УДК 004.72, 004.772

С. Н. ПЕТРОВ, Д. В. АХРАМЕНКО, С. М. ГОРОШКО, Т. А. ПУЛКО

РАЗГРАНИЧЕНИЕ ДОСТУПА В ЛОКАЛЬНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ БАЗОВЫХ НАСТРОЕК СЕТЕВОГО ОБОРУДОВАНИЯ

Белорусский государственный университет информатики и радиоэлектроники

Целью работы являлась разработка рекомендаций по защите локальной сети предприятия от несанкционированного доступа сотрудников (инсайдерских атак) на основе разграничения доступа, с использованием базовых настроек имеющегося оборудования. Предлагается использование профилей доступа на основе MAC-адресов (MAC-based Access Control). Рассмотрены проблемы защиты информации на физическом и канальном уровнях, а также наиболее распространенные типы атак. Дано описание, созданной для целей исследования, натурной модели локальной сети организации гостиничного бизнеса, включающей персональные компьютеры, модем ZTE ZXHN H208N с поддержкой функций WiFi-точки доступа и коммутатор DES-1210-52, который обеспечивал объединение указанных устройств в сеть.

Произведено контактное подключение к витой паре с использованием зажимов типа «крокодил» на линиях Tx и Rx. В качестве инструмента для тестирования на проникновение использовался ноутбук с дистрибутивом Kali Linux, утилита tcpdump, фреймворк bettercap, анализатор трафика Wireshark. Был рассмотрен вариант проведения сетевой атаки ARP-spoofing с базовыми настройками сетевого оборудования. Приведены результаты атаки и пассивного исследования модели сети. Рассмотрен вариант повторной атаки после активации и настройки функций привязки IP- и MAC-адресов (IP-MAC-Port Binding), а также аутентификации пользователей на основе стандарт IEEE 802.1X (MAC-Based 802.1X). Результаты доказали действенность выбранных мер защиты.

Ключевые слова. *Информационная безопасность; тестирование на проникновение; анализ сетевого трафика; инсайдерские атаки; разграничение доступа, ARP-spoofing.*

Введение

Согласно результатам исследования аналитического центра InfoWatch [1], в 2016 году центром было зарегистрировано 1556 случаев утечки конфиденциальной информации. В 61,8% случаях утечка информации произошла вследствие действий внутренних нарушителей, 33,9% из которых являлись действующими или бывшими (2,1%) сотрудниками организаций. На сетевой канал пришлось 69,5% зафиксированных утечек, причем подавляющее число случаев компрометации данных (более 90%) носило намеренный характер. Учитывая данные исследований компании InfoWatch, следует уделять внимание вопросам подбора новых сотрудников и контроля уже существующих, среди которых могут оказаться психологически слабые люди, таящие обиду на начальство. Так же стоит учитывать конкурентов, которые подкупают людей, в особенности системных администраторов, для организации утечки информации.

Организации не всегда располагают денежными ресурсами на покупку лицензионного программного обеспечения, антивирусной защиты, межсетевых экранов актуального сетевого оборудования, не говоря о специализированных решениях на подобии систем управления учетными данными (IdM), систем предотвращения утечек конфиденциальной информации (DLP), систем анализ событий безопасности (SIEM) [2].

Целью работы являлось разработка рекомендаций по защите локальной сети предприятия с использованием базовых настроек имеющегося оборудования (без покупки специальных систем и средств) от несанкционированного доступа сотрудников (инсайдерских атак) на основе разграничения доступа. Разграничение прав доступа пользователей сети,

Рис. 1. Некорректно выполненный монтаж кабельной сети

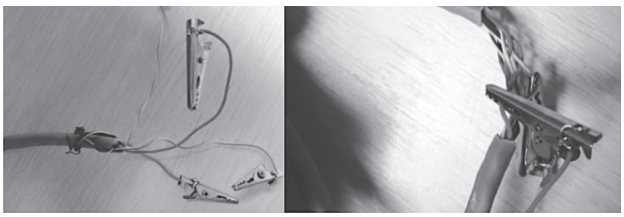


Рис. 2. Контактное подключение к витой паре

это настройки, связанные с сегментированием ЛВС-структуры на отдельные части и определение правил взаимодействия этих частей друг с другом. Предлагается использование профилей доступа на основе MAC-адресов (MAC-based Access Control).

Проблемы защиты информации на канальном уровне

Структурированная кабельная система предприятия охватывает все пространство здания, соединяет все средства передачи информации, такие как компьютеры, рабочие станции, сетевое оборудование, сервера, а так же включает в себя датчики пожарной и охранной сигнализации, видеокамеры системы видеонаблюдения, считыватели и контроллеры контроля доступа, телефонию. Все коммутационные узлы специальными магистралями объединяются в коммутационном центре здания. Сюда же подводятся внешние кабельные магистрали для подключения здания к глобальным информационным ресурсам, таким как телефония, интернет и т. п. [3].

В нормативной базе Республики Беларусь четко определены нормы и требования по монтажу систем безопасности, однако требования по монтажу локальных сетей проработаны менее детально. Кабельные коммуникации не всегда прокладываются с учетом требований безопасности, при этом подключение к сетевым коммуникациям может быть получено с минимальными усилиями (рис. 1).

Объектом исследования является предприятие гостиничного бизнеса, а именно кабельная структурированная система предприятия, включающая системы видеонаблюдения и контроля доступа, а также локальную сеть. Информацией ограниченного доступа являются: персональные данные посетителей; данные кредитных карт; данные о разработках; бухгалтерская информация; иные документы для служебного пользования.

Для исследовательских целей была создана натурная модель локальной сети, включающая персональные компьютеры, модем ZTE ZXHN H208N с поддержкой функций WiFi-точки доступа и коммутатора DES-1210-52, который обеспечивал объединение указанных устройств в сеть.

Произведено контактное подключение к витой паре с использованием зажимов типа «крокодил» на линии Tx и Rx (рис. 2). В качестве инструмента для тестирования на проникновение использовался ноутбук с дистрибутивом Kali Linux [4], утилита tcpdump, фреймворк bettercap, анализатор трафика Wireshark.

Наиболее возможными атаками внутри локальной сети предприятия являются: подмена DHCP-сервера, отказ в обслуживании DoS (часто используют совместно с подменой DHCP-сервера), разновидности атак типа «человек посередине» (например ARP-spoofing), неавторизованный доступ. Для проведения такого рода атак можно использовать миниатюрные одноплатные компьютеры Raspberry Pi с уста-

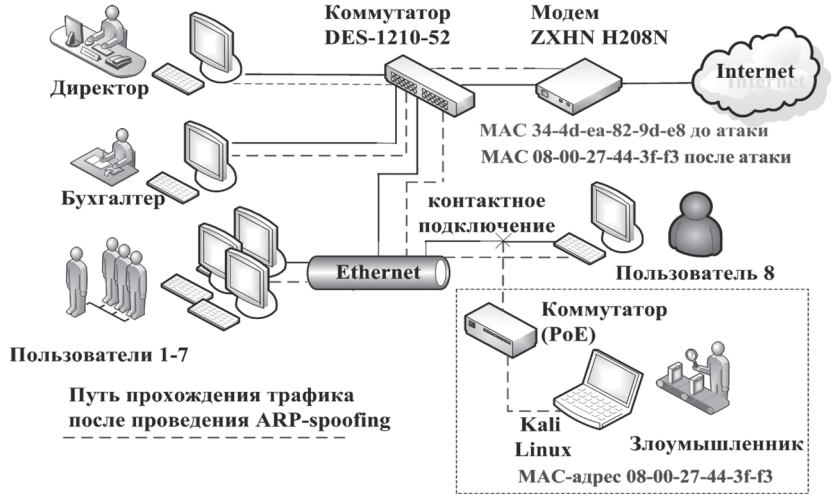


Рис. 3. Схема проведения атаки ARP-spoofing

Интерфейс: 192.168.1.130 --- 0xc

адрес в Интернете	Физический адрес	Тип
192.168.1.1	34-4d-ea-82-9d-e8	динамический
192.168.1.3	94-de-80-09-08-1c	динамический
192.168.1.5	08-00-27-44-3f-f3	динамический
192.168.1.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический

а

Интерфейс: 192.168.1.130 --- 0xc

адрес в Интернете	Физический адрес	Тип
192.168.1.1	08-00-27-44-3f-f3	динамический
192.168.1.3	94-de-80-09-08-1c	динамический
192.168.1.5	08-00-27-44-3f-f3	динамический
192.168.1.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический

б

Рис. 4. ARP-таблица жертвы: *а* – до проведения атаки; *б* – после проведения атаки

новленным дистрибутивом Kali Linux, ЖКИ дисплеем, коммутатором и питанием от аккумуляторной батареи или через PoE-сплиттер (Power over Ethernet, обеспечивает питание по сети Ethernet) [5].

Пассивный анализ сети [6], заключающийся в анализе трафика, сборке пакетов, исходящих от узлов сети для определения их составляющих, активных соединений, работающих протоколов, используемых портов, позволил получить список посещенных пользователем web-ресурсов. В случае если передаваемый в сети трафик не шифруется (использование http или ftp протоколов), то с помощью анализатора сети можно получить логины и пароли от коммутирующего оборудования. Пассивный анализ сети является весьма распространенным методом для определения топологи и построения карт сети, а также определения операционной системы, установленной на исследуемом хосте, посредством стека протоколов TCP/IP.

В случае несанкционированного подключения к сети видеонаблюдения можно получать изображение, логины и пароли непосредственно от видеокамер и серверов видеоаналитики, так как для передачи видео часто используются протоколы без шифрования, а логины и пароли передаются по протоколу http. В случае подключения к системе контроля доступа злоумышленник может получить доступ к серверам и управлять физическими точками доступа, а именно отключить важные точки прохода.

Результаты тестирования натурной модели сети

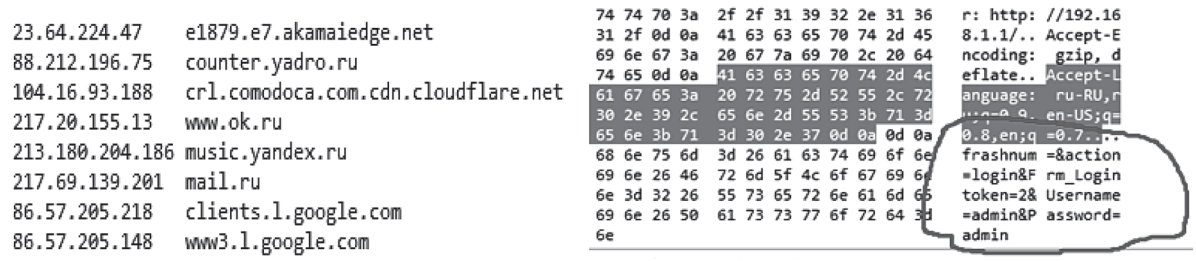
В качестве примера «активного исследования» сети рассмотрим результат проведения атаки на канальном уровне типа Man In The Middle, а именно ARP-spoofing [7].

Модель сети и схема проведения атаки приведена на рис. 3.

На рис. 4 приведены ARP-таблицы жертвы: *а* – до проведения атаки *б* – после проведения атаки

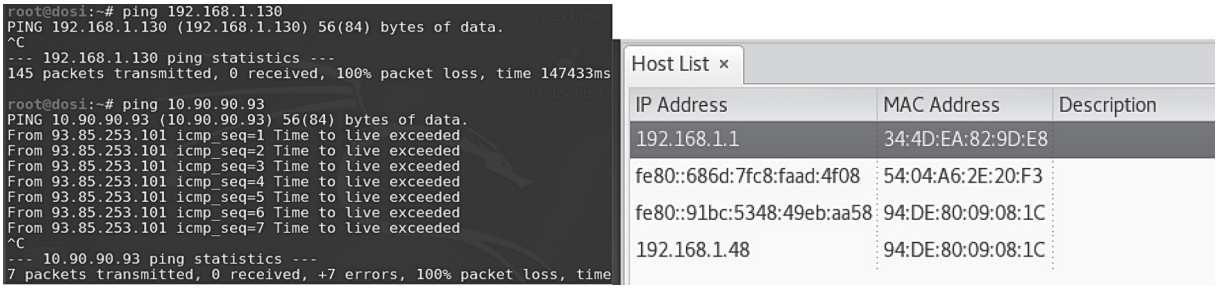
Из рисунка видно, что в процессе атаки начальный MAC-адрес модема 34-4d-ea-82-9d-e8 был изменен на 08-00-27-44-3f-f3. После проведения атаки в сети появились 2 машины с одинаковым MAC-адресом 08-00-27-44-3f-f3 и различными IP-адресами 192.168.1.1 (модем) и 192.168.1.5 (злоумышленник).

Используя сетевой анализатор трафика Wireshark можно просматривать действия жертвы в сети (рис. 5), например, просмотреть список



а *б*

Рис. 5. Анализ поведения жертвы в сети: а) список посещенных пользователем web-ресурсов, б) логины и пароли от коммутационного оборудования



а *б*

Рис. 6. Результаты повторной атаки ARP-spoofing: *а* – выполнение команды ping между злоумышленником и жертвой; *б* – список хостов отображенных в bettercap

посещенных пользователем web-ресурсов (рис. 5, *а*), извлечь логины и пароли от коммутационного оборудования (рис. 5, *б*).

Настройка функций безопасности на сетевом оборудовании

В некоторых случаях коммутаторы могут значительно ослабить угрозы информационной безопасности. Ниже перечислены решения, рекомендуемые к использованию для снижения вероятности утечки конфиденциальной информации на базе оборудования D-Link [8].

Функция IP-MAC-Port Binding (IMPB) разработана для управления подключением узлов в офисных и ETTH-сетях (Ethernet To The Home). Позволяет контролировать доступ компьютеров в сеть на основе анализа их IP- и MAC-адресов и порта подключения, таким образом, позволяет бороться с атаками типа ARP-spoofing.

Механизм действия IMPB позволяет пользователям получать доступ к сети в случае совпадения MAC- и IP-адреса компьютера, портов подключения коммутатора с «белым» списком, созданным администратором сети (режим работы ARP mode). В случае если указанные выше параметры отличаются от внесенных в список, коммутатор блокирует MAC-адрес соответствующего узла и заносит его в «черный» список (с отметкой Drop).

Для проверки эффективности IMPB был создан «белый» список, после чего проведены манипуляции с Kali Linux, аналогичные описанным выше. Результаты повторной атаки ARP-spoofing приведены на рис. 6. Результат выполнения команды ping между злоумышленником и жертвой (рис. 6, *а*), список хостов отображенных в bettercap (рис. 6, *б*).

Из рис. 6 видно, что после активации и настройки IP-MAC-Port Binding, злоумышленник не может подключиться к хосту жертвы и провести атаки типа ARP-spoofing.

Стандарт IEEE 802.1X позволяет контролировать доступ и не позволять неавторизованным устройствам подключаться к локальной сети через порты коммутатора. Коммутаторы D-Link поддерживают две версии реализации этого стандарта: Port-Based 802.1X и MAC-Based 802.1X. Для развертывания системы аутентификации 802.1X необходим сервер аутентификации RADIUS, коммутатор с поддержкой стандарта и настройка протокола EAP (Extensible Authentication Protocol) на целевом компьютере.

Помимо использования функции IP-MAC-Port Binding, в числе предлагаемых мер по защиты от ARP-spoofing предлагается использовать статические ARP-таблицы на ключевых узлах, а также IP-адрес с маской и DNS. Также

предлагается разделение локальной сети на несколько виртуальных сетей (VLAN), так как в случае, когда VLAN состоит из одного компьютера, проведение атаки становится невозможным.

Заключение

Вопрос обеспечения конфиденциальности и доступности данных, передаваемых по сетям предприятий, по-прежнему остаются актуальными. Этому способствуют простота несанкционированного подключения к локальной сети в совокупности с доступностью в открытом доступе богатого инструментария для пентестинга, например Kali Linux с набором утилит, анализаторы трафика типа Wireshark, а также методических материалов по тестированию (проведению атак в том числе). Используя снифферы, можно анализировать списки посещенных URL и хостов HTTP/S, данные, отправленные методом POST, куки и прочие учетные данные. Настройка функций безопасности маршрутизаторов и коммутаторов снижает вероятность проведения сетевых атак, что продемонстрировано на примере оборудования D-Link, которое было атаковано посредством ARP-spoofing.

ЛИТЕРАТУРА

1. **Глобальное** исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс]: Аналитический центр InfoWatch. 2017. Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_global_report_2014.pdf. – Дата доступа: 10.04.2018.

2. **Обзор** мирового и российского рынка SIEM-систем 2017 [Электронный ресурс]: Анастасия Сапрыкина, обозреватель Anti-Malware.ru. 2017. Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem#. – Дата доступа: 10.04.2018.

3. **Информационные** технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования: ГОСТ Р 53246–2008 – Введ. – 25.12.2008. – Москва: Стандартинформ, 2009. – 72 с.

4. **Kali** Linux Revealed. Mastering the Penetration Testing Distribution [Электронный ресурс]: Raphaël Hertzog, Jim O'Gorman, Mati Aharoni. 2017. Режим доступа: https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf/. – Дата доступа: 10.04.2018.

5. **Пять** шагов, чтобы построить портативную станцию хакера из Raspberry Pi и Kali Linux [Электронный ресурс]. – Режим доступа: http://infoweb.org.ua/portativnuyu-stantsiyu-hakera-iz-raspberry-pi-i-kali-linux. – Дата доступа: 10.04.2018.

6. **Пассивный** анализ сети [Электронный ресурс]: Stephen Barish. 2008. Режим доступа: https://www.securitylab.ru/analytics/350448.php. – Дата доступа: 10.04.2018.

7. **ARP-spoofing** в Kali Linux [Электронный ресурс]. – Режим доступа: https:// defcon.ru/network-security/3731/. – Дата доступа: 10.04.2018.

8. **D-Link** DES-3028/DES-3028P/DES-3052/DES-3052P Управляемые коммутаторы 10/100Мбит/ с Fast Ethernet Версия I [Электронный ресурс]: Руководство пользователя. 2007. Режим доступа: http://ftp.dlink.ru/pub/Switch/DES-3028-3052/Description/DES-3028_28P_52_52P_Manual_v1_01_RUS.pdf/. – Дата доступа: 10.04.2018.

REFERENCES

1. **Global'noe** issledovanie utechek konfidencial'noj informacii v 2016 godu [Jelektronnyj resurs]: Analiticheskij centr InfoWatch. 2017. Rezhim dostupa: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_global_report_2014.pdf. – Data dostupa: 10.04.2018.

2. **Obzor** mirovogo i rossijskogo rynka SIEM-sistem 2017 [Jelektronnyj resurs]: Anastasija Saprykina, obozrevatel' Anti-Malware.ru. 2017. Rezhim dostupa: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem#. – Data dostupa: 10.04.2018.

3. **Informacionnye** tehnologii. Sistemy kabel'nye strukturirovannye. Proektirovanie osnovnyh uzlov sistemy. Obshhie trebovanija: GOST P 53246-2008 – Vved. – 25.12.2008. – Moskva: Standartinform, 2009. – 72 s.

4. **Kali** Linux Revealed. Mastering the Penetration Testing Distribution [Jelektronnyj resurs]: Raphaël Hertzog, Jim O'Gorman, Mati Aharoni. 2017. Rezhim dostupa: https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf/. – Data dostupa: 10.04.2018.

5. **Pjat' shagov,** chtoby postroit' portativnuju stanciju hakera iz Raspberry Pi i Kali Linux [Jelektronnyj resurs]. – Rezhim dostupa: http://infoweb.org.ua/portativnuyu-stantsiyu-hakera-iz-raspberry-pi-i-kali-linux. – Data dostupa: 10.04.2018.

6. **Passivnyj** analiz seti [Jelektronnyj resurs]: Stephen Barish. 2008. Rezhim dostupa: https://www.securitylab.ru/analytics/350448.php. – Data dostupa: 10.04.2018.

7. **ARP-spoofing** v Kali Linux [Jelektronnyj resurs]. – Rezhim dostupa: https://defcon.ru/network-security/3731/. – Data dostupa: 10.04.2018.

8. **D-Link** DES-3028/DES-3028P/DES-3052/DES-3052P Upravljaemye kommutatory 10/100Мбит/с Fast Ethernet Version I [Jelektronnyj resurs]: Rukovodstvo pol'zovatelja. 2007. Rezhim dostupa: http://ftp.dlink.ru/pub/Switch/DES-3028-3052/Description/DES-3028_28P_52_52P_Manual_v1_01_RUS.pdf/. – Data dostupa: 10.04.2018.

Поступила *05.05.2018* | *После доработки* *16.08.2018* | *Принята к печати* *31.08.2018*

S. N. Petrov, D. V. Ahramenko, S. M. Goroshko, T. A. Pulko

ACCESS CONTROL IN A LOCAL NETWORK USING THE BASIC CONFIGURATION OF NETWORK DEVICES

The Belarusian State University of Informatics and Radioelectronics

The article focused on recommendations for the local network protection from unauthorized access of employees (insider attacks) on the basis of access control, using the basic settings of existing equipment. The use of MAC-based access profiles (MAC-based Access Control) is proposed. The problems of information security at the physical and channel levels, as well as the most common types of attacks are considered. For research purposes, a mockup of a typical local area network was created, including personal computers, ZTE ZXHN H208N modem with support WiFi-access point and the switch DES-1210-52, which connected these devices to the network.

Made contact connection to the twisted-pair with clips on the lines Tx and Rx. Kali Linux, tcpdump, bettercap, Wireshark are using as a tools for penetration testing. The network attacks ARP-spoofing with the basic settings of network equipment is discussed. The results of the attack and passive study of the network model are presented. The attack was repeated after activation and configuration IP-MAC-Port Binding, as well as authentication of users based on IEEE 802.1 X standard (MAC-Based 802.1 X). The results proved the effectiveness of the chosen protective actions.

Keywords. *Information security; penetration testing; network traffic analysis; insider attacks; access control, ARP-spoofing.*

Петров Сергей Николаевич, кандидат технических наук, доцент, доцент кафедры защиты информации БГУИР. Область научных интересов: информационная безопасность.

220013, Республика Беларусь, Минск, ул. П. Бровки, 6, Белорусский государственный университет информатики и радиоэлектроники,

Тел: + 37517 2938558; E-mail: petrov@bsuir.by

Petrov Sergei Nikolaevich, Ph. D., Assoc. Prof., Associate Professor of Information Security department BSUIR. Scientific interests: information security.

Ахраменко Дмитрий Викторович, магистрант кафедры защиты информации БГУИР («Методы и системы защиты информации, информационная безопасность»). Окончил БНТУ по специальности «Техническое обеспечение безопасности». Область научных интересов: информационная безопасность, администрирование сетей и оптимизация.

E-mail: d.axramenko@mail.ru

Ahramenko Dmitriy Viktorovich, master student of Information Security department BSUIR («Methods and systems of information protection, information security»). Graduated from BNTU «Technical security». Scientific interests: information security, network administration and optimization.

Горошко Сергей Максимович, аспирант кафедры защиты информации БГУИР. Окончил БГУИР по специальности «Радиоэлектронные системы», магистратуру по специальности «Радиотехника, в том числе системы и устройства радиолокации, радионавигации и телевидения». Область научных интересов: информационная безопасность, цифровая обработка сигналов. E-mail: status7777777@mail.ru

Goroshko Sergei Maximovich, postgraduate student of BSUIR. Graduated from BSUIR «Radioelectronic systems», Master of Technical Sciences «Radio engineering, including systems and devices of radar, radio navigation and television». Scientific interests: information security, digital signal processing.

Пулко Татьяна Александровна, кандидат технических наук, доцент, доцент кафедры защиты информации БГУИР. Область научных интересов: информационная безопасность, радиопоглощающие покрытия.

220013, Республика Беларусь, Минск, ул. П. Бровки, 6, Белорусский государственный университет информатики и радиоэлектроники,

Тел: + 37517 2938558; E-mail: pulko@bsuir.by

Pulko Tatsiana Alexandrovna, Ph. D., Assoc. Prof., Associate Professor of Information Security department BSUIR. Scientific interests: information security, radio-absorbing coatings.