Confidential

# RUSSIA

**The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.**

**This issue is for your personal use only.**

**Published monthly in Russian and in English by *Trialogue Company Ltd.***

**Issue № 10 (202), vol.12. October 2013**

11 октября 2013 г.

Олег Демидов сообщает из Москвы:

## ДЕСЯТЬ РАЗОБЛАЧЕНИЙ СНОУДЕНА, КОТОРЫЕ ПОТРЯСЛИ МИР:

## КАК ОТВЕТИТ РОССИЯ И ЕЕ ПАРТНЕРЫ

***АННОТАЦИЯ***

***За короткий промежуток времени с июля 2013 г. американский перебежчик Эдвард Сноуден стал настоящей информационной бомбой, рассекретив колоссальные объемы информации о негласной деятельности США и Великобритании по осуществлению слежения и сбора данных в интернете и иных коммуникационных сетях.***

***Директор программы ПИР-Центра "Международная информационная безопасность и глобальное управление интернетом" Олег Демидов систематизировал разоблачения Сноудена, выделив из них те, что оказали наиболее серьезное влияние на руководство России и ее партнеров, а также на всю мировую общественность. Эксперт ПИР-Центра приходит к выводу, что разоблачения Сноудена способны стать катализатором далеко идущих решений и инициатив как в России, так и в мире в целом.***

ДЕСЯТЬ РАЗОБЛАЧЕНИЙ ЭДВАРДА СНОУДЕНА

***1. Программа Bullrun – масштабный комплекс мер по обходу криптографической защиты в Сети.***

С 2000 г. Агентство национальной безопасности (АНБ) и другие американские спецслужбы практикуют *добровольно-принудительное сотрудничество* с разработчиками средств шифрования в США, в рамках которого последние в результате давления или подкупа оставляют программные и аппаратные закладки (*бэкдоры* – англ. *backdoors*) в создаваемые ими продукты для ИТ-сервисов, банков и других клиентов, в том числе иностранных. Речь идет об использовании бизнеса для создания продукта с фундаментальными уязвимостями защиты и их последующей эксплуатации. В рамках связанной с *Bullrun* программы *SIGINT* АНБ ежегодно тратит до 250 млн долл. на подкуп компаний, которые встраивают *бэкдоры* в свои коммерческие продукты.

***Нет надежной криптографии – нет надежных сервисов и, как следствие, нет доверия к интернету вообще, априори. Эффект не просто выходит за пределы США и «целевых» объектов АНБ, пусть и весьма многочисленных - он имеет глобальный, планетарный характер.***

Несомненно то, что методы АНБ в рамках *Bullrun* ломают самые принципы и технологию обеспечения безопасности в Сети, а потому представляют собой фундаментальную угрозу. По оценке всемирно известного эксперта в области кибербезопасности Брюса Шрайнера, «правительство США предало Интернет».

***2. Возможно, еще с 2002 г. эксплуатируются фундаментальные уязвимости в национальном стандарте криптографии США Advanced Encryption Standard (AES) – блочном алгоритме шифрования, распространенном по всему миру.***

В России очень многие сервисы, не обязанные законодательством использовать национальные стандарты криптографии (ГОСТ), используют продукты на основе AES. Во всем мире, кроме КНР и ряда других стран, ситуация сходная: системы дистанционного банковского обслуживания, социальные сети, чаты, корпоративные сети и электронная почта – все эти ключевые сервисы полагаются на AES. Кроме того, АНБ успешно работает над взломом протокола шифрования SSL, который составляет основу безопасности большинства коммуникаций в Сети. Действует единая база данных для мгновенного подбора криптоключей к зашифрованным данным. Новый приоритет для АНБ, согласно данным Сноудена, - взлом виртуальных частных сетей (VPN) и технологий защиты 4G. В числе планов спецслужбы на 2013 г. также - встраивание *бэкдоров* в чипы популярных аппаратных средств, то есть переход от программного уровня обхода шифрования к физическому.

***3. Система слежения за платежами физических лиц по картам VISA, а также межбанковскими транзакциями через SWIFT: программа Follow the money и база данных «Тракфин».***

В 2011 г. в этой базе данных были накоплены записи по 180 млн операций, из них 84% - операции частных лиц по кредитным картам. АНБ как минимум с 2012 г. обеспечило себе доступ к сетям системы межбанковских транзакций *SWIFT*, через которую проходят три миллиарда операций в месяц. Целевые регионы отслеживания операций – Африка, Ближний Восток и Европа. Сама *Visa* все отрицает – то есть речь идет о взломе платежной системы, а не о факте ее сотрудничества со спецслужбами. Хотя иная версия вряд ли могла быть озвучена публично, ситуация представляет собой серьезный удар по глобальной финансовой безопасности.

***4. Масштабная программа PRISM - негласный сбор информации, передаваемой по сетям электросвязи.***

*PRISM*, запущенная в 2007 г., позволяет скачать закрытую информацию с серверов интернет-гигантов США (включая *Microsoft*, *Yahoo!*, *Google*, *Facebook*, *AOL*, *Skype*, *YouTube*, *Apple* и *PalTalk*). При этом доступ к информации обычно осуществляется с ведома самих интернет-корпораций, что говорит об их тесной аффилированности с американскими спецслужбами. С помощью PRISM АНБ, ЦРУ и ФБР имеют доступ к данным частной email-переписки, видео- и голосовых чатов, видеозаписей, фото, хранимой на HDD информации, голосового трафика (VoIP), передаваемых через сеть файлов, онлайн-видеоконференций, введенных логинов и

паролей, записей и действий в соцсетях - список можно продолжать. Также отслеживаются звонки абонентов крупнейших сотовых операторов США, как внутри страны, так и по миру.

***5. Масштабная программа XKeyscore – универсальное орудие поиска и анализа данных.***

Перечислим лишь некоторые функции программы: при вводе адреса *e-mail* - перехват содержимого ящика, списка контактов, IP-адреса, с которого произошел вход в почту. При вводе IP осуществляется перехват всех посещенных с него сайтов, введенных паролей и запросов, просмотренных документов, взлом аккаунтов в соцсетях, переписки в чатах. Обеспечивается отслеживание данных о сеансах связи, перехват и сохранение всех логов текстовой коммуникации, распознание национальности субъекта по тексту перехваченной почты, а также выявление аномалий в коммуникации - например, использование субъектом шифровальных программ типа *PGP* при работе в интернете. Поддерживается даже функция выявления исходного авторства и источника копируемых и передаваемых по Сети документов. Программа работает посредством 700 серверов, большая часть из которых размещена в зарубежных посольствах и консульствах США, включая сервер в Москве. В планах по развитию программы – обеспечение перехвата трафика VoIP и данных геолокации (GPS).

Отдельного упоминания в этой связи заслуживает VoIP-сервис *Skype*, инициатива запрета которого циркулирует в кремлевских кабинетах с февраля 2011 г. с подачи ФСБ РФ как раз по причине отсутствия у спецслужб доступа к исходному коду шифра его VoIP-трафика. Проблема, по некоторым данным, была отчасти решена в 2011 г., когда сервис был приобретен *Microsoft*, более склонной к сотрудничеству с властями РФ, но с повестки она до конца не снята. Апелляция к тому, что *Skype* подконтролен АНБ и британцам – отличный повод под давлением спецслужб перевести контроль над сервисом в самой России из негласной и внеправовой практики сотрудничества в систематизированное правовое русло – либо ограничить использование сервиса на российской территории.

***6. Систематическая практика наступательных кибероперациий спецслужб США против сетей иностранных государств, включая КНР, Иран, КНДР и РФ.***

Согласно секретному бюджету американских спецслужб, раскрытому Сноуденом, на операции в зарубежных сетях в 2013 г. предусмотрено 4,3 млрд долл. В 2011 г. 231 операций такого рода были *проактивными*, то есть наступательными. Что любопытно, помимо стандартного предотвращения вторжений в сети США, на такие операции также возлагается цель «предотвращения распространения ядерного оружия». Это еще раз подтверждает происхождение вирусов *Flame*, *Gauss*, *Duqu*, и, конечно, *Stuxnet*, объектом атак которого стал преимущественно Иран. Само по себе это не новость – но неожиданно выглядят масштабы финансирования. С 2010 г. в ходу аксиома о *дешевом кибероружии* – так сколько подобных продуктов и операций можно реализовать на миллиард долларов в год? Параметры бюджета спецслужб США позволяют предположить, что линейка средств, разработанных для *удушения* иранского мирного атома, намного обширнее, чем предполагалось; а судя по динамике роста объема этой статьи, ее развитие отнюдь не закончилось на Иране.

***7. Многочисленные серии операций АНБ и британского Центра правительственной связи (англ. Government Communications Headquarters, GCHQ) по перехвату данных высокопоставленных иностранных чиновников и делегаций, в том числе перехват защищенной спутниковой связи с Москвой Д.А.Медведева из посольства РФ в Лондоне во время саммита G20 в апреле 2009 г.***

Перехват осуществлялся со шпионской станции Менвит-Хилл, его результаты неизвестны. Тогда же был произведен взлом шифра смартфонов *BlackBerry* для прослушивания звонков участников G20 и слежки за их перепиской.

Подобные операции осуществлялись в отношении зарубежных делегаций, государственных органов, посольств многих стран, включая те, что считают себя союзниками Вашингтона. Особенно неожиданной такая практика стала для стран Латинской Америки, включая Мексику и Бразилию, президенты которых стали объектами телефонного прослушивания и слежения

через e-mail со стороны АНБ. Постановка вопроса об отмене запланированной на октябрь 2013 г. встречи бразильского лидера Дилмы Руссеф с Бараком Обамой – возможно, лишь начало снежного кома осложнений в двусторонних отношениях, который способен нарастать и дальше, с каждым новым эпизодом разоблачений Сноудена.

### 8. Программа британского GCHQ Tempora и ее составляющие - Mastering the Internet и Global Telecoms Exploitation.

В рамках программы ведется сбор данных телефонных разговоров и интернет-трафика в колоссальных объемах. Полученные данные могут храниться до 3 дней, метаданные – до 30 дней. Осуществляется запись телефонных звонков, данных e-mail-переписки, сообщений и личных данных в *Facebook*. В 2011 г. для получения, обработки и хранения данных в рамках *Tempora* были задействованы 200 линий по 10 гигабит/сек каждая, в планах правительства – расширение этих мощностей в 10 раз. При этом список объектов слежения не был раскрыт, по выражению экспертов, он «бесконечный».

Основной и весьма неприятный вывод из этого для Москвы – британцы немногим уступают своему заокеанскому партнеру в части аппетитов и масштабов электронного слежения.

### 9. Массированная слежка АНБ за коммерческими компаниями в Бразилии и ряде других стран.

АНБ систематически прослушивало телефонные звонки и просматривало электронную почту руководства бразильского нефтяного гиганта *Petróleo Brasileiro S.A. (PetroBras)*. Этот эпизод примечателен тем, что ломает основную *линию обороны* Белого Дома – «мы вынуждены шпионить во имя святой цели - борьбы с международным терроризмом». Разъяренная Дилма Руссеф справедливо заметила, что «*PetroBras* не является угрозой национальной безопасности какой-либо из стран». Зато она в полной мере является стратегическим и крупнейшим частным активом бразильской экономики с капитализацией более 100 млрд долл., годовым валовым доходом в 144 млрд. долл., обеспечивая 80% всей национальной нефтедобычи.

И вот тут аргументы США заканчиваются, а американская позиция по вопросам поведения государств в интернете трещит по швам. Шпионаж за стратегическими экономическими объектами всегда подавался Вашингтоном как одно из главных *табу* и обвинений в адрес Пекина; во многом именно этой угрозой со стороны Китая оправдывалось наращивание бюджета и штата Киберкомандования США и других подобных структур армии и спецслужб. Весьма симптоматично, что с июля 2013 г. критика Белого дома в адрес Пекина за осуществление кибершпионажа и кибератак внезапно прекратилась.

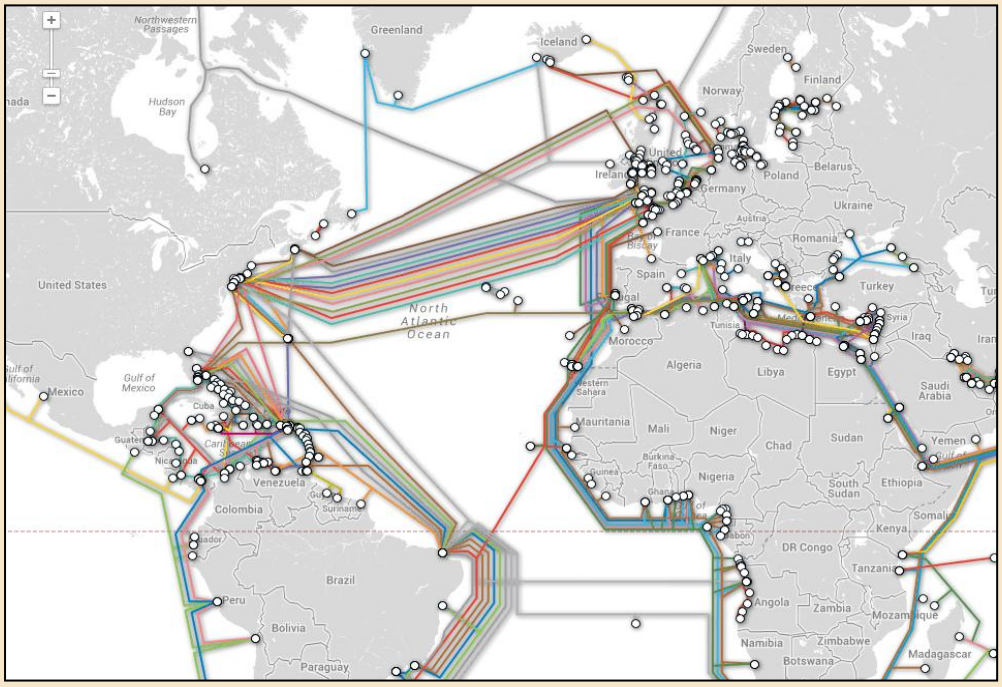
### 10. Совместная деятельность АНБ и британского GCHQ по установке аппаратных врезок для снятия информации в инфраструктуру подводных оптоволоконных кабелей, в том числе дальнемагистральных.

Помощь британцев здесь крайне удобна по географическим причинам – только через графство Корнуолл на юго-западе Англии проходят более десятка магистральных кабелей, по которым между Европой и США передается около четверти мирового интернет-трафика (см. Карту 1 на с. 5); другого такого узла оптоволоконной инфраструктуры в Европе нет. В том числе, через Корнуолл передается значительная часть трафика из России.

*Врезка* аппаратных устройств для извлечения данных напрямую из подводного оптоволокна, наряду с *Bullrun*, – яркий пример *нечестной игры* даже в отношении *заклятых друзей* Белого дома, не говоря о его близких союзниках. Дело в том, что в этом случае США и их *коллеги* эксплуатируют уникальное преимущество – доступ к базовой инфраструктуре Сети, которая вроде бы считается общей, как и сам интернет. На уровне шпионского ПО сервисов и приложений возможности у крупных игроков более или менее равны, и АНБ с ЦРУ могут противостоять на равных русским или китайским хакерам – а то и иранским. Но когда, перепрыгивая через все вышестоящие уровни инфраструктуры интернета, Вашингтон и Лондон достают из рукава козырь контроля над проводами, реакция остального мира будет одна – физически нивелировать это несправедливое преимущество.

В этом смысле разоблачения Сноудена – *подарок свыше* для активизации проектов БРИКС по прокладке собственных дальнемагистральных оптоволоконных кабелей. В их числе – проект *кабеля БРИКС* длиной 34 тыс. км, который должен соединить все страны форума по маршруту от Владивостока до бразильской Форталезы и тем самым снизить их инфраструктурную зависимость от существующих каналов (см. Карту 2). Реализация проекта была намечена на 2013 г., однако существенно запаздывает – пока что кабель по-прежнему существует лишь на бумаге.

Карта 1. Трансатлантические подводные оптоволоконные кабели




*Источник*: TeleGeography. Submarine Cable Map 2013. http://submarinecablemap.com

Карта 2. Проект трансконтинентального оптоволоконного кабеля БРИКС


*Источник*: BRICS Cable. http://www.bricscable.com/network/

С учетом реакции РФ и Бразилии на разоблачения Сноудена шансы этого проекта на скорое и успешное завершение существенно возрастают, причем скорее за деньги Бразилиа и Пекина, чем Претории, продвигавшей его ранее.

***Суммируем все вышеизложенное**: США (Лондон здесь все же не играет ключевой роли) серьезно вложились в обеспечение своего превосходства в Сети на всех основных уровнях ее инфраструктуры – от кабелей и чипов до VoIP-сервисов и соцсетей. Каждый факт по отдельности – не откровение, но беда в том, что по их совокупности успехи Белого Дома выглядят необратимо в глазах международного сообщества. Никто уже не убедит Дилму Руссеф в том, что ее мобильный не прослушивается АНБ. Никто не может гарантировать ФСБ и Госдуме РФ, что АНБ не читает переписку российских чиновников в Gmail, а британцы не "перемывают" российский трафик в Корнуолле. И вряд ли кто-то заставит PetroBras думать, что мотивы американских спецслужб не распространяются на экономику и ограничиваются национальной безопасностью.*

Поезд, пожалуй, уехал – а прибывает он прямиком на станцию адептов концепции *цифрового суверенитета*, особенно популярной в лагере БРИКС и среди других гигантов развивающегося мира. *Топлива* от разоблачений Сноудена им хватит надолго – перипетии его истории и нынешний статус таковы, что никто не может сказать точно, знает ли *странный парень* всю правду и сдал ли он все свои карты. Его разоблачения обречены выглядеть лишь вершиной айсберга *англо-саксонского цифрового империализма*. Да, Эдвард Сноуден – не тектоническая плита, которая толкает развивающиеся страны навстречу суверенитету в Сети – но он идеальный предлог и *катализатор* этих процессов, возникший как нельзя кстати.

КАК ОТВЕТИТ РОССИЯ

Россия, с 1998 г. привыкшая штурмовать бастионы *несправедливого миропорядка* в сфере интернета, оказалась в непривычной, но приятной ситуации. Если прежде Китай и другие союзники молчаливо прятались за спиной Москвы, выглядевшей одиноким воином в этом поле, то сегодня сама Россия может перевести дух и пропустить вперед разгневанную Бразилию.

Маховик понемногу раскручивается на всех уровнях: *PetroBras* обещает вложить невиданные 10 млрд долл. в повышение уровня информационной безопасности; Бразилия объявила о том, что обратится в ООН с требованием пересмотра принципов глобального управления интернетом и выдвинула инициативу, полностью созвучную той, что была озвучена членами российского Совета Федерации в июле 2013 г. – обязать транснациональные ИТ-корпорации перенести сервера, на которых обрабатываются персональные данные граждан страны, на ее территорию. На этом фоне можно ожидать и ратификации российско-бразильского соглашения о сотрудничестве в сфере международной информационной безопасности, зависшего на стадии подписания в 2010 г.

Что может последовать дальше? Внутри страны - рост давления на *Google* и *Facebook*, первыми попавших под огонь критики российских законодателей; ужесточение регулирования VoIP-сервисов на территории России; законодательное расширение сферы обязательного применения криптографии ГОСТ для бизнеса, госучреждений и других юридических лиц; активизация усилий по созданию национальной защищенной операционной системы; разработка законодательства о регулировании соцсетей, электронной почты для госучреждений и т.д.

На внешней арене – новый *крестовый поход* вместе с союзниками по БРИКС против ICANN и *мультистейкхолдерского* подхода под лозунгом наделения ООН ответственностью за Сеть. Полями битвы в этом начинании могут стать Полномочная конференция Международного союза электросвязи в ноябре 2014 г. и процесс *ВВУИО+10* в 2015 г. А первый сигнал может прозвучать уже на октябрьском Всемирном форуме по управлению интернетом (Internet Governance Forum, IGF) на Бали, к которому готовится российская делегация. Кроме того, несложно представить дополнение российских мега-проектов подводных трубопроводов оптоволоконными кабелями, связующими нас с партнерами по БРИКС.

***Хватит ли у России ресурсов и технологий, чтобы пройти достаточно далеко по этому пути? Пожалуй, что да. Затруднят ли перечисленные стратегии в случае своего успешного воплощения работу АНБ и GCHQ в российских сетях? Несомненно. Выиграют ли от этого российский ИТ-сектор и, соответственно, национальные интересы? Вопрос весьма спорный. Полное подчинение логики регулирования интернет-сектора императивам безопасности может обернуться весомым бременем для его развития. В ситуации явного вхождения России в полосу стагнации или даже депрессии к 2014 г. речь может идти о лишении отечественной экономики одного из самых мощных и надежных несырьевых моторов роста за все последние годы.***

***Вот в этом ни АНБ, ни Сноуден уже не будут виноваты.***

Автор – Олег Демидов, директор программы ПИР-Центра "Международная информационная безопасность и глобальное управление интернетом"

*Выпускающий редактор: Юлия Фетисова*


*Москва – Женева, Октябрь 2013*

---

***Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».***

***3. Права членов Клуба***

*3.1. Индивидуальные члены Клуба имеют право:*
*3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.*
*[…]*
*3.2. Корпоративные члены Клуба имеют право:*
*3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.*
*[…]*

***4. Обязанности членов Клуба***

*4.1. Все срочные члены Клуба обязаны:*
*4.1.6. Не передавать полученные материалы бюллетеня Russia Confidential, а также пароли доступа на клубную часть сайта ПИР-Центра физическим и юридическим лицам, не являющимся членами Клуба.*
*[…]*

***6. Russia Confidential***

*6.1. Бюллетень эксклюзивной аналитики Russia Confidential выпускается ООО «Триалог» по заказу ПИР-Центра исключительно для личного пользования членов Клуба.*
*6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную штатными и приглашенными экспертами ПИР-Центра специально для Russia Confidential.*
*6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.*
*6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он публикуется в других изданиях ПИР-Центра и может быть использован для цитирования членами Клуба.*
*6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русском или английском языке, по выбору члена Клуба.*
*6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.*

---

*Уважаемые члены клуба Триалог,*


***В 2013 году Клуб отмечает свое 20-летие!***

*Сегодня Клуб Триалог играет роль уникального для России неформального сообщества ведущих дипломатов, экспертов, представителей бизнеса. В Юбилейный год членов Клуба ожидают* ***5*** *встреч с ведущими российскими и зарубежными экспертами в области международной безопасности,* ***4*** *номера журнала Индекс Безопасности,* ***12*** *номеров бюллетеня эксклюзивной аналитики Russia Confidential и* ***бесплатное*** *участие в научных мероприятиях ПИР-Центра, а также* ***несколько приятных сюрпризов*** *для наших постоянных членов.*

*Как Вам известно, мы приветствуем и ценим, когда действующие члены Клуба рекомендуют членство в Клубе или участие в наших заседаниях другим лицам. Помимо того, что такая рекомендация автоматически открывает двери для членства в Клубе, она также* ***вознаграждается нами одним из двух способов.*** *Ниже представлены условия вознаграждения.*

*Надеюсь встретить Вас и Ваших коллег на встречах Клуба в 2013 г.!*

***С уважением,***
***Д.В.Поликанов***
***Председатель Международного клуба Триалог***

**Вознаграждения за рекомендацию членства в Международном клубе *Триалог* другим лицам**

| **Вариант 1 – Скидка на членство в следующем периоде** | |
|---|---|
| **5%** | за 1 нового индивидуального члена |
| **10%** | за 1 нового корпоративного члена |
| **10%** | за 2 новых индивидуальных членов |
| **15%** | за 3 новых индивидуальных членов |
| **20%** | за 4 и более новых индивидуальных членов |
| **20%** | за 2 новых корпоративных членов |
| **30%** | за 3 новых корпоративных членов |
| **35%** | за 4 и более новых корпоративных членов |

| **Вариант 2 – Единовременное возмещение в наличной форме** | |
|---|---|
| **100 USD** | за 1 нового корпоративного члена |
| **200 USD** | за 2 новых корпоративных членов |
| **300 USD** | за 3 новых корпоративных членов |
| **500 USD** | за 4 и более новых корпоративных членов |