– C_PopUpCalendar –виджет выбора даты;
– C_Print - библиотека организации печати.

В результате удалось разработать сервис-браузер, работающий в среде Linux. Нужно отметить, что вместе сервис-браузером в новую среду мигрирует также базовый модуль «Администратор системы», с помощью которого производится настройка параметров функционирования информационной системы. Прикладные модули требуется переносить самостоятельно, используя правила и компоненты, разработанные в процессе создания сервис-браузера.

Литература:

1. В поисках альтернативы: варианты импортозамещения ПО в России. – URL: https://aif.ru/boostbook/importozameshchenie-po.html?ysclid=lkwlesp6bu729683692#solut (дата обращения 07.08.2023).

2. Реестр российского программного обеспечения. – URL: https://reestr.digital.gov.ru/ (дата обращения 15.12.2023).

3. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. – 2017. – Том 8, № 9. – С. 413-421. – DOI: 10.17587/prin.8.413-421.

4. *Курако Е.А., Орлов В.Л.* Способ организации взаимодействия клиента с сервером приложений с использованием сервис-браузера: Патент на изобретение RU 2656735 C1; Зарегистрирован 06.06.2018. Заявлено 17.05.2017. Опубликовано: 06.06.2018 Бюллетень № 16.

5. Моно – Лаборатория 50 (lab50.net). – URL: https://lab50.net/моно (дата обращения 10.01.2024).

Чебан А.Г., Анисимова Е.А.

Принципы организации и построения защищенных систем видеоконференции

Аннотация: В работе рассмотрены принципы организации и построения защищенных систем видеоконференцсвязи, рассмотрены современные технологии шифрования

информации, а также оборудование, предназначенное для защиты конфиденциальной информации.

Ключевые слова: видеоконференции, информационная безопасность, защита конфиденциальной информации, защищённая видеоконференцсвязь, шифрование

Современные системы видеоконференцсвязи представляют собой технологию, которая позволяет участникам, находящимся в разных локациях, проводить личные или деловые встречи (совещания), без необходимости собираться в одном месте. Они предназначены для рабочих встреч, заключения деловых сделок и собеседований с кандидатами на работу. А если видеоконференция проводится в неформальных целях, то ее, как правило, называют видеозвонком или видеочатом, чем регулярно пользуются сотни тысяч пользователей посредством своих смартфонов. В настоящее время известными решениями для видеоконференцсвязи являются системы: IVA, Skype, True Conf, Zoom, Яндекс Телемост, Google Meet, а также современные мессенджеры Telegram, WhatsApp, Viber и другие.

Одним из пионеров организации видеоконференцсвязи в начале 2000-х годов стала компания Skype, но триггером к стремительному росту стал фактор массового перехода на удаленную работу сотрудников по всему миру из-за пандемии коронавирусной инфекция COVID-19. На конец 2019 года у Skype насчитывалось 25 млн зарегистрированных пользователей, а уже к апрелю 2020 года это число составило свыше 100 млн пользователей. Компания Zoom до начала 2020 года насчитывала всего 10 млн пользователей, а в марте 2020 года этот показатель увеличился двадцатикратно до 200 млн. У Google Meet в 2019 году насчитывалось 100 млн посещений в месяц, а спустя год их было уже более 1,25 млрд.

В связи с экстренным выходом на удаленную работу большинство сотрудников государственных учреждений и предприятий оказались не готовы к организации видеоконференций по ряду причин: отсутствовало специализированное оборудование и/или необходимое количество лицензий для входящих/исходящих соединений участников видеоконференции. Следствием этого стало то, что значительная часть организаций государственного и производственного сектора Российской Федерации арендовала у

различных компаний (Skype, Zoom, TrueConf и др.) системы видеоконференций как сервис.

Проведение видеоконференций через посредников всегда несет риски утечки конфиденциальной информации, так как посредник может: добавить участников; записать разговор; добавлять элементы виртуальной или дополненной реальности.

Ситуация усугубилась в феврале 2022 года, когда ряд иностранных компаний заявил о прекращении своих контрактных обязательств и об «уходе из России», тем самым кратно возросли риски по утечке или трансформации данных.

Во избежание потерь или трансформации данных, передаваемых в видеоконференциях посредством глобальной сети Интернет, необходимо обеспечить «гарантированную» передачу данных от источника к приемнику.

По классической схеме (рисунок 1) организация видеоконференции происходит через арендованный сервис (посредник).

Предлагаемая авторами технология защищенной видеоконференцсвязи предполагает следующие шаги:

– установку российских межсетевых экранов нового поколения;
– организацию защищённых каналов связи между межсетевыми экранами;
– установку российских видеотерминалов;
– установку российских видеосерверов (при необходимости);
– приобретение российского программного обеспечения для организации видеоконференций.

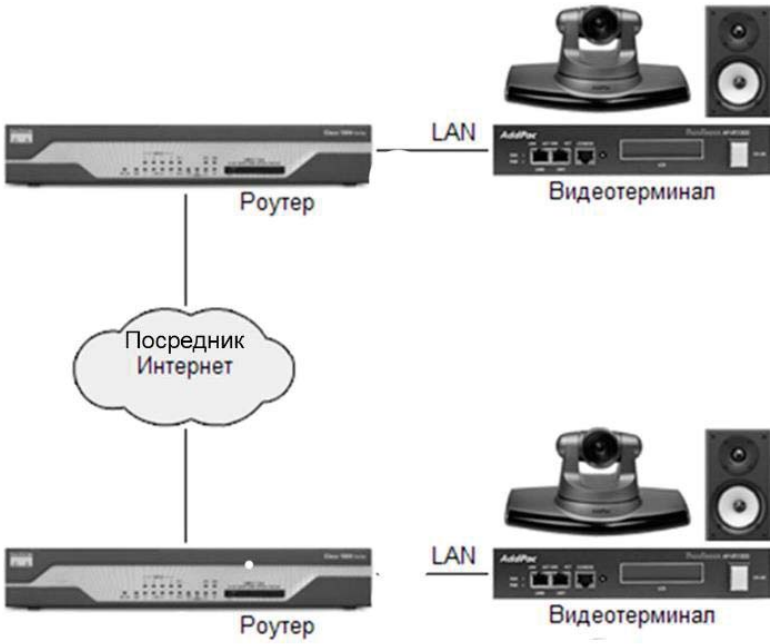

Рисунок 1 – Классическая схема организации видеоконференции через посредника

Каждый из участников устанавливает российский межсетевой экран нового поколения, между сетевыми экранами необходимо создать VPN-соединения при помощи протоколов IPSec, тем самым будет достигнуто доверенное соединение между источником и приемником данных. Далее необходимо настроить соединение от видеотерминала к роутеру локальной сети, а от него к межсетевому экрану, при соединении рекомендуется создать внутри локальной сети виртуальную локальную сеть (VLAN) и настроить на портах фильтрацию MAC адресов только для текущих устройств (рисунок 2).

Таким образом, при проведении единоразового конфигурирования устройств между постоянными участниками видеоконференции будет достигнута гарантированная передача достоверных данных.

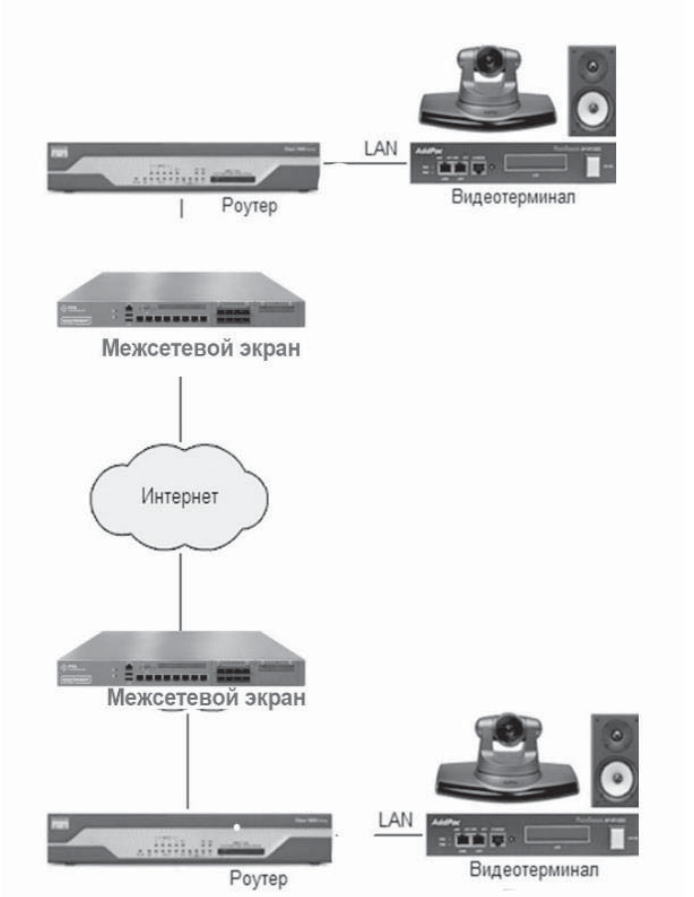

Рисунок 2 – Схема организации защищённой видеоконференцсвязи между постоянными участниками

Как в предыдущем варианте предполагается, что организатор установил межсетевой экран и обеспечил доступ к видеокодеку, далее на межсетевом экране генерируется сертификат, ограниченный по времени действия на период организации видеоконференции, и одновременно организовывается сервер VPN-подключения, через который осуществляется передача пользователю сертификата и реквизитов подключения к VPN серверу (рисунок 3).

Таким образом, при проведении конфигурирования межсетевого экрана будет организован временный канал связи и передача по нему данных.

Рисунок 3 – Схема организации защищённой видеоконференцсвязи между непостоянными участниками

Для обеспечения защищенного канала связи необходимо использовать межсетевой экран нового поколения (NGFW - Next Generation FireWall), представляющий собой интеграцию современных технологий сетевой безопасности. NGFW определен как интегрированная сетевая платформа со скоростью передачи данных, выполняющая глубокую проверку трафика и блокирующая атаки.

Межсетевые экраны нового поколения (NGFW) обладают широкими возможностями контроля и наблюдения за приложениями, которые могут идентифицировать с помощью анализа и сопоставления сигнатур. NGFW могут использовать белые списки или систему предотвращения вторжений на основе сигнатур, чтобы различать безопасные и вредоносные приложения, которые идентифицируются с помощью расшифровки протокола

SSL. Кроме того, в отличие от большинства традиционных межсетевых экранов, у них есть возможность для получения будущих обновлений.

По результатам проведенного исследования были сделаны следующие выводы.

Использование технологии защищённой видеоконференцсвязи позволит избежать утечки конфиденциальной информации. Данная технология полностью импортонезависима, что позволяет получить сертификацию ФСТЭК и ФСБ.

Технология защищённой видеоконференцсвязи не требует ежемесячных платежей третьему лицу за предоставление услуг видеосвязи.

Межсетевые экраны нового поколения рекомендуется активно применять в защищенных системах видеоконференций по причине совмещения несколько базовых функций при организации защищенного канала связи таких как безопасность, учет и анализ данных.

Литература:

1. *Иконников С.Е., Ермакова А.Е., Антонов Д.А.* Оценка защищенности сети предприятия при помощи межсетевых экранов / Интеллектуальные транспортные системы: Материалы II Международной научно-практической конференции (г. Москва, 25 мая 2023 года). – Москва: РУТ (МИИТ), 2023. – С. 470-474.

2. *Чебан А.Г., Король С.А.* Особенности защиты информации в сети предприятия при помощи межсетевых экранов / Интеллектуальные транспортные системы: Материалы III Международной научно-практической конференции (г. Москва, 30 мая 2024 года). – Москва: РУТ (МИИТ), 2023. – С. 741-744.

Логинова Л.Н., Дроздов А.Д.

Анализ угроз информационной безопасности при использовании Telegram-ботов в бизнесе

Аннотация: В данной работе анализируются угрозы информационной безопасности при использовании