# Защита и нападение – история со счастливым финалом?

**Владимир Воротников,** *руководитель отдела интеграционных решений ООО "С-Терра СиЭсПи"*

Любой ЦОД является привлекательной мишенью для атак злоумышленников. Во-первых, количество хранимой там информации несоизмеримо с любым другим ИТ-объектом. Во-вторых, концентрация ценной информации там существенно выше: в отличие от компьютеров среднестатистических пользователей в центрах обработки данных реже хранится ненужная мусорная информация.

Поскольку проблема защиты ЦОДов является актуальной, механизмы защиты ЦОДов непрерывно совершенствуются. Но и злоумышленники не стоят на месте. Исследуются, находятся и используются новые, все более и более продвинутые виды атак. Простые инструменты разведки и взлома уже давно доступны в виде хорошо документированных продуктов. Архитектура и функциональные возможности современных ботнетов поражают воображение и часто превосходят по сложности даже ведущие средства защиты информации.

Это вечная борьба защиты и нападения, которая, как показывает история, никогда не закончится. Или все-таки у нее может быть конец? И если да, то кто все-таки победит? О том, на каком витке этой борьбы мы находимся, а также о том, как законы квантовой физики делают нас на шаг ближе к победе "белых шляп", мы и поговорим в данной статье.

## Больше производительности – для "больших" каналов!

Мы с вами живем в годы экспоненциального роста количества передаваемой информации. Какой бы совершенной ни была система защиты, она будет бесполезной, если не будет справляться со своей задачей на все более и более возрастающих скоростях. Кроме того, с учетом распространенности DDoS-атак оборудование должно иметь еще и запас по производительности для адекватной реакции на такие атаки. Понимая эту проблему, компания "С-Терра СиЭсПи" предлагает в составе своей продуктовой линейки высокопроизводительное решение для защиты высокоскоростных (от 10 Гбит/с) каналов между ЦОДами. Решение защищает трафик на всех уровнях от канального до прикладного (L2 – L7). При этом его производительность позволяет зашифровать даже наиболее тяжелые с позиции сетевого оборудования передаваемые данные, такие как, например, IP-телефония, где размер пакетов очень мал, а накладные расходы и требования к качеству крайне велики. Решение основано на применении уникального высокопроизводительного устройства С-Терра Шлюз 10G на базе Intel® Compute Module HNS2600TP. Характеристики его работы приведены в таблицах 1, 2.

**Таблица 1. Производительность**

| Вид трафика | Производительность, Мбит/с |
|---|---|
| UDP 512 | 9500 |
| UDP 1400 | 14 200 |

**Таблица 2. Показатели задержки**

| Режим шифрования | Задержка, мс |
|---|---|
| Без нагрузки | 0,27 |
| С нагрузкой 9 Гбит/с (UDP 512) | 0,4–0,6 |

## Не шифрованием единым

Но задача обеспечения конфиденциальности и целостности передаваемых данных является не единственной в рамках защиты ЦОДов. Для более надежной защиты сетевой инфраструктуры нужны продвинутые, интеллектуальные решения, которые могут анализировать сетевой трафик на предмет наличия вредоносной активности. Поэтому компания "С-Терра СиЭсПи" включила в свою продуктовую линейку систему обнаружения вторжений. Механизмы, используемые в С-Терра СОВ, позволяют администратору своевременно обнаруживать и адекватно реагировать на инциденты, возникающие в ЦОДах. Кроме того, СОВ предоставляет важные сведения для расследования уже произошедших инцидентов.

В гонке злоумышленников и администраторов безопасности важно не только решать текущие задачи, но и думать на шаг вперед. Ряд современных научных и инженерных исследований в области дает нам возможность радикально повысить безопасность передаваемых данных.

## Квантовая физика и криптография – связь уже очевидна

Читая новости квантовой физики, с первого взгляда может показаться, что практическая часть ее применения находится где-то в далеком будущем. Однако системы квантовой криптографии уже действуют. И они не так далеки, как может показаться. Прототипы таких систем уже есть в России и готовы вот-вот начать применяться в реальном секторе.

Механизм квантового распределения ключей (далее КРК) позволяет двум пользователям вырабатывать и обмениваться между собой случайными двоичными данными, которые могут быть использованы как секретный ключ. При этом законы квантовой механики исключают возможность незаметного

прослушивания такого обмена информацией. Это достигается за счет того, что ключ передается одиночными фотонами. Злоумышленнику, чтобы получить информацию о ключе, требуется тем или иным способом взаимодействовать с этим фотоном, но любое такое взаимодействие неминуемо вызовет изменение состояния фотона, что будет замечено на принимающей стороне. Схема проверена и хорошо зарекомендовала себя на практике: на данный момент подобные системы работают в США, Швейцарии, Японии в интересах банков и государственных организаций.

При этом КРК имеет и свои ограничения. Так, например, скорость передачи ключа очень сильно зависит от расстояния и уменьшается на порядки при переходе от 100 м к 10 км. Инженерным пределом на данный момент является передача квантового ключа на расстоянии 100 км. Кроме того, схема требует наличие не конфиденциального, но защищенного от модификаций классического канала.

Полученный с помощью КРК ключ обычно используют для защиты передаваемых данных. Если мы хотим получить максимальный уровень защиты, то мы можем использовать его в системе с абсолютной криптографической стойкостью, такой как шифр Вернама (одноразовый блокнот). Здесь, однако, мы ограничены длиной ключа, которая должна быть не меньше длины передаваемого сообщения. Это серьезная инженерная проблема, т.к. современные системы квантового распределения ключей позволяют генерировать ключ на скоростях десятков и сотен килобит в секунду, что на несколько порядков ниже требуемых для ЦОДов скоростей. Тем не менее, технологии КРК активно развиваются, и мы можем ждать значительного увеличения скорости генерации и передачи ключа в будущем.

Кроме того, если использовать данный ключ как элемент на одной из стадий построения IPsec-туннеля, то вышеназванных скоростей генерации оказывается вполне достаточно. Именно над таким решением работают сейчас инженеры компании "С-Терра СиЭсПи" и исследователи в Российском квантовом центре. На данный момент успешно проведены испытания первого прототипа решения. Был разработан и реализован протокол передачи квантового ключа между системой КРК и шлюзами безопасности. Работа данного протокола, а также принципиальная возможность использования квантового ключа в технологии IPsec была продемонстрирована на стенде. Испытания были успешными, и сейчас ведутся работы по более глубокой интеграции системы КРК и шлюзов безопасности С-Терра.

## Из пушки по?..

Квантовое распределение ключей, безусловно, является перспективной технологией, дающей нам надежду на получение чрезвычайно высокого уровня безопасности. Кроме того, ряд компаний по достоинству оценит репутационный выигрыш от использования такой системы. Как показала западная практика, именно крупные европейские (в частности, швейцарские) банки стали одними из первых, кто применил у себя на практике КРК. Такой шаг логично вписывается в образ компаний, для которых надежность – основа имиджа. Но за все приходится платить: решения с применением КРК, выйдя на рынок, ожидаемо будут существенно дороже своих "не квантовых" аналогов. Мониторинг работы такой системы, ее обслуживание и ремонт также потребуют существенно больше ресурсов и времени.

Поэтому не следует забывать, что уровень защищенности должен быть пропорционален ценности защищаемой информации. Во многих случаях вполне достаточной является проверенная временем связка IKE с использованием протокола Диффи-Хеллмана, которая применяется во всех современных продуктах компании "С-Терра СиЭсПи".

## В заключение

Помимо фундаментальных причин роста количества передаваемого и хранимого трафика и, как следствие, роста количества ЦОДов, в России есть ряд локальных факторов, которые только усиливают данную тенденцию: необходимость хранения персональных данных граждан на территории РФ, пакет Яровой-Озерова и др. К счастью, уже сейчас есть решения, которые готовы к такому развитию событий. Высокопроизводительное решение на основе уникального устройства С-Терра Шлюз 10G, как карьерный экскаватор от ИБ, способно обработать огромное количество трафика, а С-Терра СОВ, как саперная лопатка, поможет провести аккуратный и точный анализ передаваемых данных. ●

Какой бы совершенной ни была система защиты, она будет бесполезной, если не будет справляться со своей задачей на все более и более возрастающих скоростях. С учетом распространенности DDoS-атак оборудование должно иметь запас по производительности для адекватной реакции на такие атаки.

Уровень защищенности должен быть пропорционален ценности защищаемой информации. Во многих случаях вполне достаточной является проверенная временем связка IKE с использованием протокола Диффи-Хеллмана, которая применяется во всех современных продуктах компании "С-Терра СиЭсПи".

NM
АДРЕСА И ТЕЛЕФОНЫ компании С-ТЕРРА СИЭСПИ см. стр. 80