УДК 528.71
DOI 10.33764/2618-981X-2023-6-197-202

Д. С. Пельц[1], А. В. Шабурова[1]*

Построение защищенного канала связи для системы видеоконференцсвязи в органах местного самоуправления

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: diana4ka-00@mail.ru

Аннотация. Предмет исследования**.** Проблема построения защищенных каналов связи для передачи конфиденциальной информации в информационных системах видеоконференцсвязи играет важную роль в организации защиты информации в органах местного самоуправления. Потребность в использовании систем видеоконференцсвязи в муниципалитетах с течением времени становится все более необходимой. Особенно важно в информационных системах такого типа при шифровании канала связи сохранить качество изображение, скорость звука и другие технические характеристики. В данной статье проведено исследование влияния средств криптографической защиты на пропускную способность канала передачи данных. Цели исследования. Определение влияния шифрования канала связи сертифицированными средствами криптографической защиты на его пропускную способность с последующим внедрением защищенной системы видеоконференцсвязи в органы местного самоуправления при использовании собственных технических средств. Методология**.** В процессе исследования проблемы шифрования каналов для систем видеоконференцсвязи использовались сравнительный методы и метод тестирования. Результаты. В ходе исследования был проведен сравнительный анализ открытого канала передачи данных системы видеоконференцсвязи и защищенного сертифицированными средствами криптографической защиты информации. В процессе эксперимента по выбранным техническим критериям были сняты показатели передачи информации по открытому и закрытому каналам связи. По результатам было выявлено минимальное расхождение значений открытого и закрытого каналов системы видеоконференцсвязи. Выводы. Сделан вывод о том, что шифрование каналов связи информационной системы ВКС сертифицированными средствами криптографической защиты информации не сказывается на технических характеристиках каналов передачи данных, но позволяет предотвратить утечку конфиденциальной информации в органах местного самоуправления.

Ключевые слова: защищенный канал связи, система видеоконференцсвязи, средства криптографической защиты информации

D. S. Pelts[1], A. V. Shaburova[1]*

Definition of the Characteristics of the Unmanned Aviation System when Carrying out Search and Rescue Operations in Wetted Areas

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: diana4ka-00@mail.ru

Abstract. Subject researches. The problem of building secure communication channels for transmitting confidential information in videoconferencing information systems plays an important role in organizing information protection in local governments. The need for the use of video conferencing systems in municipalities is becoming more and more necessary over time. It is especially important

in information systems of this type to preserve image quality, sound speed and other technical characteristics when encrypting a communication channel. This article will study the effect of cryptographic protection on the throughput of a data transmission channel. Goals researches. Determination of the impact of the encryption of the communication channel by certified cryptographic protection means on its bandwidth, followed by the introduction of a secure VCS system to local governments using their own technical means. Methodology**.** In the process of studying the problem of channel encryption for videoconferencing systems, measuring, comparative methods and a testing method were used. Results**.** In the course of the study, a comparative analysis of the open data transmission channel of the videoconferencing system and the protected by certified cryptographic information protection was carried out. In the course of the experiment, according to the selected technical criteria, indicators of information transmission over an open and closed communication channel were taken. According to the results, the minimum discrepancy between the values of the open and closed channel of the videoconferencing system was revealed. Conclusions**.** It is concluded that the encryption of communication channels of the videoconferencing information system with certified means of cryptographic information protection does not significantly affect the technical characteristics of data transmission channels, but it helps to prevent the leakage of confidential information in local governments.

Keywords: secure communication channel, videoconferencing system, means of cryptographic information protection

Введение

В современное время значительно возросла актуальность систем видеоконференцсвязи в рабочем процессе органов местного самоуправления. Видеоконференцсвязь (ВКС) – это сеанс связи между двумя пользователями или группой пользователей, независимо от их месторасположения, при этом, участники видят и слышат друг друга согласно правилам, определяемым видом видеоконференции.

В качестве среды передачи данных может использоваться как сеть органов местного самоуправления, так и глобальная сеть интернет. Поэтому при проведении видеоконференции в муниципалитетах важную роль играют вопросы информационной безопасности, особенно при реализации связи с удаленными филиалами при помощи сети интернет. В связи с этим остро встал вопрос обработки в информационных системах ВКС не только общедоступной информации, но и информации ограниченного доступа [1, 12]. В данных условиях передача данных по открытым сетям недопустима, ведь даже минимальная утечка сведений может привести к утере информации ограниченного доступа, что накладывает определенные требования для обеспечения защищенности информации с точки зрения законодательства Российской Федерации [7 – 9, 11, 13].

Защиту информации в информационных системах ВКС можно разделить на следующие аспекты: защита аудиовизуальной информации из помещений; защита конечных точек и серверов от несанкционированного доступа; защита информации по каналам передачи связи между пользователями и серверами. Если первые два аспекта не вызывают вопросов и ничем не отличаются от защиты информации в иных информационных системах, то третий аспект требует дополнительного внимания. Это обусловлено тем, что системы ВКС не накапливают информацию, а ведут обработку информации в режиме реального времени, что

в свою очередь, накладывает определенные требования к скорости сетевого взаимодействия и качеству передаваемой информации.

Наиболее универсальным способом защиты информации по линиям связи смешанного типа, включающим в себя отрезки как внутри контролируемой зоны, так и вне ее, является шифрованием трафика между конечными оппонентами и (или) серверами. Так как рассматриваемая информационная система содержит конфиденциальную информацию, то средства криптографической защиты информации должны быть сертифицированы органами ФСБ (Приказ ФСБ России от 10.07.2014 N 378) [10].

Поэтому цель настоящей работы заключается в установлении влияния шифрования канала связи сертифицированными средствами криптографической защиты на его пропускную способность с последующим внедрением защищенной системы ВКС в органы местного самоуправления при использовании собственных технических средств.

Методы и материалы

Для реализации поставленной цели по защите, имеющейся ВКС применялось аппаратное шифрование каналов с использованием маршрутизаторов «Cisco ASA» (IPsec) и аппаратно-программный комплекс шифрования (АПКШ) защиты информации «ViPNetCoordinatorHW-1000» (рис. 1).

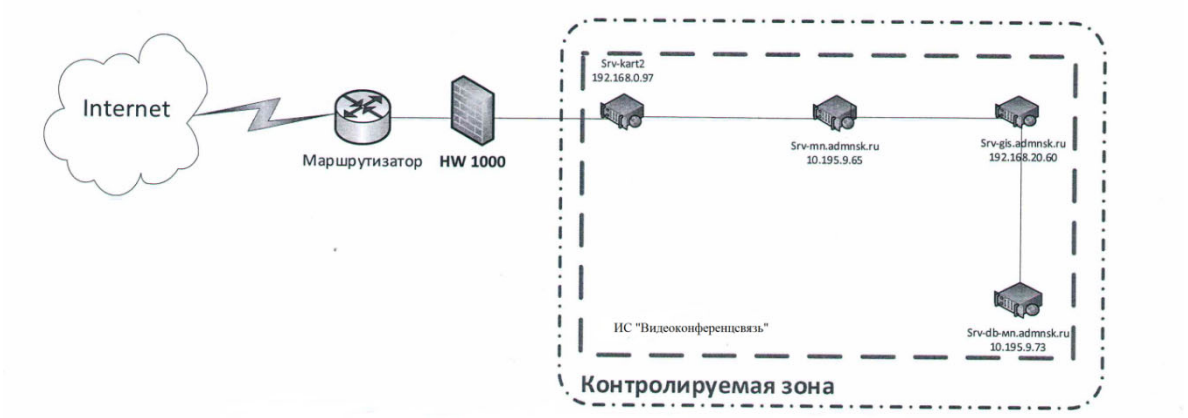

Рис. 1. Структурная схема ИС «Видеоконференцсвязь»

Эксперимент проводили с участием 20 пользователей системы ВКС, находящихся в равных условиях, таких как наличие одинаковых камер, типа подключения к системе, ширины канала, динамичности изображения т.д. Результаты были получены в течение 4 сеансов ВКС. В качестве критериев для сравнительного анализа каналов были приняты количество ошибок на порту, количество потерянных пакетов и скорость отправки и приема.

Результаты

В ходе построения и модернизации защищенного канала системы ВКС был проведен сравнительный анализ открытого и защищенного сертифицирован-

ными средствами криптографической защиты информации (СКЗИ) каналов передачи данных системы ВКС. Результаты, полученные экспериментальным методом, представлены в табл. 1 и 2.

Таблица 1

Анализ открытого канала передачи данных системы ВКС

Название критерия	Отправка				Прием			
	1	2	3	4	1	2	3	4
Скорость передачи данных, (кбит/сек)	403,1	982,4	4096	1024	1024	1024	4096	1024
Количество потерянных пакетов, %	0	0	0	0	0	0	0	0
Количество ошибок на порту	0	0	0	0	0	0	0	0

Таблица 2

Анализ защищенного канала передачи данных системы ВКС

Название критерия	Отправка				Прием			
	1	2	3	4	1	2	3	4
Скорость передачи данных, (Мбит/сек)	400,3	949,4	1024	985,8	1024	1024	1024	1024
Количество потерянных пакетов, %	0	1	0	0	0	0	0	0
Количество ошибок на порту	0	0	0	0	0	0	0	0

Сопоставив значения, представленные в табл. 1 и 2, можно сделать вывод о том, что канал передачи данных, зашифрованный сертифицированными СКЗИ, обладает меньшей пропускной способность на (1-3) %, чем открытый канал передачи данных. Это свидетельствует о том, что защищенный канал передачи данных не уступает по своим техническим характеристикам открытому каналу передачи данных, а также предотвращает возможную утечку конфиденциальной информации и защищает от несанкционированного доступа.

Обсуждение

С помощью внедрения системы ВКС в криптографическую сеть под управлением аппаратно-программного комплекса шифрования «ViPNetCoordinator HW-1000» появилась возможность объединить через интернет территориально распределенные локальные сети филиалов в единую сеть VPN. Данное решение определено рядом преимуществ аппаратно-программного комплекса шифрования «ViPNetCoordinatorHW-1000». В их число входят неограниченное количество узлов аудио и видеосвязи, возможность группирования как стационарных систем аудио- и видеосвязи, так и удаленных рабочих мест, оснащенных программными компонентами системы аудио- и видеосвязи; полноценная поддержка технологии виртуальных адресов в мультимедийных протоколах типа SIP, SCCP (CiscoSkinnyClientProtocol), H.323, обеспечение беспрепятственного прохождения защищенного трафика или в случаях противодействия интернет-провайдера.

Существенным фактором является наличие всех необходимых сертификатов ФСБ и ФСТЭК России [4, 5, 6]. Реализованные в СКЗИ обнаружение и предотвращение утечки информации, а также блокировка трафика сетевых приложений значительно повышают действенность фильтрации. Следует отметить, что созданные администратором правила разграничения трафика на основе команд протоколов HTTP(S) и FTP гарантируют эффективность контроля доступа пользователей в сеть интернет. А интегрированный детектор атак при обнаружении угрозы даст межсетевому экрану на криптошлюзе команду на создание временного правила для фильтрации трафика источника атаки, позволяющего активно и оперативно отражать нежелательный трафик, направленный на сеть органов местного самоуправления.

Заключение

Таким образом, в рамках проведенного исследования можно сделать вывод о том, что применение сертифицированного СКЗИ в системе ВКС не ведет к потере качества проведения видеоконференций в органах местного самоуправления, но позволяет объединить муниципалитеты в сегмент закрытой локально-вычислительной сети, включающий в себя разграничение пользователей на группы с правами доступа, которые соответствуют уровню доступа к сведениям, содержащим конфиденциальную информацию, а также успешно интегрировать систему закрытой ВКС в муниципалитеты [2, 3, 14].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Банк данных угроз безопасности информации // ФСТЭК России: официальный сайт – URL: https://bdu.fstec.ru/threat (дата обращения: 20.02.2023).

2. Болик, В. Н. О правомерности законодательных ограничений конституционного права на неприкосновенность частной жизни / В. Н. Болик // Законы России: опыт, анализ, практика. – 2015. – № 7. – С. 78-84.

3. Буркова, А. Ю. Локализация баз данных на территории Российской Федерации / А. Ю. Буркова. - 1. - Москва: Законодательство и экономика, 2015. – С. 54-57.

4. Выписка из перечня средств защиты информации, сертифицированных ФСБ России // Центр по лицензированию, сертификации и защите государственной тайны ФСБ России : официальный сайт: clsz.fsb.ru/clsz/certification.htm- (дата обращения: 20.02.2023).

5. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина – Москва: Форум, 2017. – 159 с.

6. Меры по обеспечению защиты персональных данных в организации // СерчИнформ: официальный сайт – URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/mery-po-obespecheniyu-zashchity-personalnyh-dannyh-v-organizacii/ (дата обращения: 28.02.2023).

7. Постановление правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Справочная правовая система КонсультантПлюс. - Режим доступа: по подписке (дата обращения: 06.03.2023).

8. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 10.03.2023).

9. Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 14.03.2023).

10. Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 14.03.2023).

11. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 16.04.2022).

12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 29.03.2023).

13. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 29.03.2023).

14. Яковец, Е. Н. Своеобразие состава защищаемой конфиденциальной информации/ Е.Н. Яковец // Право и кибербезопасность. – 2014. – № 2. – С. 51-58.