ОБОБЩЕННАЯ МОДЕЛЬ ЗАЩИТЫ ОТ КИБЕРАТАК НА VOIP

Израилов К.Е.[1], Макарова А.К.[2], Шестаков А.В.[3]

Цель исследования: *создание модели защиты от кибератак на информационно-телекоммуникационные ресурсы используемых на практике интернет-сервисов речевого обмена (VoIP).*

Методы исследования: *анализ Best Practices и научных публикаций, системный анализ, критериальное сравнение.*

Полученный результат: *произведена систематизация основных способов кибератаки на VoIP и методов защиты от них, исходя из существующих Best Practices и научных публикаций. Описана методологическая схема проведенного исследования, представленная в схематичном виде. В результате получен список из 8 специализированных и 9 основных способов кибератак, а также 4 специализированных и 10 основных методов защиты, что позволило создать обобщенную модель защиты от кибератак на VoIP. Представление модели в табличном виде состоит из 17 строк и 14 столбцов, что соответствует числу всех способов кибератак и методов защиты. В ячейках таблицы расположены экспертно полученные значения результативности противодействия кибератакам каждым из методов защиты по 3-х бальной системе. Модель расширена дополнительными интегральными показателями опасности кибератак, и результативности защиты, полученными аналитически. Определены 3 наименее поддающихся защите кибератаки и 3 наиболее результативных методов защиты.*

Научная новизна *заключается в сведении всего множества способов кибератак на VoIP и методов защиты от них в единую систему, характеризующую результативность противодействия.*

Ключевые слова: *VoIP, способ кибератаки, метод защиты, модель защиты, категориальное деление.*

DOI:10.21681/2311-3456-2023-2-109-121

Введение

Телекоммуникационное взаимодействие различных потребителей информационных услуг является важнейшим трендом современного мира. При этом удаленность и местоположение пользователей все больше уходит на второй план, поскольку обмен информацией происходит посредством сети Интернет, распространившейся на практически все точки мира.

Поскольку наиболее привычным способом общения людей является голос (по возможности, визуализация, а в перспективе – тактильность коммуникации), то это объясняет потребность людей в использовании технологии VoIP (*аббр. от* Voice over Internet Protocol, *перев. на русс.* Голос через Интернет Протокол). Суть заключается в использовании набора протоколов, технологий и методов для аудио и/или видеообщения.

С другой стороны, передача информации, которая может быть не только персональной, но и коммерческой или конфиденциальной, подвержена классическим угрозам информационной безопасности – нарушению конфиденциальности, целостности и доступности. Например, в первом случае голосовой канал может быть раскрыт и передан 3-м лицам, во втором – злоумышленник может подключиться к речевому информационному обмену и передать неверные сведения, а в третьем – DoS-атака приведет к недоступности оконечных средств участников информационного обмена или соответствующего сетевого и серверного оборудования.

Указанные «потребность» (как «желание» пользователей в классическом взаимодействии в любой точке пространства и времени) ***vs*** «возможность» (как уязвимость VoIP трафика к кибератакам (далее по тек-

1 Израилов Константин Евгеньевич, кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCHID: http://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56122749800. E-mail: konstantin.izrailov@mail.ru

2 Макарова Александра Константиновна, студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия. ORCHID: https://orcid.org/0000-0001-7745-3364. Scopus Author ID: . E-mail: alex-ecureuil@mail.ru

3 Шестаков Александр Викторович, доктор технических наук, старший научный сотрудник, помощник начальника Санкт-Петербургского университета ГПС МЧС России, Санкт-Петербург, Россия. ORCHID: 0000-0002-8462-6515. Scopus Author ID: 57219712387. E-mail: alexandr.shestakov01@yandex.ru.

сту – атаки, сетевые атаки) вследствие их передачи через открытые сети через множество точек промежуточных хостов) и определяют основное научное противоречие, на частичное разрешение которого и направлено текущее исследование.

Очевидно, что разрешение такого рода противоречий (как и аналогичных, таких, как создание абсолютно безопасного программного обеспечения (далее – ПО), создание «невскрываемых» стеганографических каналов, физическая защита серверных, гарантированное противодействие социальным атакам) является, скорее всего, неразрешимой задачей. Поэтому, хотя бы некоторое повышение безопасности VoIP будет существенным достижением в области информационной безопасности [1]. Первым шагом, сделанным в направлении данного исследования, будет систематизация всех возможных способов атак на VoIP и методов защиты, которые могут им противодействовать. Это, в частности, позволит определить, с какой результативностью каждый из методов защиты противодействует каждому способу атаки, что в исследовании отражается в модели защиты.

Опишем общий путь исследования, который хотя и является классическим для такого рода задач, требует некоторого уточнения. Путь основан на частичном применении аппарата категориального деления, суть которого заключается в делении множества однородных объектов на группы, согласно их соответствия элементам-антагонистам некоторой категориальной пары. В данном случае такой парой выбрана – «Специализированный» ***vs*** «Общий». К первому элементу будут относиться способы атак и методы защиты, которые исходят из специфики VoIP; ко второму же элементу отнесем исходящие из общих принципов проведения атак и защиты, но которые были адаптированы к VoIP.

Исходя из выбранного деления способов атак и методов защиты (на специализированные и общие), подход к их выделению может быть выбран следующим образом. Поскольку специализированные способы и методы, как правило, носят частный характер, не позволяющий соотнесения их с подобными в других областях, то и информацию о них целесообразно получать из так называемых Best Practices – т. е. из реального опыта людей «в боевых условиях» (например, с форумов тематических конференций). С другой стороны, общие методы и способы являются классическими в данной области и, следовательно, подтверждаются научными публикациями – касательно сетевых атак и защиты облачных систем. Такая методологическая схема исследования приведена на рис. 1.

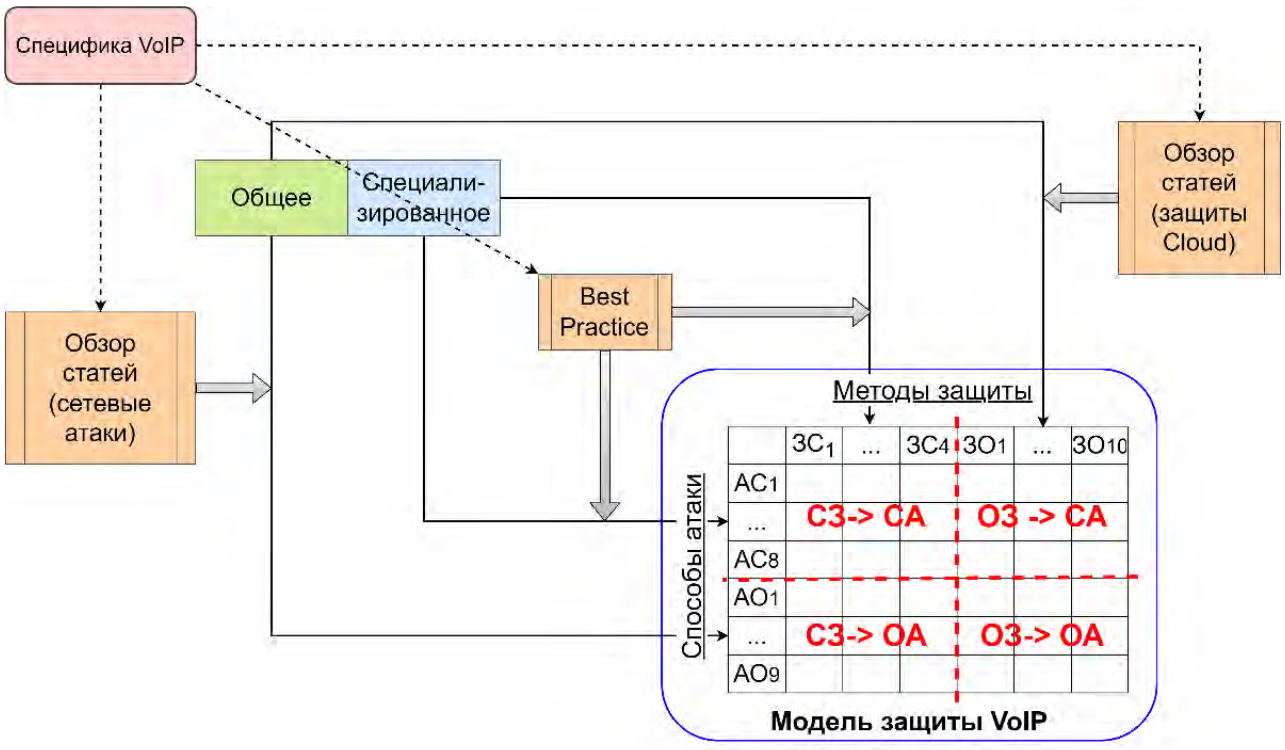

Рис. 1. Методологическая схема проведения исследования

Примечание к рис.1: «Cloud» – перев. на рус. «Облако», обозначает облачные системы

Перейдем к исследованию специализированных и общих способов атак с позиции возможностей по их нейтрализации. Аналогичным образом опишем специализированные и общие методы защиты, применимые к этим атакам.

Способы атаки

Способы атак на VoIP целесообразно рассматривать в рамках двух групп: специализированных и общих.

Специализированные способы атак состоят из следующих восьми, полученных на основе анализа Best Practices.

AC_1. Перехват регистрации SIP

Протокол инициации сеанса SIP (аббр. от Session Initiation Protocol) функционирует на прикладном уровне и используется для установления, изменения или завершения приложений VoIP во время сеанса [2]. Прокси-сервер (т. е. регистратор сеанса) позволяет обеспечить инфологическое взаимодействие пользовательских агентов (т. е. IP-телефоны) по SIP и другим коммуникационным протоколам VoIP. Суть атаки заключается в перехвате регистрации SIP, когда злоумышленник заменяет регистрацию пользовательского IP-телефона на собственный, что приводит к потере вызовов для предполагаемого законного пользовательского агента.

Частичное противодействие атаке может быть достигнуто путем использования при SIP-регистрации пользовательского агента протоколов UDP и TCP, а также применением протокола безопасности транспортного уровня TLS (*аббр. от* Transport Layer Security) для установления аутентифицированного безопасного соединения.

AC_2. Модификация SIP-сообщения

Злоумышленник может перехватить и изменить SIP-сообщение, например, путем проведения предварительной атаки «человек посередине» MITM (*аббр. от* Man in the Middle), подмены IP или MAC-адреса, а также перехвата регистрации SIP. Предотвратить атаку можно путем использования TLS для защиты транспортных механизмов UDP и TCP, тем самым защищая конфиденциальность содержимого сообщения.

AC_3. SIP-перенаправление

Серверное приложение SIP получает запросы от мобильной станции и возвращает ответ о перенаправлении, указывая то, где запрос должен быть повторен. Тем самым, злоумышленник может произвести атаку на сервер, дав ему команду перенаправить вызовы жертвы на собственный номер, позволяя принимать вызовы жертвы. Причина уязвимости, которая позволяет проводить данную атаку, существует из-за недостаточной аутентификации SIP-протокола. Противодействовать атаке можно с помощью повышения надежности системы аутентификации (например, использованием TLS с стойкими к перебору паролями) или настройкой номерного плана на IP-АТС.

AC_4. Фальсификация пакетов транспортного протокола реального времени

Протокол реального времени RTP (*аббр. от* Real-time Transport Protocol) обеспечивает передачу мультимедийной шифрованной информации (аудио, видео) между двумя абонентами. Используя атаки типа MITM (например, путем подслушивания) [3], можно изменить поток информационного трафика, вставив или заменив пакеты RTP. Эта атака, проведенная должным образом, позволяет модифицировать разговор, вводя различные фрагменты предварительно записанного звука, реализовав тем самым весь спектр информационных угроз – нарушить конфиденциальность путем прослушивания, целостность путем вставки собственных голосовых сообщений и доступности путем генерации шума. Атака успешна, потому что протокол RTP уязвим для подделки мультимедиа, особенно если он используется без шифрования и с использованием транспортного протокола без установления соединения UDP.

Применение безопасного транспортного протокола в реальном времени SRTP (*аббр. от* Secure Real-time Transport Protocol) окажет некоторое нейтрализующее воздействие.

AC_5. Спам по IP-телефонии

Спам по IP-телефонии SPIT (*аббр. от* SPAM over Internet Telephony) является еще одной актуальной атакой на VoIP, суть которой заключается в передаче нежелательного набора сообщений по сети. Атака SPIT оказывается крайне результативной, когда злоумышленник подделывает идентификатор вызывающего абонента (например, с помощью предварительной проведенной атаки Caller ID спуфинг, который исследуется далее), создавая у получателя впечатление, что с ними связывается доверенная компания (банк, государственный орган и т. п.). Также подобные сообщения отправляются на множество IP-адресов, «забивая» VoIP канал, и переполняя голосовой почтовый ящик (что приводит к исчерпанию ресурсов). Спам-

сообщения могут содержать вирусы и шпионские программы. Предложено несколько методов противодействия SPIT в системах VoIP, таких как фильтрация, ведение репутации вызывающего абонента, а также черные и белые списки.

AC_6. Caller ID спуфинг

Caller ID спуфинг представляет собой подделку вызова от доверительной компании. Для этого злоумышленник манипулирует с личным идентификатором (т. е. с Caller ID) доверительного звонящего, повышая вероятность того, что жертва ответит на его звонок. Значение Caller ID [4] часто изменяется на телефонный номер или строку текста, совпадающего с аналогичным значением для государственного учреждения, банка или даже кого-то из списка контактов жертвы. Поскольку поля значения телефонных номеров включены в заголовки пакетов SIP-протокола, то скрыть Caller ID нельзя; следовательно, даже если злоумышленник подменяет текст, то его можно обнаружить по номеру.

AC_7. Фрикерская атака

Фрикерская атака — тип мошенничества, который заключается во взломе VoIP-системы в интересах совершения междугородних, международных (и иных) звонков, а также пополнение счета за счет жертвы. Хакеры, используя современные средства взлома, могут в результате получать доступ к голосовой почте абонента, перенастраивать стратегии переадресации и осуществлять маршрутизацию вызовов.

Определение фрикерской атаки возможно путем мониторинга текущего плана вызовов, отслеживания чрезмерного количества новых номеров в истории звонков, подозрительном времени сделанных вызовов и т. п.

AC_8. Программа VOMIT

Программа VOMIT (*аббр. от* Voice Over Misconfigured Internet Telephone, *перев. на рус.* Передача голоса по неправильно настроенным интернет-телефону) представляет собой инструмент для взлома VoIP. Программа предназначена для получения аудиофайла (формата WAV) из перехваченного сетевого трафика. В функционал утилиты входит поддержка распаковки трафика для IP-телефонов от компании Cisco, полученных с помощью кодека G.711 [5].

Данный тип прослушивания не только осуществляет сбор данных из системы, но позволяет злоумышленнику собирать бизнес-данные, такие как источник вызова, пароли, имена пользователей, номера телефонов и банковскую информацию.

Общие способы

Общие способы атак состоят из следующих девяти, полученных на основе анализа научных публикаций [6, 7, 8, 9, 10].

AO_1. Физические атаки

Сетевая инфраструктура VoIP, состоящая из таких элементов, как соединительные линии, серверы VoIP, коммутаторы и т. д., может быть физически модифицирована злоумышленниками с целью реализации угроз информационной безопасности. Атака может быть частично ограничена путем установки физического контроля доступа элементам инфраструктуры [11].

AO_2. Атаки типа ARP спуфинг

Злоумышленники могут комбинировать собственный MAC-адрес с другим IP-адресом в кэше протокола разрешения адресов ARP *(аббр. от* Address Resolution Protocol) пострадавшего узла, отправляя поддельные пакеты и выдавая себя либо за регистратора SIP, либо за конечную точку в этой конкретной системе VoIP. Использование Dynamic ARP Inspection (*перев. на рус.* Динамическая Проверка ARP) позволит останавливать все ARP-пакеты на коммутаторе для проверки действительных привязок $\{ IP \Longrightarrow MAC \}$ перед обновлением локального кэша ARP и пересылкой в соответствующий пункт назначения.

AO_3. Подмена MAC-адреса

Суть атаки заключается в том, что злоумышленник вытесняет существующий узел в сети VoIP, дублируя его MAC-адрес, тем самым делая свой узел «напоминающим» уже настроенный и авторизованный. Защитный механизм использования аутентификации портов, указанный в стандартах IEEE 802.1x для проверки подлинности каждого нового узла с портом, соединяющим его с сетью VoIP, предотвратит данный вид атаки.

AO_4. Перехват пакетов

Одной из наиболее распространенных VoIP-атак считается перехват пакетов. Принцип ее работы близок к традиционному захвату данных в сетях. Атака требует получения пакетов установления связи и ассоциированного медиа потока. В случае успешности атаки злоумышленник может перехватить имена пользователей, пароли и другую конфиденциальную

информацию. При этом не все реализации VoIP поддерживают шифрование или в некоторых они по умолчанию выключены. Использование виртуальных частных сетей VPN (*аббр. от* Virtual Private Network) и дополнительное шифрование сделает процесс передачи информации через Интернет более безопасным.

AO_5. Вредоносное программное обеспечение

Вредоносное ПО снижает безопасность приложений, используемых в VoIP. Как результат, может снижаться пропускная способность сети и увеличиваться перегрузка сигнала, приводя к угрозе нарушения доступности (что, например, повлияет на возможность осуществление вызовов VoIP [12]). Также могут повреждаться данные, передаваемые по сети (приводя к угрозе нарушения целостности). Нанося большой ущерб сами по себе, вредоносные приложения способствуют будущим уязвимостям, например, бэкдорам, что ведет как к краже информации (нарушению конфиденциальности), так и к потере контроля за программно-аппаратными компонентами VoIP [13].

Для предотвращения вредоносной активности в рамках атаки необходимо своевременное обновление ПО (потенциально содержащего уязвимости), а также использование антивирусов. Необходимо отметить, что некоторые маршрутизаторы умеют блокировать как вредоносное ПО, так и целые сайты в VoIPсети.

AO_6. Спуфинг интернет-протокола

В данной атаке злоумышленники используют тот же подход, что и в случае MAC-адресов, за исключением того, что целью является IP-адрес. Противодействие атаке возможно путем настройки маршрутизаторов на соответствующие сетевые аномалии [14] во входящих и исходящих пакетах (например, адреса которых не входят в локальный диапазон конкретной сети VoIP [7]).

AO_7. DoS-атаки

Одной из существенных проблем сервиса IP телефонии на базе протокола SIP является подверженность атакам отказа в обслуживании [15] – DoS (*аббр. от* Denial of Service) или их более опасной распределенной версии – DDoS (*аббр. от* Distributed Denial-of-Service, *перев. на рус.* Распределённый Отказ в Обслуживании). Реализация атаки представляют серьезную угрозу для VoIP, поскольку может вывести из строя не отдельный узел, а всю сеть. Типичными признаками успешной DoS-атаки являются длительные сигналы занятости и принудительные отключения вызовов [1].

AO_8. Фарминговые атаки

Под фарминговой атакой подразумевает использование уязвимостей сервера доменных имен DNS (*аббр. от* Domain Name Server) для манипулирования доверенной связью между удаленным сервером и клиентом путем сопоставления известного имени Интернет-ресурса с IP-адресом узла злоумышленника. Так, клиенты сервера «верят», что они взаимодействуют с валидным источником и получателем данных и могут быть подвержены информационным угрозам, основанными на подмене узлов (утечка одних конфиденциальных данных, предоставление других неверных данных и т. п.). Существует также форма фарминговой атаки на VoIP, когда большое количество вызовов перенаправляется на конкретный домен, что может привести к его отказу в обслуживании; таким образом, данная атака переходит в DDoS.

AO_9. Человек посередине

Одной из наиболее опасных и реализуемых атак на VoIP является атака «человека посередине», при которой злоумышленник устанавливает независимые соединения с жертвами и обеспечивает передачу сообщений между ними. При этом, поскольку жертвы верят, что общаются друг с другом без посредников, злоумышленник может контролировать весь проходящий через его узел мультимедиа трафик – компрометировать оригинальные (нарушая конфиденциальность) и вставлять собственные (нарушая целостность) сообщения, а также временно прерывая их доставку (нарушая доступность). Для реализации данной атаки возможно проведения другой – ARP-спуфинга, в результате которой сетевой трафик для IP-адреса жертв будет отправлен злоумышленнику.

Методы защиты

Методы защиты от атак на VoIP целесообразно рассматривать как специализированные и общие.

Специализированные методы

Специализированные методы защиты от атак состоят из следующих четырех, полученных на основе анализа Best Practices.

ЗС_1. Отказ от подключения к общедоступному Wi-Fi

Метод предназначен для защиты данных и соединений за счет ограничения свободы подключения пользователя к общедоступным Wi-Fi сетям. Метод

может быть реализован как на уровне политик безопасности, так и программными средствами. Метод позволяет предотвратить такие атаки, как SPIT, MITM, Dos и подбор ключей, так как снизит для злоумышленника вероятность получить нелегитимный доступ.

ЗС_2. Разделения сети данных и сети телефонии

Метод направлен на разграничение составляющих корпоративной сети на VoIP и IP сети, как для исключения сторонних угроз и упрощения их поиска, так и для разгрузки сети VoIP от ненужных широковещательных запросов QoS или VLAN. Метод позволит предотвратить распространение вирусов или стороннего доступа из IP в VoIP сеть.

ЗС_3. Объединение подразделений компании в общую VPN сеть

Суть метода заключается в подключении пользователей VoIP через VPN, приводя к тому, что абоненты получают доступ к виртуальному и шифрованному VoIP каналу внутри сети. Зачастую VoIP-сервер расположен в облаке и, следовательно, злоумышленники могут реализовывать перехваты данных, DDoS-атаки и несанкционированный доступ в корпоративную сеть. Применение метода снизит подобного рода атаки.

ЗС_4. Использование специализированного программного обеспечения для противодействия перебору паролей

Метод основан на использовании такого ПО, как Fail2Ban и SSHGuard, которые блокируют IP-адреса пользователей при превышении развешенного количества попыток доступа. Данный метод предотвращает атаки типа «грубой силы», что не дает злоумышленнику осуществить подбор пароля к VoIP-серверу. Использование такого ПО является достаточно распространенной практикой для сетевые администраторов.

Общие методы

Общие методы защиты от атак состоят из следующих десяти, полученных на основе анализа научных статей [10, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23].

ЗО_1. Обеспечение компьютерной грамотности пользователей

Метод предусматривает обучение пользователей базовым навыкам безопасной работы с информацией, таким, как применение надежных паролей, работа в современной ОС с обновлениями (т. е. имеющими актуальные исправления уязвимостей), использование антивирусного ПО, защита от социальных атак и т. п. Метод способен исключить множество атак, как на VoIP, так и на IP сети на начальных этапах проведения и повысить общую безопасность корпоративной сети.

ЗО_2. Управление доступом и проверка на соответствие принадлежности устройства сети

Метод заключается в разграничении прав доступа и проверке на соответствие принадлежности устройства данной локальной сети; разделение сетей Wi-Fi на гостевую и внутреннюю, выделение прав доступа пользователей, безопасная (многофакторная) аутентификация, коммутируемая передача данных и номерной план. Метод обеспечивает возможность предупреждения несанкционированного доступа, потенциально ведущего к триаде угроз информационной безопасности – нарушению конфиденциальности, целостности и доступности [24, 25].

ЗО_3. Применение планов маршрутизации и звонков

Аналогично плану маршрутизации в IP сетях, в VoIP есть так называемый номерной план (перев. на англ. dialplan), с помощью которого система имеет порядок действий при определенном сценарии звонков: передавать их дальше, сохранять, отвечать самостоятельно, блокировать и др. Это позволяет исключить из нежелательный трафик, заблокировать запрещенные направления вызовов и предотвратить такие атаки, как спам, DDos и фарминг. Применение метода позволит осуществлять своевременную защиту в случае взлома сервера, или же по крайне мере минимизировать ущерб.

ЗО_4. Защита BYOD/мобильных устройств

Использование одного устройства для личных и рабочих целей приводит к перемешиванию корпоративной и персональной информации сотрудника, что усложняет контроль над данными. Как результат, возможны риски в виде подключения к незащищённой сети Wi-Fi, скачивания и установления вредоносного ПО, краже или потеря устройства с данными и т. п. Для обеспечения контроля над данными может использоваться VPN, в результате чего сотрудники будут хранить данные в защищенном облаке, а не на личном устройстве.

ЗО_5. Внедрение криптосистем и протоколов шифрования

Метод заключается в шифрование трафика (IP или VoIP) при его передаче в сети, что, очевидно, существенно усложняет его компрометацию при перехвате

(например, в процессе атаки MITM). Наиболее часто применяемыми для этого протоколами являются SSH, TLS, SMTP, IPSEC и SRTP.

ЗО_6. Применение программных и аппаратных межсетевых экранов

Суть метода заключается в настройке сетевого экрана таким образом, чтобы он обслуживал только заведомо доверенные пакеты и направления их передачи. Возможной реализацией метода является применение специально настроенных цепочек правил. Так, например, типичной защитой АТС на базе Asterisk является использование правил фильтрации и перенаправления пакетов с помощью утилиты iptables. Так, чтобы к серверу Asterisk могли подключаться IP-телефоны и из внутренней сети, то необходимо наличие соответствующего правила. Корректная и полная настройка правил сведет практически на ноль вероятность получения доступа злоумышленника к VoIP-серверу.

ЗО_7. Мониторинг подозрительной активности и внедрение системы обнаружения и предотвращения вторжений

Метод основан на постоянном мониторинге подозрительной активности рабочих устройств сети (например, с помощью SIEM-систем). Также, метод включает в себя обнаружения и предотвращения вторжений (например, с помощью IPS/IDS систем) в результате проведения атак злоумышленником [26]. Данный метод способен исключить множество атак, используемых в своей схеме манипуляции с служебным трафиком и передаваемыми данными (например, атаки типа грубой силы, DoS, использование уязвимостей и вредоносного ПО, неавторизованный доступ и повышение привилегий пользователя, и т. п.).

ЗО_8. Резервное копирование и восстановление конфигураций системы

Метод заключается в восстановлении переставшей работать системы, для чего, в частности, требуется ее резервное копирование. Например, если АТС не функционирует из-за сбоя после DoS-атаки, то ее корректная конфигурация может быть восстановлена из резервной копии.

ЗО_9. Использование инструментов виртуализации

Применение метода позволяет разделить физический сервер с помощью гипервизора на несколько изолированных виртуальных серверов, которые являются независимыми друг от друга [27]. Как результат, сбой на одной них не повлияет на работоспособность остальных. Метод особо эффективен для защиты от атак типа «грубой силы» и DoS.

ЗО_10. Применение антивирусного программного обеспечения

Исходя из актуальнейшей проблемы наличия уязвимостей в ПО, приводящих к критическим последствиям для любой системы [28, 29], в рамках данного метода используется актуальное антивирусное ПО (как на стороне клиента, так и на стороне сервера). Помимо классических и хорошо известных антивирусных продуктов для клиентской стороны, для серверов существуют специализированные решения, такие, как Dr.Web Server Security Suite, Avast Essential Business Security, Microsoft Windows Defender, McAfee Server Security и др.

Модель защиты от атак

Исходя из описанных способов атак и методов защиты от них, построим соответствующую модель защиты в следующей матричной форме (см. таблицу): строкой является одна из атак на VoIP, поделенных на две группы – специализированных и общих; аналогично, столбцом является один из методов защиты от атаки; а ячейкой таблицы – результативность противодействия конкретной атаке (т. е. строка) с помощью конкретной защиты (т. е. столбец). Балльное значение результативности может быть одним из следующих: 0 – метод не применим, 1 – метод частично противодействует атаке, 2 – метод полностью нейтрализует атаку. Также в табличном представлении модели присутствует крайний правый столбец, суммирующий все балы в строке, и крайняя нижняя строка, суммирующая все баллы в столбце. Очевидно, что крайний столбец может быть проинтерпретировано как опасность каждого из способов атаки (от меньшего значения к большему), а крайняя строка – результативности каждого из методов защиты (от большего к меньшему).

Произведем анализ полученной модели (см. таблицу). Рейтинг опасности атак согласно значениям в крайнем правом столбце приведен в виде гистограммы на рис. 2.

Как результат, можно выделить Топ-3 наименее поддающихся защите атак на VoIP:

— АО_1. Физические атаки (10 баллов);
— АС_1. Перехват регистрации SIP (13 баллов);
— АС_2. Модификация SIP-сообщения (14 баллов).

Наиболее опасными с точки зрения отсутствия методов защиты оказались физические атаки, т. к. все

Таблица

Схема модели защиты от атак на VoIP (в табличном виде)

	ЗС_1	ЗС_2	ЗС_3	ЗС_4	ЗО_1	ЗО_2	ЗО_3	ЗО_4	ЗО_5	ЗО_6	ЗО_7	ЗО_8	ЗО_9	ЗО_10	∑
АС_1	1	1	2	0	0	1	1	1	2	2	1	1	0	0	13
АС_2	1	1	1	1	1	1	1	1	2	2	1	1	0	0	14
АС_3	1	1	1	1	1	1	2	1	2	2	2	1	1	0	17
АС_4	1	1	2	1	1	1	1	1	2	2	1	1	0	0	15
АС_5	2	1	2	1	1	2	2	1	1	1	2	2	1	0	19
АС_6	2	1	1	1	2	2	2	1	1	1	1	1	1	1	18
АС_7	2	1	1	2	1	2	2	1	2	1	2	2	1	1	21
АС_8	1	1	1	1	1	2	1	1	2	1	2	1	1	1	17
АО_1	0	1	0	0	2	1	0	1	0	0	2	1	0	2	10
АО_2	1	1	2	1	1	2	2	1	2	1	2	1	1	1	19
АО_3	1	1	1	0	1	2	1	1	2	2	2	1	1	0	16
АО_4	2	1	2	0	1	1	2	1	2	2	2	0	0	0	16
АО_5	1	1	1	1	2	2	2	1	1	2	2	2	2	2	22
АО_6	2	1	2	1	1	2	2	1	2	2	2	1	1	0	20
АО_7	1	1	2	1	1	2	1	2	2	2	2	2	2	1	22
АО_8	1	1	2	2	1	2	2	1	2	1	2	2	1	2	22
АО_9	2	1	2	1	1	2	1	1	2	1	1	1	1	1	18
∑	22	17	25	15	19	28	25	18	29	25	29	21	14	12	

Примечание. *Используются следующие цветовые обозначения результативности методов (кроме последних столбца и строки): красный – не применяется, белый – частично влияет на защиту, зеленый – полностью нейтрализует атаку. Также цветовая градация для последнего столбца показывает интегральную опасность атаки: от зеленого к красному, а для последней строки – интегральную результативность защиты – от красного к зеленому.*

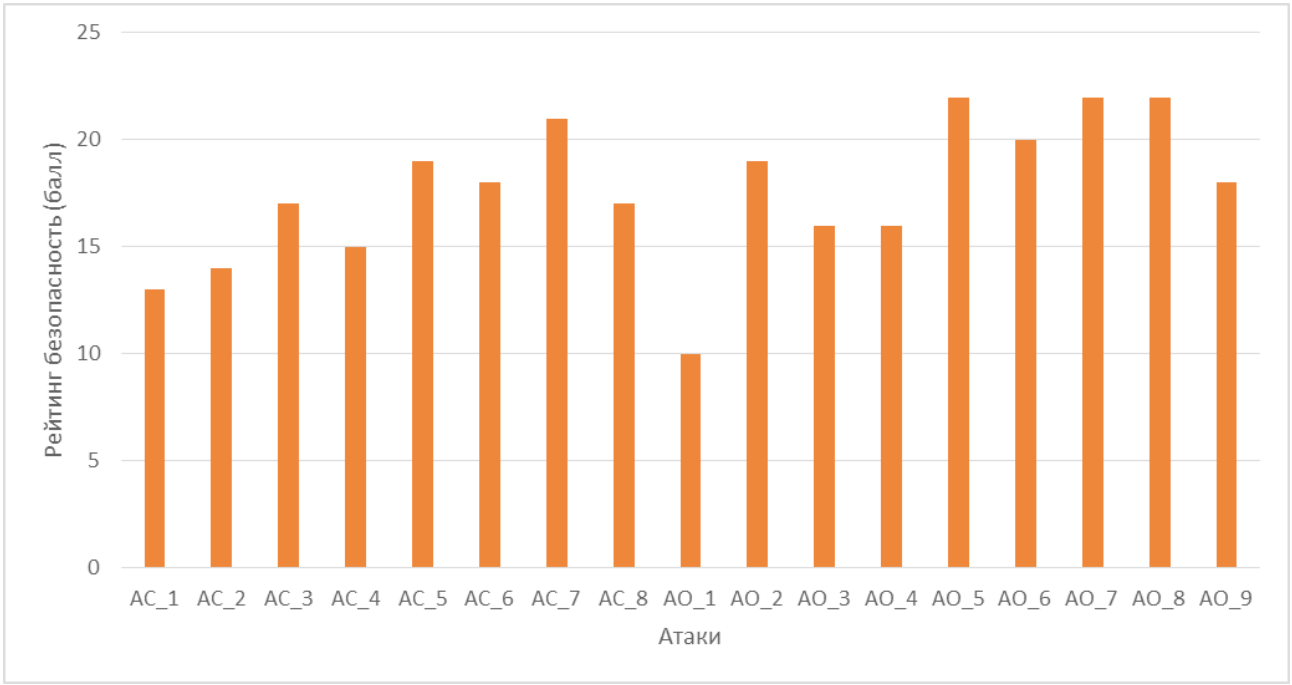

Рис.2. Рейтинг опасности атак на VoIP

методы в основном относятся к области сетевой защиты, что не подходит для физической. На втором и третьем местах оказались точечно направленные специализированные атаки на SIP, которые в большинстве случаев включаются в остальные атаки, являясь их началом; поэтому их сложно отследить по системам мониторинга подозрительной активности.

Рейтинг результативности методов защиты согласно значениям в крайней нижней строке приведен в виде гистограммы на рис. 3.

Как результат, можно выделить Топ-3 наиболее результативных методов защиты от всего множества атак на VoIP:

— 3О_5. Внедрение криптосистем и протоколов шифрования; 3О_7. Мониторинг подозрительной активности и внедрение системы обнаружения и предотвращения вторжений (29 баллов);
— 3О_2. Управление доступом и проверка на соответствие принадлежности устройства сети (28 баллов);
— 3С_3. Объединение подразделений компании в общую VPN сеть; 3О_3. Применение планов маршрутизации и звонков; 3О_6. Применение программных и аппаратных межсетевых экранов (25 баллов).

Первое место сразу двух методов 3О_5 и 3О_7 объясняется тем, что достаточно результативным является как защита самих данных (шифрованием), так и доступа к ним (предотвращением вторжений). Наличие метода 3О_2 на втором месте обосновывается тем, что большинство многошаговых атак начинается с получения доступа к корпоративному оборудованию, против чего высокую результативность показывают методы управления доступом. На третьем месте расположились методы (3С_3, 3О_3, 3О_6), который в основном посвящены управлению сетевыми каналами передачи трафика, что может считаться значимым дополнением к методам на первых двух местах.

Заключение

В работе проведена систематизация основных способов атаки на VoIP, как специализированные и общие; первая группа получена на основании анализа Best Practices, а вторая – из научных публикаций. Как результат, список наиболее актуальных атак содержит 17 элементов. Аналогичным образом получен список (из 14 элементов) наиболее часто применяемых методов защиты, частично или полностью применяемых хотя бы для одной из атак.

Перекрестное наложение множества способов атак на множество защит от атак позволит сформировать модель защиты, представленную в табличном виде (в виде таблицы из 17 строк и 14 столбцов). Модель расширена введением в таблицу дополнительного столбца опасности каждого способа атаки и строки результативности каждого метода защиты. Экспертный анализ модели выявил целесообразность ее дополнения значениями результативности противодей-

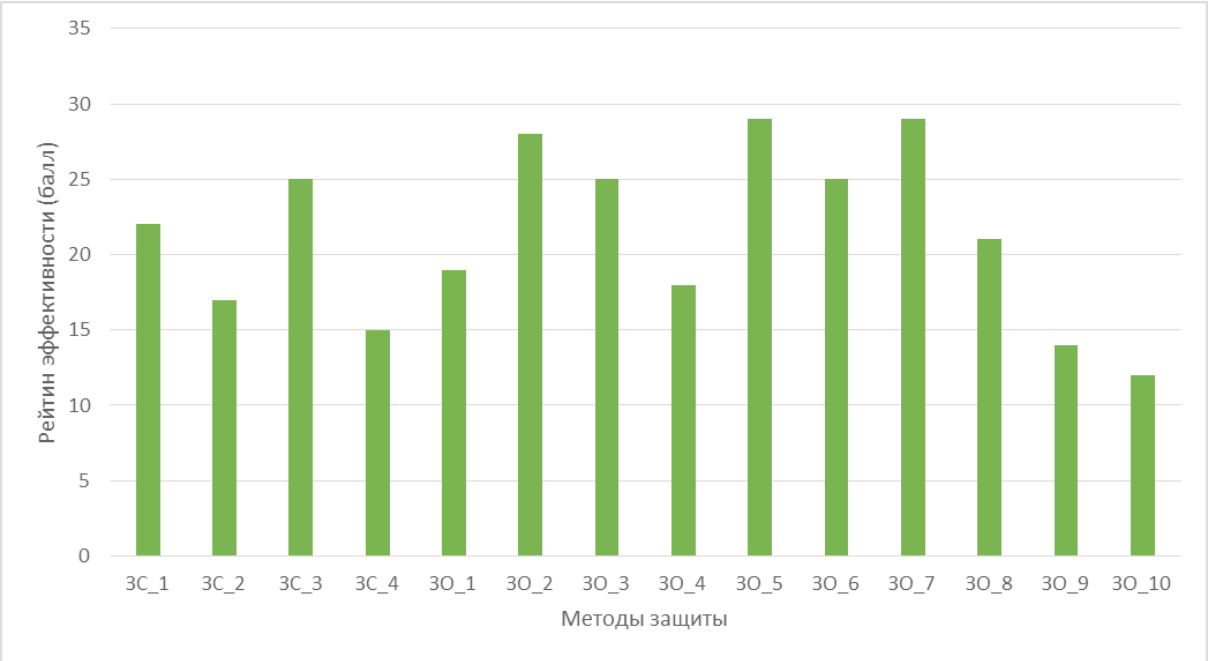

Рис. 3. Рейтинг результативности методов защиты от атак на VoIP

ствия каждого из методов защиты каждой атаке – что указано в ячейках табличного представления модели. Также, были выявлены Топ-3 наиболее опасных атак и наиболее результативных защит.

Теоретическая значимость модели, помимо более широкого охвата предметной области безопасности VoIP с позиции противодействия атакам, заключается в экспертном получении характеристик каждого способа атаки и метода защиты, а также принципа их ранжирования (задача, которой уделяется крайне мало внимания со стороны научной общественности) [30, 31, 32].

Практическая значимость модели заключается в получении формального аппарата для выбора необходимого набора методов защиты, позволяющего с нужной результативностью противодействовать актуальному пулу атак на VoIP.

Продолжением исследования должно стать экспериментальное уточнение модели в части результативности противодействия атакам методами защиты, поскольку в настоящее время носит эвристический характер. Требуется дальнейшее развитие математического аппарата как для формирования списка строк и столбцов табличного представления модели защиты VoIP, так и для аналитического вычисления значений их элементов [33, 34, 35].

Статья подготовлена в рамках выполнения в 2023 году прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР №1022052000002-2-2.2.6; 2.11.2.

Лиература

1. Калашников А.О., Бугайский К.А. Модель оценки безопасности сложной сети. (часть 1) // Вопросы кибербезопасности. 2022. № 4 (50). С. 26-38.
2. Перминов А.А., Тезин А.В. Повышение защищенности использования протокола SIP в IP-АТС на платформе Asterisk // Технические и математические науки. Студенческий научный форум : сборник статей по материалам LVI студенческой международной научно-практической конференции (Москва, 14 декабря 2022 года). Том 11 (56). 2022. С. 63-73.
3. Conti M., Dragoni N., Lesyk V. A Survey of Man In The Middle Attacks // IEEE Communications Surveys & Tutorials. Vol. 18. No. 3. PP. 2027-2051.
4. Кузьмин Ю.А. Предупреждение телефонного мошенничества (криминологический аспект) // Oeconomia et Jus. 2022. № 3. С. 47-54.
5. Шендевицкий И.М., Сячин К.И. Исследование стандарта аудиокомпандирования G.711 используемого в оборудовании мультиплексирования // Студенческий вестник. 2023. № 1-10 (240). С. 70-75.
6. Липатников В.А., Шевченко А.А., Косолапов В.С., Сокол Д.С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя // Информационно-управляющие системы. 2022. № 1 (116). С. 54-67.
7. Алексеев А.С., Сокол Д.С. Обеспечение защищённости VoIP // Вестник современных исследований. 2019. № 3.3(30). С. 4-8.
8. Tas I.M., Unsalver B.G., Baktir S. A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism // IEEE Access. 2020. V. 8. PP. 112574-112584.
9. Zhou C.V., Leckie C., Ramamohanarao K. Protecting SIP server from CPU-based DoS attacks using history-based IP filtering // IEEE Communications Letters. Vol. 13. No. 10. PP. 800-802.
10. Srivatsa M., Iyengar A., Liu L., Jiang H. Privacy in VoIP Networks: Flow Analysis Attacks and Defense // IEEE Transactions on Parallel and Distributed Systems. Vol. 22. No. 4. PP. 621-633.
11. Mentsiev A.U., Dzhangarov A.I. VoIP security threats // Ingineering Journal of Don. 2019. No 1(52). P. 75.
12. Mochalov V.P., Bratchenko N.Yu., Palkanov I.S., Aliev E.V. Mathematical model of the load balancing system of DPC server clusters under fractal load conditions // Modern Science and Innovations. 2022. № 4 (40). С. 41-49.
13. Акилов М.В., Ковцур М.М., Несудимов Е.Ю., Потемкин П.А. Исследование методик обнаружения уязвимостей Web-приложений IAST и SAST // Информационная безопасность регионов России (ИБРР-2021): Материалы XII Санкт-Петербургской межрегиональной конференции (Санкт-Петербург, 27–29 ноября 2021 г.). 2021. С. 378-379.
14. Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И. Предупреждение dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70-77
15. Melih Tas I., Unsalver B.G., Baktir S. A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism // IEEE Access. 2020. Т. 8. С. 112574-112584.
16. Макарова А.К., Поляничева А.В., Саматова К.А. Анализ уязвимостей оборудования передачи голосового трафика // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022) : сборник научных статей XI Международной научно-технической и научно-методической конференции (Санкт-Петербург, 15–16 февраля 2022 г.). 2022. С. 665-669.
17. Слончак Э.В., Шабалин А.М. Организация IP-телефонии в сети предприятия // Математическое и информационное моделирование : материалы Всероссийской конференции молодых ученых (Тюмень, 18–23 мая 2022 года). 2022. С. 310-318.
18. Зурахов В.С., Андрианов В.И., Давыдович И.В., Степанова А.А., Методология проведения стресс тестирования на целевой вебсервер в целях поиска скрытых уязвимостей // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 59-62.

19. Елисеев Д.И., Савельев Е.А., Иванов Д.А., Ачкасов Н.Б. Проблемы защиты речевых сервисов в мультисервисной сети специального назначения // Известия Тульского государственного университета. Технические науки. 2021. № 2. С. 290-300.
20. Березина Е.О., Виткова Л.А., Ахрамеева К.А., Классификация угроз информационной безопасности в сетях IOT // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 2. С. 11-18.
21. Штеренберг С.И., Полтавцева М.А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59-68.
22. Butcher D., Li X., Guo J. Security Challenge and Defense in VoIP Infrastructures // IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). Vol. 37. No. 6. PP. 1152-1162.
23. Rohloff K., Cousins D.B., Sumorok D. Scalable, Practical VoIP Teleconferencing With End-to-End Homomorphic Encryption // IEEE Transactions on Information Forensics and Security. Vol. 12. No. 5. PP. 1031-1041.
24. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Detection of stego-insiders in corporate networks based on a hybrid NoSQL database model // The proceedings of 4th International Conference on Future Networks and Distributed Systems (New York, USA, 26-27 november 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442612.
25. Kotenko I., Krasov A., Ushakov I., Izrailov K. Approach to combining different methods for detecting insiders // The proceedings of 4th International Conference on Future Networks and Distributed Systems (New York, USA, 26-27 november 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442619.
26. Скорых М.А., Израилов К.Е., Башмаков А.В. Задачаориентированное сравнение средств анализа сетевого трафика // Теория и практика обеспечения информационной безопасности: сборник научных трудов по материалам Всероссийской научно-теоретической конференции (Москва, 03 декабря 2021 г.). 2021. С. 103-107.
27. Дибиров Г.М., Бабков И.Н., Ковцур М.М. Сравнительный анализ решений для контейнеризации // Молодежная школа-семинар по проблемам управления в технических системах имени А.А. Вавилова. 2022. Т. 1. С. 27-29.
28. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335
29. Izrailov K., Levshun D., Kotenko I., Chechulin A. Classification and analysis of vulnerabilities in mobile device infrastructure interfaces // Communications in Computer and Information Science. 2022. Т. 1544 CCIS. PP. 301-319. DOI: 10.1007/978-981-16-9576-6_21
30. Буйневич М.В., Ахунова Д.Г., Ярошенко А.Ю. Комплексный метод решения типовой задачи риск-менеджмента в инфологической среде (на примере ранжирования требований пожарной безопасности). Часть 1 // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2020. № 3. С. 88-99.
31. Буйневич М.В., Ахунова Д.Г., Ярошенко А.Ю. Комплексный метод решения типовой задачи риск-менеджмента в инфологической среде (на примере ранжирования требований пожарной безопасности). Часть 2 // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2020. № 4. С. 78-89.
32. Ярошенко А.Ю. Предпосылки к необходимости непрерывного ранжирования требований пожарной безопасности // Национальная безопасность и стратегическое планирование. 2021. № 3 (35). С. 100-105.
33. Буйневич М.В., Матвеев А.В., Смирнов А.С. Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2022. № 3. С. 1-17.
34. Бородушко И.В., Матвеев А.В., Максимов А.В. Информационно-аналитическая поддержка проблемно-ориентированного управления стратегически значимыми организационными системами России // Современные наукоемкие технологии. 2022. № 7. С. 26-31.
35. Израилов К.Е., Буйневич М.В., Котенко И.В., Десницкий В.А. Оценивание и прогнозирование состояния сложных объектов: применение для информационной безопасности // Вопросы кибербезопасности. 2022. № 6(52). С. 2-21. DOI 10.21681/23113456-6-2022-2-21.

PROTECTION GENERALIZED MODEL AGAINST CYBER ATTACKS ON VOIP

Izrailov K.E.[4], Makarova A.K.[5], Shestakov A.V.[6]

The goal of the study *creation of a protection model against cyberattacks on information and telecommunication resources used in practice Internet voice exchange services (VoIP).*

Research methods: *analysis of Best Practices and scientific publications, system analysis, criterion comparison.*

4 Konstantin E. Izrailov, Ph.D., Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. Russia. ORCHID: https://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru.

5 Alexandra K. Makarova, Student of The Bonch-Bruevich Saint-Petersburg state university of telecommunications, Saint-Petersburg. Russia. ORCHID: https://orcid.org/0000-0001-7745-3364. Scopus Author ID: . E-mail: alex-ecureuil@mail.ru.

6 Alexander V. Shestakov, Dr.Sc., Senior Researcher, Assistant chief of Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint-Petersburg. ORCHID: https://orcid.org/0000-0002-8462-6515. Scopus Author ID: 57219712387. E-mail: alexandr.shestakov01@yandex.ru.

Result: *systematization of the cyberattacks main methods on VoIP and methods of protection against them, based on existing Best Practices and scientific publications. The investigation methodological scheme presented in a schematic form, is described. As a result, a list of 8 specialized and 9 main methods of cyberattacks, as well as 4 specialized and 10 main methods of protection was obtained, which made it possible to create a protection generalized model against cyberattacks on VoIP. The model representation in tabular form consists of 17 rows and 14 columns, which corresponds to the number of all cyberattack methods and protection methods. The cells of the table contain expertly obtained values of the effectiveness of counteracting cyberattacks by each of the protection methods according to a 3-point system. The model is extended with additional integral indicators of the danger of cyberattacks and the effectiveness of protection obtained analytically. 3 cyberattacks least amenable to protection and 3 most effective protection methods were identified.*

The scientific novelty *consists in bringing together the whole set of cyberattacks methods on VoIP and protection against them methods into a single system that characterizes the effectiveness of countering.*

Keywords: *VoIP, cyberattack method, protection method, protection model, categorical division*

References

1. Kalashnikov A.O., Bugayskiy K.A. Model' otsenki bezopasnosti slozhnoy seti. (chast' 1) // Voprosy kiberbezopasnosti. 2022. № 4 (50). S. 26-38.
2. Perminov A.A., Tezin A.V. Povysheniye zashchishchennosti ispol'zovaniya protokola SIP v IP-ATS na platforme Asterisk // Tekhnicheskiye i matematicheskiye nauki. Studencheskiy nauchnyy forum : sbornik statey po materialam LVI studencheskoy mezhdunarodnoy nauchno-prakticheskoy konferentsii (Moskva, 14 dekabrya 2022 goda). Tom 11 (56). 2022. S. 63-73.
3. Conti M., Dragoni N., Lesyk V. A Survey of Man In The Middle Attacks // IEEE Communications Surveys & Tutorials. Vol. 18. No. 3. PP. 2027-2051.
4. Kuz'min YU.A. Preduprezhdeniye telefonnogo moshennichestva (kriminologicheskiy aspekt) // Oeconomia et Jus. 2022. № 3. S. 47-54.
5. Shendevitskiy I.M., Syachin K.I. Issledovaniye standarta audiokompandirovaniya G.711 ispol'zuyemogo v oborudovanii mul'tipleksirovaniya // Studencheskiy vestnik. 2023. № 1-10 (240). S. 70-75.
6. Lipatnikov V.A., Shevchenko A.A., Kosolapov V.S., Sokol D.S. Metod obespecheniya informatsionnoy bezopasnosti seti VoIP-telefonii s prognozom strategii vtorzheniy narushitelya // Informatsionno-upravlyayushchiye sistemy. 2022. № 1 (116). S. 54-67.
7. Alekseyev A.S., Sokol D.S. Obespecheniye zashchishchonnosti VoIP // Vestnik sovremennykh issledovaniy. 2019. № 3.3(30). C. 4-8.
8. Tas I.M., Unsalver B.G., Baktir S. A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism // IEEE Access. 2020. V. 8. PP. 112574-112584.
9. Zhou C.V., Leckie C., Ramamohanarao K. Protecting SIP server from CPU-based DoS attacks using history-based IP filtering // IEEE Communications Letters. Vol. 13. No. 10. PP. 800-802.
10. Srivatsa M., Iyengar A., Liu L., Jiang H. Privacy in VoIP Networks: Flow Analysis Attacks and Defense // IEEE Transactions on Parallel and Distributed Systems. Vol. 22. No. 4. PP. 621-633.
11. Mentsiev A.U., Dzhangarov A.I. VoIP security threats // Ingineering Journal of Don. 2019. No 1(52). P. 75.
12. Mochalov V.P., Bratchenko N.Yu., Palkanov I.S., Aliev E.V. Mathematical model of the load balancing system of DPC server clusters under fractal load conditions // Modern Science and Innovations. 2022. № 4 (40). C. 41-49.
13. Akilov M.V., Kovtsur M.M., Nesudimov Ye.YU., Potemkin P.A. Issledovaniye metodik obnaruzheniya uyazvimostey Web-prilozheniy IAST i SAST // Informatsionnaya bezopasnost' regionov Rossii (IBRR-2021): Materialy XII Sankt-Peterburgskoy mezhregional'noy konferentsii (Sankt-Peterburg, 27–29 noyabrya 2021 g.). 2021. S. 378-379.
14. Lavrova D.S., Popova Ye.A., Shtyrkina A.A., Shterenberg S.I. Preduprezhdeniye dos-atak putem prognozirovaniya znacheniy korrelyatsionnykh parametrov setevogo trafika // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2018. № 3. S. 70-77
15. Melih Tas I., Unsalver B.G., Baktir S. A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism // IEEE Access. 2020. T. 8. C. 112574-112584.
16. Makarova A.K., Polyanicheva A.V., Samatova K.A. Analiz uyazvimostey oborudovaniya peredachi golosovogo trafika // Aktual'nyye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2022) : sbornik nauchnykh statey XI Mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii (Sankt-Peterburg, 15–16 fevralya 2022 g.). 2022. S. 665-669.
17. Slonchak E.V., Shabalin A.M. Organizatsiya IP-telefonii v seti predpriyatiya // Matematicheskoye i informatsionnoye modelirovaniye : materialy Vserossiyskoy konferentsii molodykh uchenykh (Tyumen', 18–23 maya 2022 goda). 2022. S. 310-318.
18. Zurakhov V.S., Andrianov V.I., Davydovich I.V., Stepanova A.A., Metodologiya provedeniya stress testirovaniya na tselevoy veb-server v tselyakh poiska skrytykh uyazvimostey // Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizayna. Seriya 1: Yestestvennyye i tekhnicheskiye nauki. 2021. № 1. S. 59-62.
19. Yeliseyev D.I., Savel'yev Ye.A., Ivanov D.A., Achkasov N.B. Problemy zashchity rechevykh servisov v mul'tiservisnoy seti spetsial'nogo naznacheniya // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskiye nauki. 2021. № 2. S. 290-300.
20. Berezina Ye.O., Vitkova L.A., Akhrameyeva K.A., Klassifikatsiya ugroz informatsionnoy bezopasnosti v setyakh IOT // Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizayna. Seriya 1: Yestestvennyye i tekhnicheskiye nauki. 2020. № 2. S. 11-18.
21. Shterenberg S.I., Poltavtseva M.A. Raspredelennaya sistema obnaruzheniya vtorzheniy s zashchitoy ot vnutrennego narushitelya // Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy. 2018. № 2. S. 59-68.

22. Butcher D., Li X., Guo J. Security Challenge and Defense in VoIP Infrastructures // IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). Vol. 37. No. 6. PP. 1152-1162.
23. Rohloff K., Cousins D.B., Sumorok D. Scalable, Practical VoIP Teleconferencing With End-to-End Homomorphic Encryption // IEEE Transactions on Information Forensics and Security. Vol. 12. No. 5. PP. 1031-1041.
24. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Detection of stego-insiders in corporate networks based on a hybrid NoSQL database model // The proceedings of 4th International Conference on Future Networks and Distributed Systems (New York, USA, 26-27 november 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442612.
25. Kotenko I., Krasov A., Ushakov I., Izrailov K. Approach to combining different methods for detecting insiders // The proceedings of 4th International Conference on Future Networks and Distributed Systems (New York, USA, 26-27 november 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442619.
26. Skorykh M.A., Izrailov K.Ye., Bashmakov A.V. Zadachaoriyentirovannoye sravneniye sredstv analiza setevogo trafika // Teoriya i praktika obespecheniya informatsionnoy bezopasnosti: sbornik nauchnykh trudov po materialam Vserossiyskoy nauchno-teoreticheskoy konferentsii (Moskva, 03 dekabrya 2021 g.). 2021. S. 103-107.
27. Dibirov G.M., Babkov I.N., Kovtsur M.M. Sravnitel'nyy analiz resheniy dlya konteynerizatsii // Molodezhnaya shkola-seminar po problemam upravleniya v tekhnicheskikh sistemakh imeni A.A. Vavilova. 2022. T. 1. S. 27-29.
28. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335
29. Izrailov K., Levshun D., Kotenko I., Chechulin A. Classification and analysis of vulnerabilities in mobile device infrastructure interfaces // Communications in Computer and Information Science. 2022. T. 1544 CCIS. PP. 301-319. DOI: 10.1007/978-981-16-9576-6_21
30. Buynevich M.V., Akhunova D.G., Yaroshenko A.YU. Kompleksnyy metod resheniya tipovoy zadachi risk-menedzhmenta v infologicheskoy srede (na primere ranzhirovaniya trebovaniy pozharnoy bezopasnosti). Chast' 1 // Nauchno-analiticheskiy zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoy protivopozharnoy sluzhby MCHS Rossii». 2020. № 3. S. 88-99.
31. Buynevich M.V., Akhunova D.G., Yaroshenko A.YU. Kompleksnyy metod resheniya tipovoy zadachi risk-menedzhmenta v infologicheskoy srede (na primere ranzhirovaniya trebovaniy pozharnoy bezopasnosti). Chast' 2 // Nauchno-analiticheskiy zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoy protivopozharnoy sluzhby MCHS Rossii». 2020. № 4. S. 78-89.
32. Yaroshenko A.YU. Predposylki k neobkhodimosti nepreryvnogo ranzhirovaniya trebovaniy pozharnoy bezopasnosti // Natsional'naya bezopasnost' i strategicheskoye planirovaniye. 2021. № 3 (35). S. 100-105.
33. Buynevich M.V., Matveyev A.V., Smirnov A.S. Aktual'nyye problemy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti MCHS Rossii i konstruktivnyye podkhody k ikh resheniyu // Nauchno-analiticheskiy zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoy protivopozharnoy sluzhby MCHS Rossii». 2022. № 3. S. 1-17.
34. Borodushko I.V., Matveyev A.V., Maksimov A.V. Informatsionno-analiticheskaya podderzhka problemno-oriyentirovannogo upravleniya strategicheski znachimymi organizatsionnymi sistemami Rossii // Sovremennyye naukoyemkiye tekhnologii. 2022. № 7. S. 26-31.
35. Izrailov K.Ye., Buynevich M.V., Kotenko I.V., Desnitskiy V.A. Otsenivaniye i prognozirovaniye sostoyaniya slozhnykh ob»yektov: primeneniye dlya informatsionnoy bezopasnosti // Voprosy kiberbezopasnosti. 2022. № 6(52). S. 2-21. DOI 10.21681/23113456-6-2022-2-21.