаштування багатоточкової віртуальної приватної мережі є забезпечення динамічної маршрутизації.

У якості протоколу маршрутизації було обрано протокол EIGRP. Для прикладу нижче наведемо команди налаштування маршрутизації по протоколу EIGRP на hub-маршрутизаторі R_HUB:

*R_HUB(config)#router eigrp 10* – перехід в режим налагодження протоколу маршрутизації;

*R_HUB(config-router)#passive-interface default* – подавлення маршрутних оновлень на інтерфейсі, що стоїть за замовчуванням;

*R_HUB(config-router)#no passive-interface tunnel 0* – включення протоколу EIGRP на тунельному інтерфейсі;

*R_HUB(config-router)#network 11.83.10.0 0.0.0.25* – додавання в протокол маршрутизації мережі тунельних інтерфейсів;

*R_HUB(config-router)#network 190.168.8.0 0.0.3.255* – додавання в протокол внутрішньої мережі маршрутизатора;

*R_HUB(config-router)#no auto-summary* – відключення автоматичного сумування мереж;

*R_HUB(config- router)#int tunnel 0* – перехід на тунельний інтерфейс;

*R_HUB(config-if)#no ip next-hop-self eigrp 10* – відключення правила використання IP-адреси hub-маршрутизатора в якості next-hop для маршрутів, які він анонсує, навіть коли анонсує маршрути назад через той же інтерфейс, на якому вони були вивчені. Встановлюється вимога використовувати в якості next-hop IP-адреси spoke-маршрутизаторів;

*R_HUB(config-if)#no ip split-horizon eigrp 10* – відключення правила розщеплення горизонту (інакше EIGRP не буде анонсувати маршрути, вивчені через mGRE-інтерфейс назад в цей же інтерфейс).

Після того, як всі налаштування технології DM VPN виконані, переходимо безпосередньо до перевірки правильності функціонування захищеної інформаційно-комунікаційної мережі. Перевірка доступності вузлів мережі здійснювалася за допомогою команд ping[address] та tracert/traceroute[address]. На рис. 2 наведено результат роботи команди tracert з різних робочих станцій.

```
VPCS[7]> tracert 191.200.1.3
traceroute to 191.200.1.3, 64 hops max, press Ctrl+C to stop
 1   191.200.2.1   390.000 ms  234.000 ms  156.000 ms
 2   11.83.10.1    672.000 ms  *  500.000 ms
 3   11.83.10.2    468.000 ms  312.000 ms  282.000 ms

VPCS[2]> tracert 191.200.2.3
traceroute to 191.200.2.3, 64 hops max, press Ctrl+C to stop
 1   190.168.8.1   531.000 ms  531.000 ms  422.000 ms
 2     *  641.000 ms  218.000 ms
 3   11.83.10.3    672.000 ms  828.000 ms  484.000 ms

VPCS[2]> tracert 191.200.1.3
traceroute to 191.200.1.3, 64 hops max, press Ctrl+C to stop
 1   190.168.8.1   969.000 ms  265.000 ms  375.000 ms
 2     *  359.000 ms  422.000 ms
 3   11.83.10.2    734.000 ms  281.000 ms  *
```

Рис. 2. Перевірка доступності робочих станцій мережі

Для того, щоб побачити, що через тунель ідуть шифровані дані було здійснено перехоплення трафіку програмою-сніфером Wireshark (рис. 3).

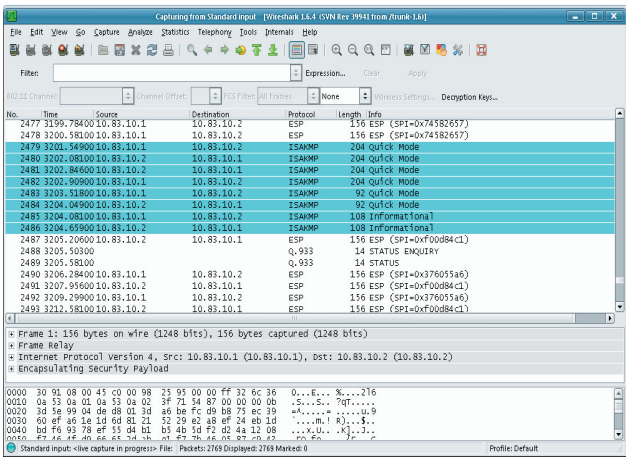

Рис. 3. Аналіз трафіку

В результаті аналізу трафіку видно, що дані циркулюють в мережі в шифрованому вигляді, що знижує імовірність їхнього несанкціонованого використання.

## 4. Висновок

Для побудови захищених інформаційно-комунікаційних мереж комерційних банків доцільно використовувати технологію багатоточкової віртуальної приватної мережі. Модернізацію інформаційно-комунікаційної мережі комерційного банку необхідно проводити на базі технології Dynamic multipoint VPN.

Література


1. Белов, Е.Б. Основы информационной безопасности: учебное пособие для студентов вузов [Текст] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.
2. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты [Текст] / В.В. Домарев.– К.: ООО „ТИД „ДС”, 2001. – 688 с.
3. Новіков, О.М. Безпека інформаційно-комунікаційних систем [Текст] / О.М. Новиков, М.В. Грайворонський.– К.: Видавнича група BHV, 2009. – 608 с.
4. Королев, М.И. Информационные системы в банковском деле: учебное пособие [Текст] / М.И. Королев, Д.М. Королев. – Белгород: Издательство БелГУ, 2004. – 330 с.
5. Гамза, В. А. Безопасность банковской деятельности [Текст] / В.А. Гамза, И.Б. Ткачук. – Маркет ДС, 2006. – 422 с.



***Abstract***

*The dynamic development of information security sphere constantly puts new demands on the creation of secure communication and information systems and networks in commercial banks. The information security of the commercial bank should be based on activities and technologies of information protection in the tools and networks of its transfer, processing and storage.*

*The article analyzes the famous methods, approaches and technologies of creation of information and commu-*

*nication systems and networks in commercial banks. As a result of examination of existing methods and means of protection a range of defects, which should be eliminated with the corresponding project, was determined. To eliminate the determined defects it was suggested to apply the technology of multipoint virtual private network (VPN). The advantages of the suggested technology are: simplicity and visualization of setting, effective scaling, dynamic routing management, high operability, full-grown connected topology in terms of data transfer at a moderate volume of service traffic.*

*Information and communication network has been designed in the software emulator GNS3 with the help of visual designer Cisco. The article represents a test example of circuit of protected information and communication network with Dynamic multipoint VPN technology*

***Keywords**: cyber attack, information and communications system, commercial bank, information security*

***У статті представлені результати досліджень впливу параметрів геометрії контролю при радіометричному митному огляді з метою виявлення напрямку подальшої модернізації пошукових приладів, використовуючих метод зворотно розсіяного гамма-випромінювання***

***Ключові слова: контрастна зліченість, зворотно-розсіяне випромінення, геометрія контролю, інтенсивність випромінення, оглядовий контроль***

***В статье представлены результаты исследований влияния параметров геометрии контроля при радиометрическом таможенном досмотре с целью определения направления дальнейшей модернизация поисковых приборов, использующих метод обратно рассеянного гамма-излучения***

***Ключевые слова: контрастная счетность, обратно рассеянное излучение, геометрия контроля, интенсивность излучения, досмотровый контроль***

УДК 539.12.04

# ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ КОНТРАСТНОЙ СЧЕТНОСТИ ОТ ГЕОМЕТРИИ КОНТРОЛЯ ПРИ РАДИОМЕТРИЧЕСКОМ ТАМОЖЕННОМ ДОСМОТРЕ

**К.С. Гаврилов**
Младший научный сотрудник
Научно-исследовательский проектно-конструкторский институт "Искра"
ул. Звейнека, 145с, г. Луганск, Украина, 91033
Контактный тел.: (0642) 71-75-92
E-mail: oficial@iskra.lg.ua

## 1. Введение. Актуальность

Одной из основных задач при таможенном досмотре является обеспечение высокой эффективности контроля транспортных средств на предмет незаконного ввода запрещенных товаров и контрабанды при повышении пропускной способности контроля [1]. При этом необходимо обеспечить неразборность объектов контроля, также нередко встречаются ситуации, когда доступ к объекту контроля со всех сторон невозможен, следовательно, необходимо обеспечить односторонний досмотровой контроль объектов.

Проведенный в [2] сравнительный анализ показал, что наиболее перспективными для решения поставленной задачи являются приборы, использующие метод регистрации обратно-рассеянного гамма-излучения, которые имеют преимущество по глубине сканирования, обеспечивают контроль объектов, в том числе с односторонним доступом, имеющих сложную форму и конструкцию и изготовленных из различных материалов. В приборах такого класса для детектирования гамма-излучения широко применяется счетный режим, а обнаружение закладки обусловлено вариациями плотности исследуемого объекта. Об изменении плотности объекта, а, следовательно, и о наличии закладки, можно судить по изменению интенсивности обратно-рассеянного гамма-излучения. Т.е. при принятии решения о наличии или отсутствии закладки необходимо учитывать изменение (увеличение или уменьшение) скорости счета импульсов, или разность счета, значение которой зависит от активности источника ионизирующего излучения (ИИИ) и геометрии контроля.