СПОСОБ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ РАЗЛИЧНЫХ УРОВНЕЙ КОНФИДЕНЦИАЛЬНОСТИ

Стародубцев Ю.И.[1], Бегаев А.Н.[2], Козачок А.В.[3]

Широкое использование сетей связи с различным уровнем конфиденциальности обрабатываемой информации требует использование новых принципов управления доступом. Существующие принципы управления имеют ряд недостатков, заключающихся в относительно низкой защищенности внутреннего сегмента сети, так как не учитывается прямое физическое и логическое соединение между разноуровневыми (по конфиденциальности) сегментами сети, а также дублируются средства защиты информации на каждом компьютере–клиенте при многопользовательском доступе к информационным ресурсам. Вследствие этого необходима разработка предложений, устраняющих указанные недостатки.

***Ключевые слова**: компьютерная сеть, мультисервисная сеть связи, защита информации, управление доступом, конфиденциальность информации.*

Введение

Развитие информационных технологий и необходимость обработки информации на рабочих станциях различного уровня конфиденциальности требует использование принципов управления, направленных на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [1].

Доступность информации является ключевым звеном, при котором субъекты, имеющие право доступа, могут реализовывать эти права беспрепятственно, в режиме реального времени, с заданной степенью защищенности от несанкционированного доступа. Доступность информации является одной из трех главных составляющих информационной безопасности, помимо конфиденциальности и целостности информации.

Анализ существующих способов управления доступом [2-6] показал, что существует противоречие между требованиями предъявляемыми пользователями мультисервисной сети связи по доступу к информации различного уровня конфиденциальности и возможностями системы защиты информации, по реализации разграничения доступа.

Постановка задачи на исследование

Для решения указанных противоречий разработан способ по управлению доступом к информационным ресурсам мультисервисных сетей связи различных уровней конфиденциальности, обеспечивающие повышение защищенности путем исключения прямого физического и логического соединения между разноуровневыми (по конфиденциальности) сегментами сети, сокращение количества средств защиты и времени реализации запроса на доступ к информационным ресурсам за счет использования дополнительной базы данных, в которой хранятся проверенные информационные ресурсы.

Поставленная задача достигается тем, что в заявленном способе принимают запрос от компьютера-клиента, анализируют запрос доступа в отношении, разрешено ли компьютеру-клиенту только просматривать Интернет-сайты или разрешено записывать информацию на Web-серверы, проверяют, разрешен или запрещен доступ к информационному ресурсу, запрещают или разрешают доступ к информационным ресурсам, заносят указатели URL на все информационные ресурсы с указанием их уровня конфиденциальности и

1 Стародубцев Юрий Иванович, доктор военных наук, профессор, Военная академия связи им. С.М.Будённого, Санкт-Петербург

2 Бегаев Алексей Николаевич, кандидат технических наук, ЗАО «Эшелон – Северо-Запад», Санкт-Петербург, a.begaev@nwechelon.ru

3 Козачок Александр Васильевич, кандидат технических наук, Академия ФСО России, г.Орел, alex.totrin@gmail.com

перечень имеющихся средств защиты информации с указанием видов доступа, при реализации которых требуется применение данных средств защиты информации, дополнительно проверяют содержится ли запрашиваемый ресурс в базе данных проверенных информационных ресурсов. Потом отключают выход модуля шлюзов и включают вход модуля шлюзов. Принимают запрашиваемую информацию в шлюз. После чего записывают принятую информацию в ячейки памяти ОЗУ шлюза и копируют принятую информацию в шлюзы по числу средств защиты информации. По завершении копирования отключают вход модуля шлюзов.

Одновременно всеми средствами защиты информации проверяют принятую информацию. При успешном завершении работы всех средств защиты информации включают выход модуля шлюзов. Записывают проверенную информацию в базу данных проверенных информационных ресурсов. Удаляют принятую информацию из шлюзов, если хотя бы одно из средств защиты информации завершило работу неуспешно.

Способ управления доступом к информационным ресурсам мультисервисных сетей связи различных уровней конфиденциальности

Реализация заявленного способа поясняется рисунком 1 и заключается в выполнении следующей последовательности действий:

Пользователь компьютера-клиента 1.1-1.N в процессе работы указывает URL информационного ресурса 9-10, к которому желает получить доступ. На основе указанного URL программным обеспечением компьютера-клиента 1-1.N формируется запрос, который поступает в базу данных проверенных информационных ресурсов 2.

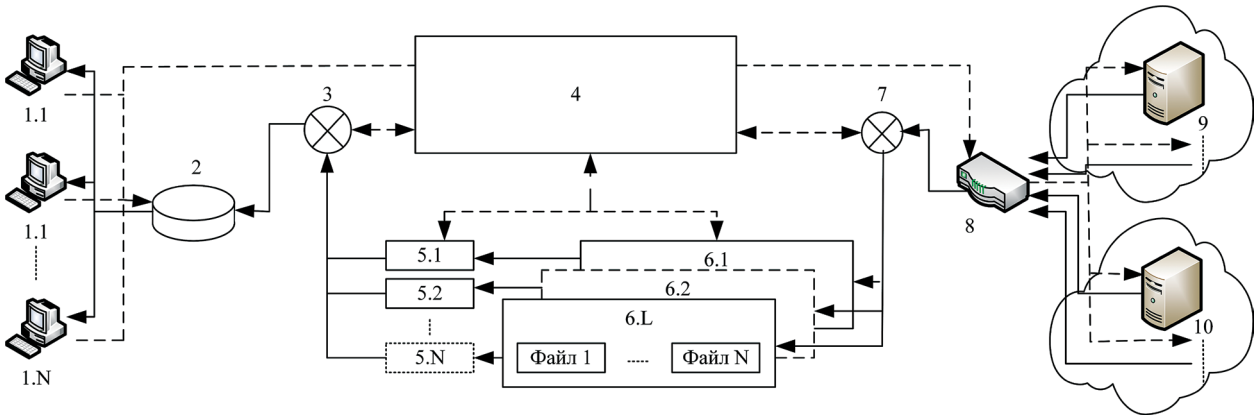
Если информационный ресурс содержится в базе данных проверенных информационных ресурсов 2, тогда устанавливается подключение к требуемому информационному ресурсу.

Если информационного ресурса нет в базе данных проверенных информационных ресурсов 2, запрос поступает на устройство управления доступом к информационным ресурсам 4.

Устройство управления доступом к информационным ресурсам 4 регистрирует попытку установления подключения компьютера-клиента 1.1-1.N к информационному ресурсу 9-10.

Устройство управления доступом 4 проверяет уровень конфиденциальности нового информационного ресурса 9-10.

Если уровень конфиденциальности совпадает с требуемым уровнем, происходит отключение выхода модуля шлюзов 3 и включение входа модуля шлюзов 7, после чего принимают запрашиваемую информацию в шлюз 6.1-6.L, отключают вход



1.1-1.N – совокупность компьютеров-клиентов;
2 – база данных проверенных информационных ресурсов;
3 – выход модуля шлюзов;
7 – вход модуля шлюзов;
5.1-5.N – совокупность средств защиты информации;
6.1-6.L – совокупность шлюзов;
9 – совокупность компьютеров-серверов, входящих в состав сети Интернет;
10 – вторая совокупность компьютеров-серверов, входящих в состав мультисервисной сети связи;
8 – маршрутизатор периметра;
4 – устройство управления доступом к информационным ресурсам.

***Рис. 1** Схема функционирования мультисервисной сети связи с использованием способа управления доступом к информационным ресурсам*

модуля шлюзов 7, записывают принятую информацию в ячейки памяти ОЗУ шлюза 6.1-6.L и копируют принятую информацию в шлюзы по числу средств защиты информации 5.1-5.N.

Если уровень конфиденциальности не совпадает с требуемым уровнем, происходит уведомление пользователя 1.1-1.N об отказе в получении доступа.

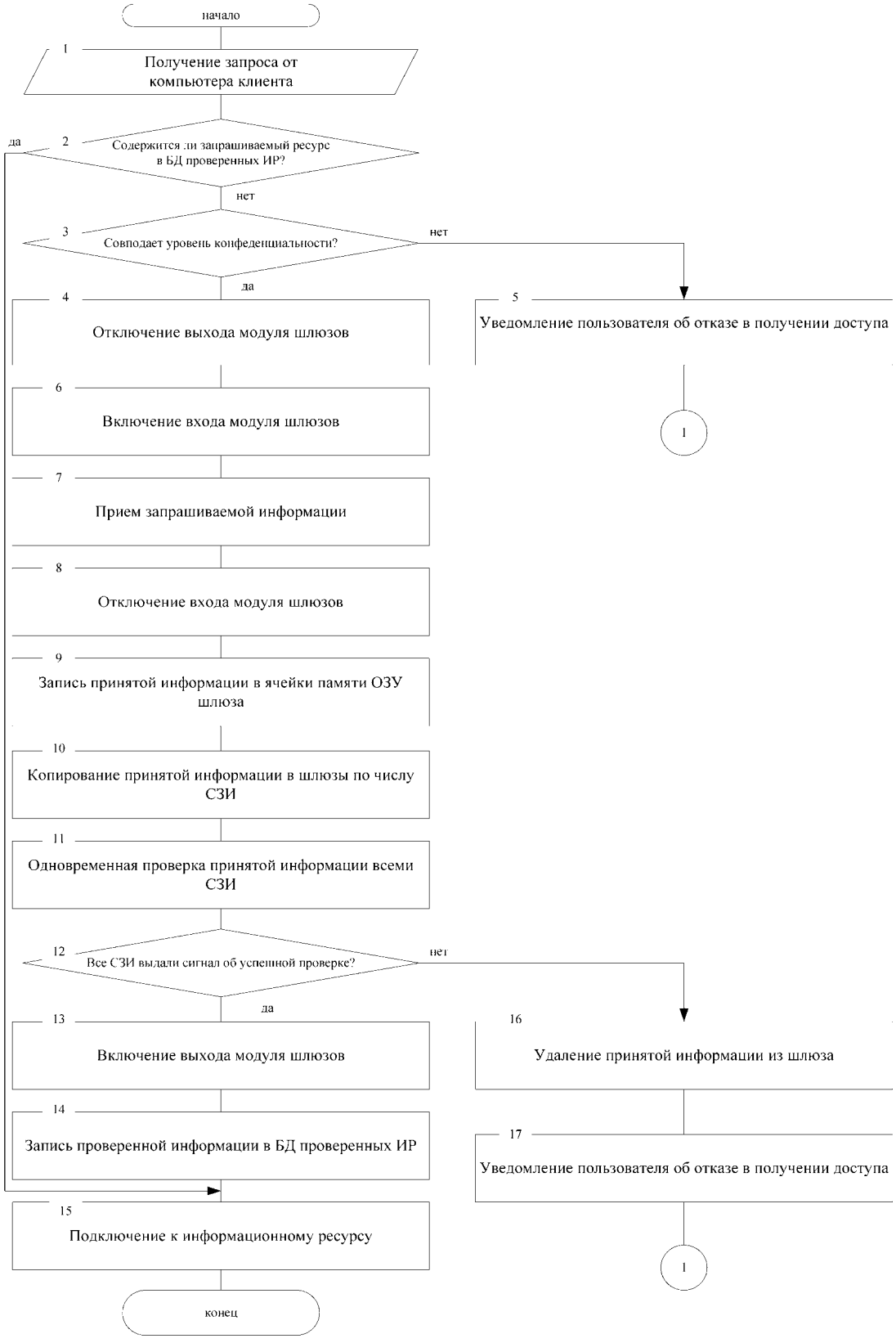


Рис. 2. *Последовательность действий способа управления доступом к информационным ресурсам*

Одновременно всеми средствами защиты информации 5.1-5.N проверяют принятую информацию.

Если все средства защиты информации 5.1-5.N выдали сигнал об успешном завершении проверки, то включают выход модуля шлюзов 6.1-6.L.

Если хотя бы одно средство защиты информации 5.1-5.N выдало сигнал о неудачном завершении проверки, то удаляют принятую информацию из шлюзов 6.1-6.L и уведомляют пользователя 1.1-1.N об отказе в получении доступа.

Записывают проверенную информацию в базу данных проверенных информационных ресурсов 2.

Устанавливают подключение к требуемому проверенному информационному ресурсу.

Более подробно последовательность действий разработанного способа по управлению доступом к информационным ресурсам мультисервисных сетей связи различных уровней конфиденциальности, представлена на рисунке 2.

Выводы

Преимущество разработанного способа состоит в исключении прямого физического и логического соединения между разноуровневыми (по конфиденциальности) сегментами мультисервисной сети связи. Кроме этого, происходит сокращение времени задействования инфо-телекоммуникационных ресурсов сети и времени реализации запроса на доступ к проверенным информационным ресурсам. Перемещение средств защиты информации 5.1-5.N от компьютеров-клиентов 1.1-1.N в модуль шлюзов 6.1-6.L дает их количественное сокращение.

Разработанный способ позволяет осуществить управление доступом к информационным ресурсам в зависимости от уровня их конфиденциальности, обеспечивает повышение защищенности путем исключения прямого физического и логического соединения между разноуровневыми (по конфиденциальности) сегментами сети, сокращает количество средств защиты и времени реализации запроса на доступ к информационным ресурсам за счет использования дополнительной базы данных, в которой хранятся проверенные информационные ресурсы, тем самым обеспечивается достижение поставленной задачи.

Разработанный способ предназначен для сетевых администраторов и пользователей мультисервисных сетей связи, обеспечивающих информационную безопасность.

Представленное в разделе научно-методическое обеспечение является основой и определяет наиболее перспективные направления для разработки подходов к разграничению доступа к информации различного уровня конфиденциальности.

Эффективность разработанного способа проверена на физической модели и повышает защищенность обрабатываемой информации от несанкционированного доступа по сравнению с аналогичными способами на 5-9 %.

Новизна разработанного способа подтверждается патентом РФ на изобретение [7].

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им.Н.Э.Баумана, v.tsirlov@cnpo.ru.*

Литература:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008.
2. Беляев Д.Л., Комашинский В.В. Устройство управления доступом к информационным ресурсам мультисервисной сети. Патент на полезную модель RUS 99880 12.07.2010.
3. Бухарин В.В., Дворядкин В.В., Шедий М.В. Метод обнаружения несанкционированного доступа к информационным ресурсам мультисервисной сети // Вестник компьютерных и информационных технологий. 2014. № 4 (118). С. 39-44.
4. Гречишников Е. В., Горелик С. П., Добрышин М. М. Способ обеспечения требуемой защищенности сети связи от внешних деструктивных воздействий // Телекоммуникации. 2015. № 6. С. 32-37.
5. Комашинский В.В., Беляев Д.Л., Васинёв Д.А., Нгуен Т.А. Способ управления доступом к информационным ресурсам компьютерных сетей различных уровней конфиденциальности и устройство, его реализующее. Патент на изобретение RUS 2436154 01.12.2009.
6. Межсетевой экран с фильтрацией трафика по мандатным меткам / Марков А.С., Цирлов В.Л., Барабанов А.В. и др. Патент на полезную модель RUS 159041 18.02.2015.
7. Стародубцев Ю.И., Кирьянов А.В., Панкова Н.В. и д.р. Способ управления доступом к информационным ресурсам компьютерных сетей различных уровней конфиденциальности. Патент на изобретение № 2541170, 10.02.2015.

PROPOSALS FOR ACCESS CONTROL TO INFORMATION RESOURCES OF COMPUTER NETWORKS DIFFERENT LEVELS OF PRIVACY

Starodubtsev Y.I.[4], Begaev A.N.[5], Kozachok A.V.[6]

The widespread use of communication networks with different levels of confidentiality of information processed requires the use of new principles of access control. The existing principles of control have some disadvantages, namely relatively low security internal network segment, as it is not considered direct physical and logical connection between different levels (for confidentiality) network segments, and duplicated security information of each client computer with multi-user access to information resources. Consequently, it is necessary to develop proposals to eliminate these shortcomings.

***Keywords**: computer network, multiservice network, information security, access controls, confidentiality of information.*

References:

1. GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniya. M.: Standartinform, 2008.
2. Belyaev D.L., Komashinskiy V. V. Ustroystvo upravleniya dostupom k informatsionnym resursam mul'tiservisnoy seti. Patent na poleznuyu model' RUS 99880 12.07.2010.
3. Bukharin V.V., Dvoryadkin V.V., Shediy M.V. Metod obnaruzheniya nesanktsionirovannogo dostupa k informatsionnym resursam mul'tiservisnoy seti, Vestnik komp'yuternykh i informatsionnykh tekhnologiy. 2014. No 4 (118), pp. 39-44.
4. Grechishnikov E. V., Gorelik S. P., Dobryshin M. M. Sposob obespecheniya trebuemoy zashchishchennosti seti svyazi ot vneshnikh destruktivnykh vozdeystviy, Telekommunikatsii. 2015. No 6, pp. 32-37.
5. Komashinskiy V.V., Belyaev D.L., Vasinev D.A., Nguen T.A. Sposob upravleniya dostupom k informatsionnym resursam komp'yuternykh setey razlichnykh urovney konfidentsial'nosti i ustroystvo, ego realizuyushchee. Patent na izobretenie RUS 2436154 01.12.2009.
6. Mezhsetevoy ekran s fil'tratsiey trafika po mandatnym metkam / Markov A.S., Tsirlov V.L., Barabanov A.V. i dr. Patent na poleznuyu model' RUS 159041 18.02.2015.
7. Starodubtsev Yu. I., Kir'yanov A. V., Pankova N. V., i d.r. Sposob upravleniya dostupom k informatsionnym resursam komp'yuternykh setey razlichnykh urovney konfidentsial'nosti. Patent na izobretenie № 2541170, 10.02.2015.

4 Yuriy Starodubtsev, Dr.Sc., Professor, Federal State Public Educational Institution of Higher Professional Education Military Telecommunication Academy named after the Soviet Union Marshal Budienny S. M., Saint-Petersburg

5 Alexey Begaev, Ph.D., NW Echelon, Saint-Petersburg, a.begaev@nwechelon.ru

6 Alexander Kozachok, Ph.D., The Academy of Federal Security Guard Service of the Russian Federation, Orel, alex.totrin@gmail.com