УДК 004.42.056
DOI: 10.17277/vestnik.2019.04.pp.535-546

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ РАСЧЕТА КОМПЛЕКСНОЙ ОЦЕНКИ VPN

И. Г. Старун, А. Н. Юганссон, Ю. А. Гатчин

Факультет безопасности информационных технологий,
ФГАОУ ВО «Национальный исследовательский университет ИТМО»,
starun.igor@yandex.ru; г. Санкт-Петербург, Россия

Ключевые слова: анонимизация; виртуальная частная сеть; VPN; защита информации; информационная безопасность; криптография; математическая модель; угрозы персональным данным.

Аннотация: Рассмотрены виды угроз персональным данным пользователя при работе в частной сети, определены критерии оценки защищенности VPN (Virtual Private Network) от потенциальных угроз. На основе проведенных исследований предложена математическая модель расчета комплексной оценки VPN в зависимости от предъявляемых требований.

Введение

Популярность использования VPN *(*англ. *Virtual Private Network* – виртуальная частная сеть) растет большими темпами [1, 2]. Такая тенденция указывает на возросшее стремление пользователей к анонимизации при работе в сети Интернет для защиты персональных данных (**ПД**) от возможных утечек, вызванных действиями злоумышленников. Одной из причин растущей популярности VPN является необходимость получения доступа к онлайн-контенту, недоступному в определенных регионах [3]. Более весомой причиной служит то, что на фоне стремительной информатизации общества растет и объем данных в сети Интернет, что приводит к увеличению числа потенциальных угроз. В этих условиях становится актуальным вопрос оценки используемой частной сети для формирования объективного понимания степени пользовательской защищенности с учетом возможных видов утечек данных.

Цель статьи – разработка модели комплексной оценки VPN.

Исходя из поставленной цели, сформулированы следующие задачи:

1. Исследовать виды угроз ПД пользователя при работе в частной сети.
2. Определить критерии оценки защищенности VPN сети от потенциальных угроз.
3. Построить математическую модель комплексной оценки VPN в зависимости от соответствия разработанным критериям. Комплексность оценки характеризуется полнотой рассматриваемых аспектов защищенности виртуальной частной сети.

Виды и классификация угроз персональным данным пользователя при работе с VPN

В зависимости от вида данных пользователя, потенциально подверженных компрометации, можно выделить две группы угроз:

– утечки персональных данных пользователя;

– обнаружения использования средств анонимизации.

Первую группу угроз можно подразделить на три подгруппы:

1) связанные с недостатками в области обеспечения криптографической защиты информации, в том числе угрозы дешифрования захваченного трафика по причинам:

– применения ненадежных алгоритмов шифрования или их отсутствия;

– использования общих ключей шифрования.

2) связанные с эксплуатацией уязвимостей стороннего программного обеспечения (**ПО**), в том числе угрозы утечки приватного IP-адреса пользователя путем эксплуатации уязвимостей:

– WebRTC;

– AdobeFlash.

3) прочие угрозы персональным данным пользователя, такие как:

– утечки данных о реальном провайдере пользователя путем перехвата DNS-трафика [2];

– утечки приватного IP-адреса на этапе переподключения.

Ко второй группе относят угрозы обнаружения использования средств анонимизации путем:

– фиксирования цифрового отпечатка Fingerprint;

– обнаружения двустороннего пинга с помощью ICMP-трафика;

– угроза обнаружения использования средств анонимизации и нарушения анонимности путем обнаружения разницы во временных зонах браузера и IP с помощью данных GeoIP.

Критерии оценки VPN сети с учетом степени ее защищенности от потенциальных угроз

Помимо всесторонней защищенности VPN для большинства пользователей особую важность представляет скорость приема и передачи данных в сети [4 – 6]. В статье [7] рассмотрено влияние используемых протоколов и алгоритмов шифрования на производительность, выделены оптимальные комбинации. На скорость соединения также непосредственно влияет взаимное географическое расположение пользователя и VPN сервера. Поэтому важным критерием при выборе VPN сервера является множество доступных серверов с точки зрения их количества и местоположения.

Таким образом, с учетом защищенности работы в частной сети, скорости соединения и ассортимента выбора серверов можно выделить 3 группы критериев для оценки VPN:

1. Критерии защищенности от угроз ПД, условно подразделяемые на три подгруппы:

1) Критерии защищенности ПД от угроз, связанных с недостатками в области обеспечения криптографической защиты информации, в том числе:

– наличие шифрования трафика внутри сети с использованием надежных алгоритмов и протоколов шифрования (подробно рассмотрено в [8]);

– использование индивидуальных ключей шифрования для каждого пользователя;

– использование индивидуальных ключей шифрования для каждого сервера.

2) Критерии защищенности от угроз, связанных с эксплуатацией уязвимостей стороннего ПО, в том числе защищенность от утечек приватного IP-адреса пользователя путем эксплуатации уязвимостей:

– WebRTC;

– AdobeFlash.

3) Критерии защищенности от прочих угроз персональным данным пользователя:

– защищенность от утечек данных о реальном провайдере пользователя путем перехвата DNS-трафика;

– защищенность от утечек приватного IP-адреса на этапе переподключения.

2. Критерии защищенности от обнаружения использования пользователем средств анонимизации, в том числе путем:

– фиксирования цифрового отпечатка Fingerprint;

– обнаружения двустороннего пинга с помощью ICMP-трафика;

– защищенность от обнаружения использования средств анонимизации и нарушения анонимности путем обнаружения разницы во временных зонах браузера и IP с помощью данных GeoIP.

3. Критерии пользовательского удобства, такие как:

– отсутствие значительного падения скоростей приема и передачи данных при использовании VPN.

– наличие широкого ассортимента доступных серверов в разных географических зонах.

В статьях [9, 10] предложен более широкий перечень аспектов, важных для оценки VPN, например, масштабируемость VPN сервиса. В настоящей работе рассматривается оценка VPN с точки зрения отдельного пользователя, поэтому целый ряд критериев отражен с помощью оценки падения скоростей приема и передачи данных, так как, в конечном счете, именно на этой характеристике VPN будет сказываться масштабируемость VPN. В настоящей работе рассматривается оценка VPN сети в ее статичном состоянии, не учитывающем уровень нагрузки на сеть (в том числе возможность применения искусственной нагрузки путем DDoS-атак [11, 12]).

Все указанные критерии оценки VPN являются отражением программно-аппаратной реализации функций частной сети, но не учитывают степень доверия к разработчику VPN. Необходимо понимать, что даже полное соответствие частной сети всем упомянутым критериям не гарантирует, что разработчик не собирает ПД пользователей для продажи или дальнейшего использования в личных целях. Поэтому для комплексной оценки VPN следует ввести критерий уровня доверия разработчику, который во многом носит субъективный характер, так как не всегда можно присвоить ему абсолютно точную оценку. В статье [13] выдвигается тезис о необходимости проверки VPN на соблюдение юридической прозрачности, а также рассмотрены политики конфиденциальности семи популярных провайдеров VPN на предмет отсутствия юридических лазеек для осуществления незаконных действий в отношении ПД пользователя.

При определении уровня доверия разработчику следует учитывать несколько факторов:

– репутацию разработчика и его продуктов;

– юридическую прозрачность нормативных и прочих документов, утвержденных разработчиком и отражающих правила и принципы функционирования VPN, в том числе обработки ПД.

Математическая модель расчета комплексной оценки VPN в зависимости от соответствия разработанным критериям

При оценке VPN будем исходить из того, что полное соответствие всем критериям оценки эквивалентно 100 % положительной оценке VPN.

Удельный вес для каждой из трех групп критериев в общей системе оценки определяется важностью с точки зрения пользовательской заинтересованности.

Для учета удельного веса группы критериев будем использовать нормирующие коэффициенты.

Расчет общего критерия защищенности VPN от угроз персональным данным $K_{\text{ПД}}$ проводится по формуле

$$K_{\text{ПД}} = K_{\text{КРИПТ}} + K_{\text{ПО}} + K_{\text{ПР}}, \quad (1)$$

где $K_{\text{КРИПТ}}$ – общий критерий защищенности ПД от угроз, связанных с недостатками в области обеспечения криптографической защиты информации, равный сумме оценок VPN по критериям соответствующей подгруппы $K_{\text{КРИПТ}} = \sum_{1}^{3} x_{\text{КРИПТ}_i}$; $K_{\text{ПО}}$ – общий критерий защищенности ПД от угроз, связанных с эксплуатацией уязвимостей стороннего ПО, равный сумме оценок VPN по критериям соответствующей подгруппы $K_{\text{ПО}} = \sum_{1}^{2} x_{\text{ПО}_i}$; $K_{\text{ПР}}$ – общий критерий защищенности от прочих угроз персональным данным пользователя, равный сумме оценок VPN по критериям соответствующей подгруппы $K_{\text{ПР}} = \sum_{1}^{2} x_{\text{ПР}_i}$.

В таблице 1 представлены распределения критериев внутри каждой группы (защищенность от угроз ПД, защищенность от обнаружения использования средств анонимизации, пользовательское удобство) по значимости. Максимальная сумма баллов в каждой из групп равна 100, чтобы в дальнейшем было проще нормировать сами группы по приоритетности для пользователя. Распределение отражает важность каждого отдельного критерия относительно других [14]. Например, наличие шифрования трафика является центральной задачей любой VPN сети, следовательно, соответствующий критерий защищенности имеет наибольший удельный вес. Конкретные значения получены в результате экспертной оценки по методу Черчмена–Аккофа [15 – 18], который заключается в последовательном уточнении оценок, удовлетворяющих системе неравенств.

Полученные в настоящей работе значения носят рекомендательный характер и могут быть изменены в случае изменения приоритетности того или иного аспекта защищенности или пользовательского комфорта.

Общий критерий защищенности от обнаружения использования пользователем средств анонимизации $K_{\text{АНОН}}$ рассчитывается как сумма оценок VPN по критериям соответствующей группы (см. табл. 1)

$$K_{\text{АНОН}} = \sum_{1}^{3} x_{\text{АНОН}_i}. \quad (2)$$

Общий критерий пользовательского удобства $K_{\text{ПУ}}$ рассчитывается как сумма оценок VPN по критериям соответствующей группы (см. табл. 1)

$$K_{\text{ПУ}} = \sum_{1}^{2} x_{\text{ПУ}_i}. \quad (3)$$

В таблице 2 представлена расшифровка всех указанных критериев, отражающая числовые эквиваленты уровней соответствия критериям каждой группы.

Таблица 1

Распределение критериев защищенности VPN по значимости

Номер критерия	Критерий	Удельный вес, %
Критерии защищенности ПД от угроз, связанных с недостатками в области обеспечения криптографической защиты информации $x_{\text{КРИПТ}_i}$		
1	Наличие шифрования траффика внутри сети с использованием надежных алгоритмов и протоколов шифрования	35
2	Использование индивидуальных ключей шифрования для каждого пользователя	15
3	Использование индивидуальных ключей шифрования для каждого сервера	10
Критерии защищенности ПД от угроз, связанных с эксплуатацией уязвимостей стороннего ПО $x_{\text{ПО}_i}$		
1	Защищенность от утечек приватного IP-адреса пользователя путем эксплуатации уязвимостей WebRTC	10
2	Защищенность от утечек приватного IP-адреса пользователя путем эксплуатации уязвимостей AdobeFlash	10
Критерии защищенности от прочих угроз персональным данным пользователя $x_{\text{ПР}_i}$		
1	Защищенность от утечек приватного IP-адреса на этапе переподключения	15
2	Защищенность от утечек данных о реальном провайдере пользователя путем перехвата DNS-трафика	5
Критерии защищенности от обнаружения использования пользователем средств анонимизации $x_{\text{АНОН}_i}$		
1	Защищенность от обнаружения использования средств анонимизации путем фиксирования цифрового отпечатка Fingerprint	35
2	Защищенность от обнаружения использования средств анонимизации путем обнаружения двустороннего пинга	35
3	Защищенность от обнаружения использования средств анонимизации и нарушения анонимности путем обнаружения разницы во временных зонах браузера и IP	30
Критерии пользовательского удобства $x_{\text{ПУ}_i}$		
1	Отсутствие значительного падения скоростей приема и передачи данных при использовании VPN	70
2	Наличие широкого ассортимента доступных серверов в разных географических зонах	30
	Итого	100

Таблица 2

Расшифровка критериев защищенности VPN

Критерий	Значение	Уровень соответствия критерию
1	2	3
Критерии защищенности ПД от угроз, связанных с недостатками в области обеспечения криптографической защиты информации $x_{\text{КРИПТ}_i}$		
Наличие шифрования трафика внутри сети с использованием надежных алгоритмов и протоколов шифрования	0	Шифрование отсутствует или проводится некорректно
	15	Шифрование проводится корректно, используемый протокол шифрования не входит в число надежных
	30	Шифрование проводится корректно, доступен один надежный протокол шифрования
	35	Шифрование проводится корректно, доступно более одного надежного протокола шифрования
Использование индивидуальных ключей шифрования для каждого пользователя	0	Общие ключи для всех пользователей
	15	Индивидуальные ключи для каждого пользователя
Использование индивидуальных ключей шифрования для каждого сервера	0	Общие ключи для всех серверов
	10	Индивидуальные ключи для каждого сервера
Критерии защищенности ПД от угроз, связанных с эксплуатацией уязвимостей стороннего ПО $x_{\text{ПО}_i}$		
Защищенность от утечек приватного IP-адреса пользователя путем эксплуатации уязвимостей WebRTC	0	Обнаружены утечки IP-адреса
	10	Утечки не обнаружены
Защищенность от утечек приватного IP-адреса пользователя путем эксплуатации уязвимостей AdobeFlash	0	Обнаружены утечки IP-адреса
	10	Утечки не обнаружены
Критерии защищенности от прочих угроз персональным данным пользователя $x_{\text{ПР}_i}$		
Защищенность от утечек приватного IP-адреса на этапе переподключения	0	Обнаружены частные утечки IP-адреса
	8	Обнаружены редкие (менее 5 % случаев) утечки IP-адреса
	15	Утечки не обнаружены
Защищенность от утечек данных о реальном провайдере пользователя путем перехвата DNS-трафика	0	Обнаружены утечки DNS-провайдера
	5	Утечки не обнаружены

Продолжение табл. 2

1	2	3
Критерии защищенности от обнаружения использования пользователем средств анонимизации $x_{\text{АНОН}_i}$		
Защищенность от обнаружения использования средств анонимизации путем фиксирования цифрового отпечатка Fingerprint	0	Значения MSS и/или MTU подозрительны
	35	Значения MSS и MTU стандартны
Защищенность от обнаружения использования средств анонимизации путем обнаружения двустороннего пинга с помощью ICMP трафика	0	Обнаружен двусторонний пинг (разница во времени ответа более 30 мс)
	35	Двусторонний пинг не обнаружен (разница во времени ответа менее 30 мс)
Защищенность от обнаружения использования средств анонимизации и нарушения анонимности путем обнаружения разницы во временных зонах браузера и IP с помощью данных GeoI	0	Зафиксирована разница во временных зонах браузера и IP
	30	Разницы во временных зонах браузера и IP нет, либо ICDP трафик VPN сервера заблокирован
Критерии пользовательского удобства $x_{\text{ПУ}_i}$		
Отсутствие значительного падения скоростей приема и передачи данных при использовании VPN	0	Падение скоростей значительно
	35	Падение скоростей не критично, но наблюдается
	70	Падение скоростей незначительно
Наличие широкого ассортимента доступных серверов в разных географических зонах	0	Выбор серверов не предусмотрен
	10	Доступные сервера территориально расположены близко друг к другу
	30	Широкий ассортимент серверов по географическому положению

Предложенные значения получены в результате оценки несколькими экспертами потенциального ущерба от несоответствия VPN тому или иному требованию обеспечения информационной безопасности (**ИБ**) и пользовательского удобства. Впоследствии экспертные оценки были усреднены методом интервальных оценок [18].

После определения степени соответствия VPN критериям оценки рассчитывается комплексный критерий оценки VPN с учетом уровня защищенности

$$K_{\text{ОБЩ}} = n_{\text{ДОВЕР}}\left(a_{\text{ПД}}K_{\text{ПД}} + a_{\text{АНОН}}K_{\text{АНОН}} + a_{\text{ПУ}}K_{\text{ПУ}}\right), \quad (3)$$

где $n_{\text{ДОВЕР}}$ – коэффициент доверия разработчику, принимающий значения от 0 до 1; $a_{\text{ПД}}, a_{\text{АНОН}}, a_{\text{ПУ}}$ – нормирующие (весовые) коэффициенты значимости первой, второй, третьей групп критериев соответственно.

Таблица 3

Рекомендации по выбору значения коэффициента доверия

Характеристика разработчика	Значение $n_{\text{ДОВЕР}}$
Юридическая прозрачность нормативных и прочих документов и репутация разработчика и его продуктов не вызывают доверия	Не более 0,35
Репутация разработчика или его продуктов сомнительна, имели место быть случаи нарушения разработчиком собственных гарантий по работе с ПД	Не более 0,5
Нормативные и прочие документы, утвержденные разработчиком и отражающие правила и принципы функционирования VPN, имеют юридические лазейки и не дают полной гарантии соблюдения принципов конфиденциальности при работе с ПД	Не более 0,7
Разработчик является доверенным лицом, юридическая прозрачность нормативных и прочих документов не вызывает сомнений	Вплоть до 1

Нормирующие коэффициенты $a_{\text{ПД}}, a_{\text{АНОН}}, a_{\text{ПУ}}$ отражают значимость каждой из групп критериев для пользователя. Числовое значение каждого из них может меняться в интервале от 0 до 1, а сумма данных коэффициентов всегда должна быть равна единице. Введение нормирующих коэффициентов обусловлено необходимостью учитывать приоритеты конкретного пользователя при работе в сети Интернет. В общем случае наиболее чувствительной для пользователя является компрометация его ПД, в связи с чем соответствующая группа критериев в большинстве случаев будет иметь наибольший нормирующий коэффициент. Если защищенность ПД имеет для пользователя второстепенное значение, то числовое значение соответствующего коэффициента $a_{\text{ПД}}$ следует понизить. Конкретные значения нормирующих коэффициентов должны быть определены в результате экспертной оценки и могут меняться в зависимости от приоритетов конкретного пользователя. Для получения усредненных значений нормирующих коэффициентов целесообразно воспользоваться методом интервальных оценок [18] ввиду небольшого количества групп критериев. В таком случае требуется привлечение нескольких экспертов.

Коэффициент доверия – это вероятность или степень уверенности в том, что разработчик VPN добросовестно выполняет свои обязательства по работе с ПД пользователей. По аналогии с [19, 20], коэффициент доверия выносится в виде множителя, так как его значение отражает степень уверенности в правильности полученной оценки для каждой группы критериев.

Рекомендации по выбору значения коэффициента доверия разработчику, составленные по результатам проведения экспертной оценки, представлены в табл. 3.

Выводы по работе и перспективы

В работе исследованы виды угроз персональным данным пользователя при работе в виртуальных частных сетях. Определены критерии оценки защищенности VPN сети от потенциальных угроз. Проведено обоснованное распределение

критериев оценки VPN по значимости, а также определены числовые эквиваленты для уровней соответствия VPN каждому из критериев.

В результате работы построена математическая модель расчета комплексной оценки VPN в зависимости от соответствия критериям оценивания. С помощью полученной модели можно проводить не только полноценную оценку качества VPN с учетом его защищенности от различных видов угроз, но и сравнение нескольких VPN сервисов.

Список литературы

1. Березин, А. С. Построение корпоративных защищенных виртуальных частных сетей / А. С. Березин, С. А. Петренко // Защита информации. Конфидент. – 2001. – № 1. – С. 54 – 61.

2. A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients / V. C. Perta [et al.] // Proceedings of Conference : 15th Privacy Enhancing Technologies, 30 June – 02 July 2015, Philadelphia, USA. – Philadelphia, 2015. – P. 77 – 91.

3. Николахин, А. Ю. Использование технологии VPN для обеспечения информационной безопасности / А. Ю. Николахин // Экономика и качество систем связи. – 2018. – № 3 (9). – С. 60 – 68.

4. Волохов, В. В. Исследование принципов работы VPN, разработка политики безопасности VPN. Использование анонимайзеров / В. В. Волохов // Наука, техника и образование. – 2018. – № 5 (46). – С. 87 – 89.

5. Дунаев, П. А. Сравнительный анализ конфигураций маршрутизатора, влияющих на изменение полосы пропускания сигнала / П. А. Дунаев, С. Ю. Рябцунов, М. А. Шукралиев // Доклады Томского гос. ун-та систем управления и радиоэлектроники. – 2016. – Т. 19, № 1. – С. 40 – 45. doi: 10.21293/1818-0442-2016-19-1-40-45

6. Есеналиева, А. Б. Обеспечение безопасности информации в VPN сетях / А. Б. Есеналиева, А. Ю. Пыркова // Изв. науч.-техн. общества «КАХАК». – 2013. – № 2 (41). – С. 5 – 8.

7. Ушаков, Ю. А. Создание мультисервисной многоточечной VPN сети с динамической автонастройкой / Ю. А. Ушаков, П. Н. Полежаев, А. Ю. Шухман // Вестн. Оренбургского гос. ун-та. – 2015. – № 9 (184). – С. 191 – 199.

8. Lawas, J. B. R. Network performance evaluation of VPN protocols (SSTP and IKEv2) / J. B. R. Lawas, A. C. Vivero, A. Sharma // Proceedings of 13th International Conference on Wireless and Optical Communications Networks, 21 – 23 July 2016, Hyderabad, Telangana State, India. – Hyderabad, 2016. – С. 112 – 116.

9. Турская, Е. Р. VPN как средство «неотложной помощи» [Электронный ресурс] / Е. Р. Турская // Сетевой журнал Data Communication. – 2000. – № 11. – 13 с. – Режим доступа : https://elvis.ru/upload/iblock/08f/08f13b5909a3f87feb777b49c38e3568.pdf (дата обращения: 25.10.2019).

10. Бельфер, Р. А. Анализ источников угроз информационной безопасности виртуальных частных сетей VPRN на базе сети MPLS / Р. А. Бельфер, И. С. Петрухин // Вестн. Московского гос. техн. ун-та им. Н. Э. Баумана. Серия: Приборостроение. – 2013. – № 4 (93). – С. 79 – 89.

11. Анисимов, В. В. Модель функционирования сети связи с неизвестным уровнем доверия и оценки ее возможностей по предоставлению услуги VPN с заданным качеством / В. В. Анисимов, А. Н. Бегаев, Ю. И. Стародубцев // Вопросы кибербезопасности. – 2017. – № 1 (19). – С. 6 – 15. doi: 10.21681/2311-3456-2017-1-6-15

12. Гречишников, Е. В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак / Е. В. Гречишников, М. М. Добрышин, П. В. Закалкин // Вопросы кибербезопасности. – 2016. – № 3 (16). – С. 4 – 12. doi:10.21681/2311-3456-2016-3-4-12

13. Берман, В. В. Медвежьи сервисы. Проверяем 7 популярных провайдеров VPN на предмет приватности [Электронный ресурс] / В. В. Берман // Хакер.ru. – Режим доступа : https://xakep.ru/2018/12/25/evil-vpn/ (дата обращения: 25.10.2019).

14. Нелюбин, А. П. Взаимосвязь качественной и количественной важности критериев в многокритериальных задачах принятия решений / А. П. Нелюбин, В. В. Подиновский // Открытое образование. – 2011. – № 6. – С. 107 – 114.

15. Фишберн, П. К. Методы оценки аддитивных ценностей / П. К. Фишберн // Статистическое измерение качественных характеристик. – М. : Статистика, 1972. – С. 8 – 34.

16. Экенроде, Р. Т. Взвешенные многомерные критерии / Р. Т. Экенроде // Статистическое измерение качественных характеристик. – М. : Статистика, 1972. – С. 139 – 154.

17. Акофф, Р. Л. Основы исследования операций / Р. Л. Акофф, М. В. Сасиени ; пер. с англ. и предисл. В. Я. Алтаева ; под ред. И. А. Ушакова. – М. : Мир, 1971. – 534 с.

18. Глотов, В. А. Экспертные методы определения весовых коэффициентов / В. А. Глотов, В. В. Павельев // Автоматика и телемеханика. – 1976. – № 12. – С. 95 – 107.

19. Колпакова, Т. А. Определение компетентности экспертов при принятии групповых решений / Т. А. Колпакова // Радіоелектроніка, інформатика, управління. – 2011. – № 1. – С. 40 – 43.

20. Рутман, Б. Ю. Принятие окончательного решения в условиях неопределенности / Б. Ю. Рутман // Доклады Белорусского гос. ун-та информатики и радиоэлектроники. – 2010. – № 5 (51). – С. 88 – 93.

Building a Mathematical Model of Calculation for VPN Integrated Assessment

I. G. Starun, A. N. Yuganson, Yu. A. Gatchin

Faculty of Information Technology Security, starun.igor@yandex.ru;
National Research University ITMO, St. Petersburg, Russia

Keywords: anonymization; virtual private network; VPN protection of information; Information Security; cryptography; mathematical model; threats to personal data.

Abstract: The types of threats to the user's personal data when working in a private network are examined; criteria for assessing VPN (Virtual Private Network) security from potential threats are defined. Based on the studies, a mathematical model is proposed for calculating a comprehensive VPN assessment depending on the requirements.

References

1. Berezin A.S., Petrenko S.A. [Construction of corporate secure virtual private networks], *Zashchita informatsii. Konfident* [Information Security. Confident], 2001, no. 1, pp. 54-61. (In Russ.)

2. Perta V.C., Barbera M.V., Tyson G., Haddadi H., Mei A. Proceedings of Conference: 15th Privacy Enhancing Technologies, 30 June - 02 July 2015, Philadelphia, USA, Philadelphia, 2015, pp. 77-91.

3. Nikolakhin A.Yu. [Using VPN technology to ensure information security], *Ekonomika i kachestvo sistem svyazi* [Economics and quality of communication systems], 2018, no. 3 (9), pp. 60-68. (In Russ., abstract in Eng.)

4. Volokhov V.V. [Research of VPN working principles, development of VPN security policy. Using anonymizers], *Nauka, tekhnika i obrazovaniye* [Science, Technology and Education], 2018, no. 5 (46), pp. 87-89. (In Russ.)

5. Dunayev P.A., Ryabtsunov S.Yu., Shukraliyev M.A. [Comparative analysis of router configurations that affect the change in signal bandwidth], *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radio Electronics], 2016, vol. 19, no. 1, pp. 40-45, doi: 10.21293/1818-0442-2016-19-1-40-45 (In Russ., abstract in Eng.)

6. Yesenaliyeva A.B., Pyrkova A.Yu. [Information security in VPN networks], *Izvestiya nauchno-tekhnicheskogo obshchestva «KAKHAK»* [Proceedings of the scientific and technical society "KAHAK"], 2013, no. 2 (41), pp. 5-8. (In Russ.)

7. Ushakov Yu.A., Polezhayev P.N., Shukhman A.Yu. [Creation of a multiservice multi-point VPN network with dynamic auto-configuration], *Vestnik Orenburgskogo gosudarstvennogo universiteta* [Bulletin of the Orenburg State University], 2015, no. 9 (184), pp. 191-199. (In Russ., abstract in Eng.)

8. Lawas J.B.R., Vivero A.C., Sharma A. Proceedings of 13th International Conference on Wireless and Optical Communications Networks, 21 - 23 July 2016, Hyderabad, Telangana State, India, Hyderabad, 2016, pp. 112-116.

9. https://elvis.ru/upload/iblock/08f/08f13b5909a3f87feb777b49c38e3568.pdf (accessed 25 October 2019).

10. Bel'fer R.A., Petrukhin I.S. [Analysis of sources of threats to information security of virtual private VPRN networks based on the MPLS network], *Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N. E. Baumana. Seriya: Priborostroyeniye* [Moscow State Technical University Bulletin N.E. Bauman. Series: Instrument Making], 2013, no. 4 (93), pp. 79-89. (In Russ., abstract in Eng.)

11. Anisimov V.V., Begayev A.N., Starodubtsev Yu.I. [A model of a communication network with an unknown level of trust and an assessment of its capabilities to provide VPN services with a given quality], *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2017, no. 1 (19), pp. 6-15, doi: 10.21681/2311-3456-2017-1-6-15 (In Russ., abstract in Eng.)

12. Grechishnikov Ye.V., Dobryshin M.M., Zakalkin P.V. [Model of a VPN access node as an object of network and stream computer intelligence and DDoS attacks], *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2016, no. 3 (16), pp. 4-12, doi:10.21681/2311-3456-2016-3-4-12 (In Russ., abstract in Eng.)

13. https://xakep.ru/2018/12/25/evil-vpn/ (accessed 25 October 2019).

14. Nelyubin A.P., Podinovskiy V.V. [The relationship of the qualitative and quantitative importance of criteria in multicriteria decision-making problems], *Otkrytoye obrazovaniye* [Open Education], 2011, no. 6, pp. 107-114. (In Russ., abstract in Eng.)

15. Fishbern P.K. *Statisticheskoye izmereniye kachestvennykh kharakteristik* [Statistical measurement of qualitative characteristics], Moscow: Statistika, 1972, pp. 8-34. (In Russ.)

16. Ekenrode R.T. *Statisticheskoye izmereniye kachestvennykh kharakteristik* [Statistical measurement of qualitative characteristics], Moscow: Statistika, 1972, pp. 139-154. (In Russ.)

17. Akoff R.L., Sasiyeni M.V., Ushakov I. A. [Ed.] *Osnovy issledovaniya operatsiy* [Fundamentals of operations research], Moscow: Mir, 1971, 534 p. (In Russ.)

18. Glotov V.A., Pavel'yev V.V. [Expert methods for determining weight coefficients], *Avtomatika i telemekhanika* [Automation and Telemechanics], 1976, no. 12, pp. 95-107. (In Russ., abstract in Eng.)

19. Kolpakova T.A. [Determination of the competence of experts in making group decisions], *Radíoyelektroníka, ínformatika, upravlínnya* [Radioelectronics, Informatics, Management], 2011, no. 1, pp. 40-43. (In Russ., abstract in Eng.)

20. Rutman B.Yu. [The final decision in the face of uncertainty], *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioelektroniki* [Reports of the Belarusian State University of Informatics and Radioelectronics], 2010, no. 5 (51), pp. 88-93. (In Russ., abstract in Eng.)

Aufbau eines mathematischen Berechnungsmodells der integrierten VPN-Bewertung

Zusammenfassung: Es sind die Arten von Bedrohungen für die persönlichen Daten des Benutzers bei der Arbeit in einem privaten Netzwerk untersucht, Kriterien für die Bewertung der VPN-Sicherheit vor potenziellen Bedrohungen sind definiert. Basierend auf den durchgeführten Untersuchungen ist ein mathematisches Modell zur Berechnung der komplexen VPN-Bewertung in Abhängigkeit von den aufgewiesenen Anforderungen vorgeschlagen.

Construction d'un modèle mathématique de calcul d'évaluation intégrée VPN

Résumé: Sont étudiés les types de menaces contre les données personnelles de l'utilisateur lors de l'utilisation d'un réseau privé, sont définis les critères d'évaluation de la sécurité du VPN des menaces potentielles. Sur la base des recherches effectuées, est proposé un modèle mathématique de calcul de l'évaluation intégrée VPN en fonction des exigences prévues.

Авторы: ***Старун Игорь Геннадьевич*** – студент; ***Югансон Андрей Николаевич*** – ассистент факультета безопасности информационных технологий; ***Гатчин Юрий Арменакович*** – доктор технических наук, профессор факультета безопасности информационных технологий, ФГАОУ ВО «Национальный исследовательский университет ИТМО», г. Санкт-Петербург, Россия.

Рецензент: ***Литовка Юрий Владимирович*** **–** доктор технических наук, профессор кафедры «Системы автоматизированной поддержки принятия решений», ФГБОУ ВО «ТГТУ», г. Тамбов, Россия.