DOI 10.36622/VSTU.2023.26.2.004
УДК 004.8

РИСК-МОДЕЛЬ АТАКУЕМОГО КАНАЛА СВЯЗИ БЕСПРОВОДНЫХ СЕТЕЙ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ VPN

Н.М. Радько, Ю.С. Хирьянова, А.Н. Мокроусов, Е.А. Москалева

В работе представлены методические и алгоритмические способы оценки рисков нарушения функционирования канала беспроводной связи. Особенностью рассматриваемой среды является повсеместное применение услуг VPN – протоколов, оборудования, алгоритмов шифрования. В научной публикации проведен анализ актуальных VPN-сервисов, их криптографических особенностей, функционала. На основе проведенного исследования построена математическая модель стойкости и безопасности вышеописанной технологии, предложена риск-модель атакуемого канала связи беспроводной сети, оснащенный VPN технологией в виде протоколов, оборудования или программно-аппаратного комплекса. Помимо этого, выработана классификация атак на канал связи беспроводной сети, целью которых является получение несанкционированного доступа к информационным ресурсам закрытого сегмента сети с VPN, а также нарушение их конфиденциальности и целостности. Полученные в ходе исследования результаты могут быть использованы для повышения криптостойкости канала связи беспроводных сетей на этапах проектирования, а также как базис для дальнейших исследований специалистов в области информационной безопасности.

Ключевые слова: VPN, канал связи, уязвимость, риск, угроза.

Введение

В связи с повсеместно происходящими информационными взрывами [1-3] на фоне специальной военной операции среди наиболее явных угроз выделяется оказание вредоносного воздействия на канал связи беспроводных сетей с применением технологий Virtual Private Network (VPN).

В настоящее время беспроводные сети связи и VPN-технологии стали неотъемлемой частью нашей повседневной жизни, обеспечивая нам доступ к интернету в любой точке мира. Огромное распространение имеют и беспроводные сети связи, такие как Wi-Fi и Bluetooth, ведь любая организация передает информацию различного вида с их помощью. Как и любая другая технология, они не лишены уязвимостей и могут быть подвержены рискам нарушения криптостойкости канала связи и утечке конфиденциальной информации. Для обеспечения требуемого уровня криптостойкости необходимо знать потенциальные угрозы и уязвимости беспроводных сетей связи, к которым можно отнести:

- хищение информационных ресурсов,
- перехват и изменение передаваемых данных в целях нарушения целостности и конфиденциальности канала связи,
- прослушивание незащищенного канала связи беспроводной сети,
- отказные технологии, которые нарушают функционирование базовых элементов сети,
- «глушение» базовой станции клиента.

Сегодня доступны различные методы шифрования информации в канале связи [4]. Эти технологии используются для шифрования интернет-трафика в целях защиты конфиденциальности пользователей интернета от угроз безопасности. Таким образом, существует необходимость в повышении криптозащищенности канала беспроводных сетей связи с применением технологии VPN. Результаты данного исследования направлены на выявление уязвимостей, возникающих в процессе использования беспроводных сетей, а также на разработку мер по их минимизации.

В ходе работы мы будем использовать современные методы оценки рисков, такие как анализ угроз, оценку уязвимостей и вероятности их эксплуатации, а также оценку последствий нарушения криптостойкости канала связи.

В результате мы сможем предложить эффективные стратегии оценки и управления рисками, классификацию вредоносных атак на компоненты канала связи, а также мероприятия по ликвидации «белых пятен» сети, которые увеличат показатель безопасности в ходе использования VPN-технологий, а также облегчат управление сетью, предотвращая вредоносные вторжения на определенных этапах.

Анализ современных VPN технологий

На данный момент существует достаточное множество сервисов, предоставляющих VPN услуги. Они отличаются протоколами шифрования и функционалом. Рассмотрим актуальные сервисы на момент 2023 года и проанализируем их криптографические параметры на возможность дальнейшего нарушения криптоустойчивости (табл.1).

Таблица 1

Популярные VPN-сервисы в 2023 году

VPN 2023г	**Протоколы шифрования**	**Технология обмена ключами**	**Шифрование канала передачи данных**
ExpressVPN	Lightway, OpenVPN IKEv2 WireGuard L2TP/IPsec SSTP PPTP	Ключ формируется на основе протокола Диффи-Хеллмана на эллиптических кривых	Симметричная схема шифрования AES (Advanced Encryption Standart) с 256-битным ключом
NordVPN	OpenVPN Internet Key Exchange v2/IPsec L2TP/IPsec PPTP	Набор шифров xChaCha20 защищает цепочку ключей и идентификационные данные	Архитектура с нулевым разглашением. Сквозное шифрование, AES-256, схема цифровой подписи Ed25519 обеспечивает безопасность цифровых подписей
Surfshark	OpenVPN IKEv2/IPsec Shadowsocks WireGuard	Perfect Forward Secrecy (PFS) – каждая новая сессия использует новый ключ шифрования	Симметричная схема шифрования AES (Advanced Encryption Standart) с 256-битным ключомФункция Camouflage Mode – маскирование VPN трафика под обычный интернет-трафик HMAC SHA-384 для аутентификации

Продолжение табл. 1

VPN 2023г	Протоколы шифрования	Технология обмена ключами	Шифрование канала передачи данных
Private Internet Access	OpenVPN WireGuard IKEv2/IPSec	Diffie-Hellman Key Exchange (DH) - две стороны безопасно обмениваются ключами без необходимости предварительного обмена ключами	AES-256 Кроме того, поддерживает Perfect Forward Secrecy (PFS) с помощью TLS (Transport Layer Security), который обеспечивает защиту от перехвата и подмены данных
ProtonVPN	OpenVPN IKEv2/IPSec и L2TP/IPSec	Perfect Forward Secrecy (PFS), что означает, что каждая новая сессия использует новый ключ шифрования	AES-256 и RSA 4096 TLS (Transport Layer Security)
CyberGhost	L2TP/IPSec IKEv2 OpenVPN WireGuard	CyberGhost использует технологию обмена ключами Diffie-Hellman для установки безопасного канала передачи данных между пользователем и VPN-сервером. Эта технология позволяет двум сторонам, которые не имеют предварительно общего секрета, безопасно обмениваться ключами шифрования	Симметричная схема шифрования AES (Advanced Encryption Standart) с 256-битным ключом
AirVPN	OpenVPN IPSec и SSL/TLS	Perfect Forward Secrecy (PFS), что означает, что каждая новая сессия использует новый ключ шифрования	Симметричная схема шифрования AES (Advanced Encryption Standart) с 256-битным ключом RSA 4096 SSL/TLS
IPVanish	OpenVPN WireGuard IKEv2/IPSec SSTP PPTP L2TP/IPSec IPSec	Если используется протокол OpenVPN, IPVanish использует алгоритм обмена ключами Diffie-Hellman для создания защищенного канала связи. При использовании протокола IKEv2/IPSec, IPVanish использует технологию обмена ключами на основе протокола шифрования AES	Симметричная схема шифрования AES (Advanced Encryption Standart) с 256-битным ключом

Несмотря на то, что VPN-провайдеры учитывают дополнительные функции безопасности, актуальным остается вопрос выбора самой безопасной и надежной технологии, которая будет снижать существующие риски безопасности. Согласно табл. 1 можно сделать вывод о наличии следующих преимуществ и недостатков.

Уязвимости протокола шифрования PPTP можно использовать для нарушения функционирования в беспроводной сети связи с коммутируемым доступом.

Протокол L2TP встроен в большинство устройств, находящихся в среде связи с поддержкой технологии VPN, что делает его таким же простым в реализации, как и PPTP. Главной проблемой использования данного протокола является то, что предварительно используются общие ключи шифрования, которые можно загрузить с веб-сайта службы. Злоумышленник может использовать предварительный общий ключ, чтобы выдать свою станцию за VPN-сервер, а затем отслеживать зашифрованный трафик или даже внедрять вредоносный код в VPN-туннель. Тем не менее, данный протокол шифрования считается безопасным до тех пор, пока поставщик VPN-услуги не полагается на предварительно опубликованные ключи.

OpenVPN – протокол шифрования с открытым исходным кодом, которые многие считают текущим стандартом по безопасности VPN технологии. Фактически данный протокол состоит из двух каналов шифрования – канала данных и канала управления, которые при правильной настройке могут повысить уровень криптозащищенности сети. Однако чем сильнее шифрование, тем медленнее соединение. В результате некоторые вышеописанные провайдеры снижают уровень шифрования в канале данных.

Secure Socket Tunneling Protokol (SSTP) предлагает те же преимущества, что и протокол OpenVPN. Однако, SSTP не является протоколом с открытым исходным кодом, что может быть преимуществом при интеграции VPN-технологии с платформой Windows. Из минусов можно отметить отсутствие интеграции с другими платформами и обрыв SSTP-соединения при переключении между сетями, а использование надежного алгоритма шифрования может отрицательно повлиять на пропускную способность сети.

Протокол WireGuard – протокол шифрования с открытым исходным кодом. Данный протокол использует такие алгоритмы шифрования как ChaCha20, Curve25519, BLAKE2s, SipHash24, HKDF, что делает его более безопасным по сравнению с другими протоколами. Криптография, которую использует WireGuard, обеспечивает более высокую пропускную способность по сравнению с другими решениями в области виртуальных частных сетей. Из минусов можно отметить назначение одного и того же IP-адреса даже с переподключением.

L2TP/IPSec – дополнительный безопасный протокол VPN. Шифрование в данной технологии является надежным, отсутствуют серьезные недостатки. Однако у протокола L2TP/IPsec существуют проблемы с брандмауэром, его сложно настроить на сервере Linux.

IKEv2 выполняет функцию аутентификации пользователя и VPN-сервера. VPN сервисы, использующие IKEv2 протокол, будут идеальном вариантом для настройки в беспроводных сетях с увеличенным количеством мобильных устройств.

Данный протокол устойчив к атакам типа «отказ в обслуживании», ведь перед обработкой сетевых запросов существует проверка фактического существования запрашивающей стороны. Также, шифрование данной технологии включает в себя множество криптографических алгоритмов, таких как Blowfish, Camellia и AES-256. Аутентификация на основе сертификатов отлично подходит для предотвращения атак типа «человек посередине», поскольку протокол отклоняет любые действия без подтверждения личности запрашивающего. Из минусов можно выделить использование только порта UDP 500, поскольку брандмауэры или сетевые администраторы могут легко его заблокировать.

Классификация атак на канал связи беспроводных сетей с применением технологий VPN

Потоком атак на канал связи беспроводных сетей можно считать конкретное действие или последовательность действий, которые приводят к успеху угрозы методом использования уязвимостей системы. Существует огромное множество типов атак на канал связи беспроводных сетей, используемых для получения доступа к секретной информации или нарушения работоспособности сетей.

Рассмотрим основные классификации атак на компоненты канала связи беспроводных сетей с применением технологий VPN. По характеру воздействия атаки разделяются на [2] активные и пассивные. Пассивные атаки осуществляются без изменения динамики трафика. Примерами могут быть перехват и анализ трафика, а также сканирование сетей для определения уязвимых узлов сети. Активные атаки осуществляются в реальном времени, когда нарушитель перехватывает и изменяет трафик среды связи, делая его нечитаемым или поврежденным для дальнейшей передачи. Общую структуру активных и пассивных атак изобразим на рис. 1 (1-2 активная атака, 3-4 пассивная атака).

По цели воздействия атаки на компоненты канала связи можно выделить атаки, направленные на [2]:

- нарушение целостности информационных ресурсов;
- нарушение конфиденциальности информационных ресурсов;
- нарушение функционирования беспроводной сети в общем, невозможности получения доступа к системе.

Главной целью атак в системе канала связи беспроводной сети является получение несанкционированного доступа к информационным ресурсам, а также нарушение их конфиденциальности и целостности. Главными целями злоумышленника, атакующего канал связи беспроводной сети являются не только подключенные технологии VPN, но и базовые нарушения потока информации в системе: модификация, перехват, фальсификация, прерывание потока информации (рис. 1).

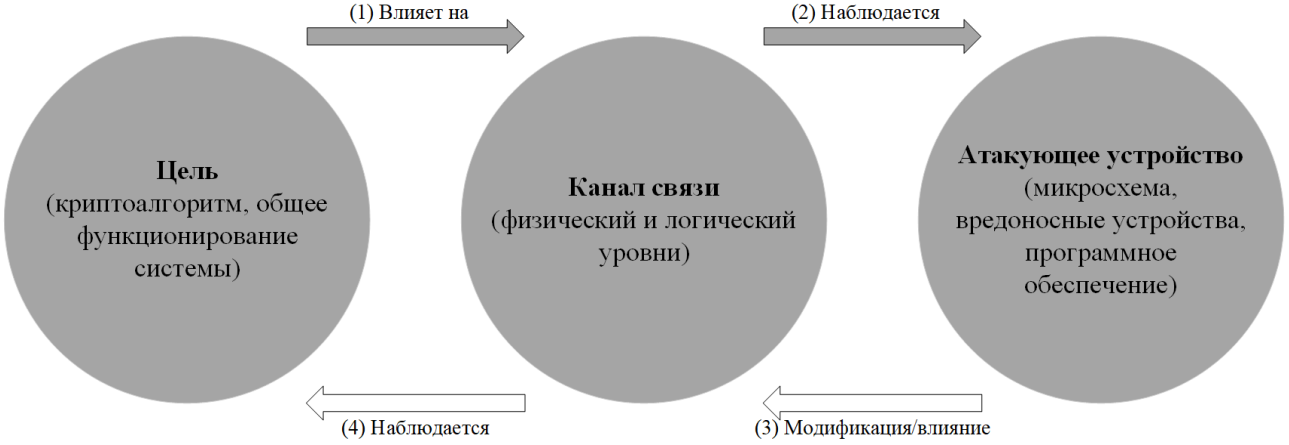

Рис. 1. Общая структура активных и пассивных атак

Прерывание информации заключается в нарушении функционала канала. При атаке этого типа трафик не доходит до адресата, доступность информации нарушается.

В ходе перехвата информации злоумышленник использует несанкционированный доступ к системе, при этом в трафике нарушаются показатели конфиденциальности.

При модификации пакета злоумышленник нарушает конфиденциальность информации в канале связи. Данная атака совершается с целью изменить функциональные свойства

информации, а также изменить содержимое пакетов.

В ходе фальсификации злоумышленник перехватывает пакет, идущий из точки беспроводной сети к пользователю сети, а после вносит в систему сети подложный пакет. При данной процедуре нарушается аутентичность информации.

На рис. 2 схематично представлен алгоритм.

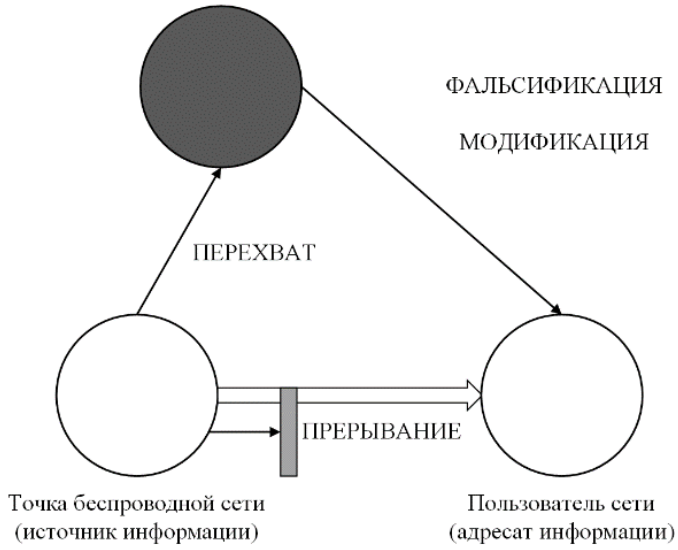

Рис. 2. Алгоритм атак на канал связи

Достаточно популярными являются атаки на побочные каналы связи беспроводной сети. При подобных атаках можем выделить два типа утечек информации: случайные и преднамеренные. Случайные утечки информации по каналу связи включают в себя, например, электромагнитное излучение вычислительного устройства, входящего в состав беспроводной сети. Преднамеренные же утечки конфиденциальной информации возникают, к примеру, из-за существования функции “поделиться”. Несмотря на то, что многие безопасные приложения используют эту функцию для благих целей, иногда эта информация попадает в руки злоумышленника, что ведет к разрушительным атакам на канал связи.

Математическая модель стойкости и безопасности технологии VPN

Грамотно настроенная технология VPN в сегменте сети должна обеспечивать передаваемый трафик не просто высокого качества, но и с сохранением достоверности информации для совокупности пользователей. Так называемыми “китами” качества технологии виртуальной частной сети являются ее стойкости и безопасность.

Проанализируем для выбранной услуги две модели: стойкости и безопасности. На рис. 3 представлена модель стойкости VPN со стороны пользователя в виде схемы с последовательным соединением блоков.

Рис.3.Схематичное представление модели VPN

Будем оценивать стойкость технологии виртуальной частной сети в виде показателя готовности к использованию данной технологии, который равен [2,3]

$$G_{\Gamma} = G_{\text{У}}^{2} G_{\text{ЛД}}^{2} G_{\text{СД}}^{2} G_{\text{ТС}} G_{\text{ПМ}}^{3} G_{\text{СЕРВ}} G_{\text{Б}},$$

где $G_У$ – показатель готовности личного устройства пользователя,

$G_{ЛД}$ – показатель завершенности абонентской линии,

$G_{СД}$ – показатель готовности к использованию сервера доступа,

$G_{ТС}$ – показатель готовности к использованию транспортной сети,

$G_{ПМ}$ – показатель готовности к использованию пограничного маршрутизатора сети,

$G_{СЕРВ}$ – показатель готовности к использованию сервера аутентификации, сервера сертификатов и сервера политики,

$G_{Б}$ – показатель готовности к использованию брандмауэра.

Рассмотрим общую модель стойкости сервера доступа как систему с такими видами резервирования, как нагруженный, ненагруженный и облегченный резервы. В сфере криптографической защиты, резервирование – это процесс создания резервной копии данных или системы в случае сбоя основной системы с сохранением критически важных данных. Перед тем, как мы опишем данную математическую модель подробнее, представим на рис. 4 основные части сервера доступа в виде схемы. Данная схема состоит из основного блока - технических инструментов сервера, а резервным блоком в данном случае являются аппаратно-программные инструменты сервера [3].

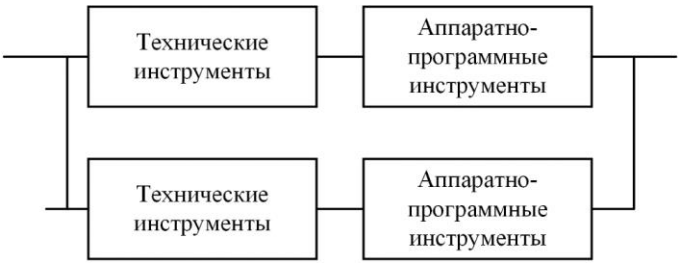

Рис. 4. Схематичное представление модели стойкости сервера доступа

Следует учитывать, что при нагруженном резерве все элементы системы работают одновременно. При успешной атаке на один компонент, другие компоненты системы не выходят из строя, а продолжают работу без перебоев. Ненагруженный резерв подразумевает наличие дополнительных компонентов, которые можно включить в работу системы при необходимости.

Облегченный резерв предполагает наличие в системе запасных компонентов на случай отказа. Несмотря на то, что не все из них являются полноценными по функционированию, в период атаки система может переключиться на них, чтобы продолжить функционирование.

Если соединить элементы сервера доступа последовательно, то показатель готовности к использованию системы равен интенсивности отказов системы, то есть скорости, с которой элементы системы при атаке выходят из строя или перестают стабильно работать [4]. Таким образом, получаем

$$G_{\Gamma} = \prod_{i=1}^{n} G_{gi}\,, \quad \lambda_{\text{с}} = \sum_{i=1}^{n} \lambda_i\,,$$

где G_{gi} - показатель готовности i-го компонента,

$G_{gi} = \lambda_i/\mu_i$,

μ_i – скорость, с которой элемент системы приходит к состоянию отказа,

n – количество всех элементов, входящих в систему.

Считаем, что интенсивность восстановлений системы – это мера скорости, с которой система может

восстанавливать свои функциональные показатели после различных атак или воздействий извне. Она характеризует уровень выносливости и адаптивности системы, а также ее готовность к скоростному восстановлению работоспособности. При параллельном соединении элементов данная мера равна коэффициенту простоя системы [5], т. е.

$$G_{П} = \prod_{i=1}^{n} G_{pi}, \quad \mu = \sum_{i=1}^{n} \mu_i,$$

где G_{pi} - показатель простоя i-го компонента.

Опишем показатели готовности системы в трех случаях, в зависимости от применяемого резервирования.

Если используется нагруженный резерв, состоящий из одного рабочего и одного запасного элемента, то готовность системы определяется следующим показателем $G_{Г}$, который выражается формулой [4,6]

$$G_{Г} = \frac{\mu^2 + 2\lambda\mu}{\mu^2 + 2\lambda\mu + 2\lambda^2},$$

где λ, μ – интенсивность отказов и восстановлений компонента системы.

Если же в системе используется ненагруженный резерв, то запасной (резервный) элемент не может выйти из строя. Конкретно в этом случае показатель готовности подобной системы вычисляется по следующей формуле:

$$G_{\Gamma} = \frac{\mu^2 + \lambda\mu}{\mu^2 + \lambda\mu + \lambda^2}.$$

При использовании системы с облегченным резервированием, следует учитывать возможность отказа запасного (резервного компонента), однако основной элемент продолжит функционировать и скорость выхода из строя резервного компонента (λ_2) меньше скорости выхода из строя основного компонента (λ_1), то есть показатель готовности системы в данном случае выражается по формуле [3]:

$$G = \frac{\mu^2 + (\lambda_1 + \lambda_2)\mu}{\mu^2 + (\lambda_1 + \lambda_2)(\lambda_1 + \mu)}.$$

Риск-модель атакуемого канала связи с учетом VPN-технологии

Способы оценки и регулирования рисков зависят от обнаружения вторжения нарушителей, атакующих канал связи.

Атакой в данном контексте будем считать действие злоумышленника или последовательность действий злоумышленника (имеющих общую направленность), которые влекут за собой реализацию угрозы методом давления на существующие уязвимости.

Мерой риска технологии VPN канала связи беспроводной сети является произведение величины ущерба на вероятность достижения именно этой величины.

Показатель защищенности будет поддерживаться в случае, когда величина риска меньше допустимого значения.

Структурная модель риска – это сложная система, которая включает в себя несколько компонентов риска $\{X_1, X_2 \dots X_n\}$, где n – количество компонентов риска. Одной из наиболее важных для расчетов является переменная Y, которая может принимать значения успеха или неуспеха. Эта бинарно-логическая операция принимает значение 1, если в системе присутствует риск, и значение 0, если данный риск отсутствует:

$$X_i = \begin{cases} 1, \text{с вероятностью } P_i, \\ \text{в случае неуспеха объекта,} \\ 0, \text{с вероятностью } Q_i = 1 - P_i. \end{cases}$$

При задании булевых переменных $X_i, i = \overline{1,n}$, где n – количество элементов, формирующих риск, мы можем описать риск неуспеха и предсказать итоговое событие с помощью логической модели

$$Y = Y(X_1, X_2, \dots, X_n).$$

Произведем замену аргументов X_i на показатель вероятности их истины $P_i = P\{X_i = 1\}$, логических операций – на арифметические операции. Эта замена

позволяет вычислить вероятностную модель риска конечного исхода с максимальной точностью [4].

$$P\{Y = 1/ X_1, X_2, \ldots, X_n\} = \psi(P_1, P_2, \ldots, P_n).$$

Свяжем с каждой компонентой X_i такие события как $\{X_{i1}, X_{i2}, \ldots, X_{iN_i}\}$, которые математически можно объединить в совокупность не связанных между собой событий, булевая переменная X_{ir} в логике принимает значение 1 с вероятностью

$$P_{ir}\left(P_{ir} = P\{X_i = 1/ X_{ir} = 1\}\right)$$

и значение 0 с вероятностью

$$Q_{ir} = 1 - P_{ir}.$$

Выявление и расчет вероятностей P_{ir} происходит по следующей формуле, аналогичной предыдущей:

$$P_i\{X_i = 1/ X_{i1}, X_{i2}, \ldots, X_{iN_i}\} = \psi(P_{i1}, P_{i2}, \ldots, P_{iN_i}).$$

Оценка вероятностей P_{ir} происходит в процессе алгоритмического итеративного обучения вероятностной модели риска на основе статистических данных [6,7].

Для вычисления вероятностей P_{ir} на основе статистической выборки применяется формула, позволяющая повысить точность и достоверность результатов оценки

$$P_{ir} = P1_{ir}(\overline{P_i} / \overline{P1_i}),$$

где $P1_{ir}$ – вероятность события в группе независимых событий, связанной с i-м объектом,

$$P1_{ir} = P\{X_{ir} = 1 / X_i = 1\},$$

$\bar{P}_i$, $\overline{P1_i}$ – статистические показатели среднего значения P_{ir}, $P1_{ir}$ для выборки независимых событий [6].

$$\overline{P1_i} = \sum_{r=1}^{N_i} P1_{ir} W_{ir}, \quad \overline{P_i} = \sum_{r=1}^{N_i} P_{ir} W_{ir},$$

где W_{ir} – показатель относительной частоты для выборки независимых событий;

$$W_{ir} = P\{X_{ir} = 1\}.$$

Применим теорию вероятности и логику для оценки рисков, существующих в канале связи беспроводной сети с применением технологии VPN.

Изобразим основные компоненты технологии VPN в виде схемы, результат представим на рис. 5.

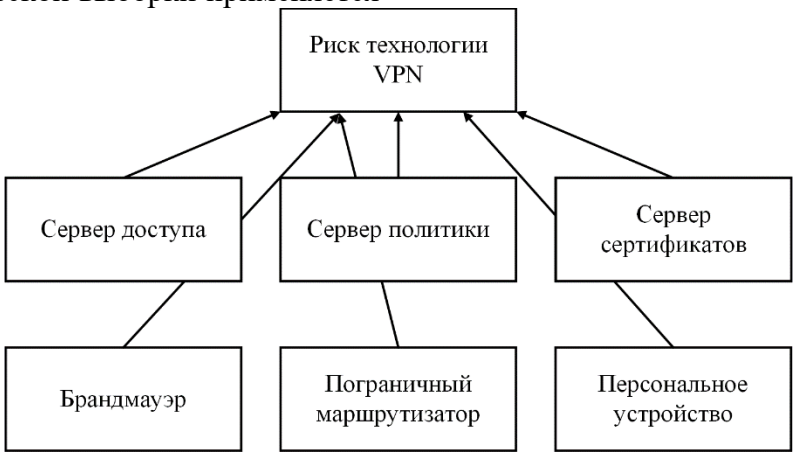

Рис.5.Составляющие риска технологии VPN

Составляющими риска $(X_i, i = \overline{1,n})$ можно считать сервера доступа, сертификации и политик, а также устройства для личного пользования. Криптоаналитик может нарушить конфиденциальность

информационных ресурсов только в том случае, когда в результате прохождения по преградам он получает результат “успех”. У каждой компоненты риска существует своя совокупность преград $(X_{ir}, r=\overline{1,N_i})$. Злоумышленником будет достигнут “успех” с вероятностью, равной

$$P_{риск} = 1 - P_{ПК}^2 P_{СД}^2 P_{СП} P_{СС} P_{ПМ} P_{ПЭ},$$

где $P_{ПК}$ – вероятность поддержания криптоустойчивости персонального устройства пользователя,

$P_{СД}$ – вероятность поддержания криптоустойчивости сервера доступа,

$P_{СС}$ – вероятность поддержания криптоустойчивости сервера сертификатов,

$P_{ПМ}$ – вероятность поддержания криптоустойчивости пограничного маршрутизатора,

$P_{МЭ}$ – вероятность поддержания криптоустойчивости брандмауэра,

$P_{СП}$ – вероятность поддержания криптоустойчивости сервера политики.

Вероятность поддержания криптоустойчивости $P_i^{защ}$ компонента риска X_i технологии VPN

$$P_i^{защ} = 1 - \prod_{r=1}^{N_i} P_{ir},$$

где N_i - количество шагов (этапов), которое необходимо преодолеть злоумышленнику для получения доступа к i-му объекту риска;

P_{ir} - вероятность того, что злоумышленник сможет преодолеть *r*-й преграду *i*-го компонента риска.

Каждый компонент меры риска технологии VPN имеет конкретный набор векторов (сценариев атак), обнаружить которые удается с помощью детального анализа, тестирования и диагностики системы.

Построенные риск-модели можно в дальнейшем использовать для оценки стойкости выбранной технологии VPN в канале связи беспроводной сети. Построения моделей будут происходить с помощью расчета показателей готовности компонентов данной услуги в выбранном канале связи. Итоговым этапом будет диагностика слабых звеньев в модели и организация мероприятий для повышения уровня криптозащищенности элемента или модели в целом.

Заключение

В процессе выполнения данного проекта была проанализирована текущая тенденция использования технологий VPN в канале связи беспроводных сетей. Актуальные сервисы были проанализированы на наличие уязвимостей в криптографическом ключе, были выделены их сильные и слабые стороны. была осуществлена классификация наиболее вредоносных атак на составные части вышеописанных услуг.

В работе были получены следующие результаты:

- проведен анализ функционала актуальных поставщиков VPN-технологий для беспроводных сетей связи, выявлены их угрозы и уязвимости. Приведены методические рекомендации для пользователей с разными ожиданиями от услуги VPN.

- в рамках математического моделирования представленн метод оценки рисков, который в отличие от аналогов может быть адаптирован под канал связи беспроводной сети с различными элементами, с учетом их особенностей, среды функционирования и расположения.

- проведена оценка стойкости технологий виртуальной частной сети в виде показателей готовности элементов данной технологии, а также описана общая модель стойкости сервера доступа в виде системы с разными видами резервирования.

С учетом вышеизложенного новизна результатов исследования заключается в следующем:

- риск-модель, в отличие от существующих аналогов, является адаптированной для оценки и регулирования рисков нарушения криптостойкости заданной системы, взаимодействующей с механизмами виртуальной частной сети;

- классификация сервисов VPN с учетом их особенностей позволит пользователям в ближайшем будущем выбрать наиболее подходящий для себя;

- освещенная в данной статье оценка стойкости технологий VPN может быть использована в качестве базиса для дальнейших исследований в области криптографической защиты каналов связи беспроводных сетей.

Список литературы

1. Социальные сети и риск-мониторинг : монография / А.Г. Остапенко, Е.Ю. Чапурин, А.О. Калашников, О.А. Остапенко, Г.А. Остапенко ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 4. М. : Горячая линия-Телеком, 2020. 266 с.

2. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М: РадиоСофт, 2010. - 232 с.

3. Кащенко, А.Г. Идентификация параметров нечетких моделей оценки рисков информационной безопасности распределенных вычислительных систем / А.Г. Кащенко // Информация и безопасность. 2010. Т. 13. № 1. С. 143-148.

4. Петров, М.Ю. Технология реализации системы анализа информационных рисков на базе высокопроизводительной вычислительной системы / М.Ю. Петров, С.В. Савков, В.М. Шишкин // Информационное противодействие угрозам терроризма. 2009. № 13. С. 73-77.

5. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, Н.П. Мухин, В.И. Шестопалов. М.: Радио и связь, 2000. 384 с.

6. Карпеев, Д.О. Идентификация параметров нечетких моделей оценки информационных рисков информационных систем / Д.О. Карпеев, А.Ю. Татаринцев, Д.С. Яковлев, А.В. Заряев // Информация и безопасность. 2010. Т. 13. № 1. С. 37-42.

7. Андреев, Д.А. Измерение рисков при значительном количестве атак и малых значениях вероятности успеха / Д.А. Андреев, В.Г. Щербаков, Ю.Е. Филиппов // Информация и безопасность. 2007. Т. 10. № 3. С. 499-502.

Концерн «Созвездие»
Concern «Sozvezdie»

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 17.05.2023

Информация об авторах

Радько Николай Михайлович – канд. техн. наук, заместитель генерального директора, Концерн “Созвездие”, e-mail: alexanderostapenkoias@gmail.com

Хирьянова Юлия Сергеевна – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Мокроусов Александр Николаевич – старший преподаватель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

RISK MODEL OF THE ATTACKED WIRELESS NETWORK COMMUNICATION CHANNEL USING VPN TECHNOLOGIES

N.M. Radko, Yu.S. Khiryanova, A.N. Mokrousov, E.A. Moskaleva

The paper presents methodological and algorithmic ways of assessing the risks of disruption of the wireless communication channel. The peculiarity of the considered environment is the widespread use of VPN services - protocols, equipment, encryption algorithms. In the scientific publication the analysis of actual VPN-services, their cryptographic features and functionality is carried out. On the basis of the study built a mathematical model of the strength and security of the above technology, proposed a risk model of the attacked wireless network communication channel, equipped with VPN technology in the form of protocols, equipment or hardware and software complex. In addition, a classification of attacks on the wireless network communication channel, which aims to gain unauthorized access to information resources of the closed network segment c VPN, as well as violation of their confidentiality and integrity. The results obtained in the study can be used to improve the cryptographic strength of the wireless network communication channel at the design stage and as a basis for further research by specialists in the field of information security.

Keywords: VPN, communication channel, vulnerability, risk, threat.

Submitted 17.05.2023

Information about the authors

Nikolay M. Radko – Cand. Sc. (Technical), Deputy General Director, Concern "Sozvezdie", e-mail: alexanderostapenkoias@gmail.com

Julia S. Khiryanova – Student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander N. Mokrousov – Senior Lecturer, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com