Понимание безопасности и устойчивости Интернета

Кибербезопасность трактуется достаточно расплывчато и в разных контекстах может означать что угодно: безопасность информации и компьютера, безопасность инфраструктуры Интернета, безопасность любого устройства, подключенного к Интернету (включая важнейшие коммунальные услуги, например, распределение электроэнергии), безопасность данных, приложения и связь, безопасность пользователей Интернета (в частности, детей), и часто включает в себя такие понятия, как национальная безопасность, а также безопасность частной жизни. Действительно, пока еще не удалось прийти к консенсусу относительно того, что означает данный термин.

Данный документ не является попыткой предложить более четкое определение понятия «кибербезопасность» или решение для всех ее аспектов, подпадающих под это понятие. Здесь рассматриваются основные компоненты безопасности и отказоустойчивости экосистемы Интернета (что составляет основу надежной стратегии в области кибербезопасности). Такими компонентами являются: технические решения и решения в области политики, согласованные с неизменными ценностями Интернета, индивидуальная и коллективная ответственность за риск, а также совместная работа.

Неизменные ценности Интернета

С момента своего изобретения Интернет претерпел значительные изменения и постоянно продолжает меняться. Очень важно понять, что именно составляет неизменную *часть Интернета – основные свойства или неизменные ценности, «благодаря которым Интернет является платформой для практически безграничных инноваций. Следует выделить не только технологические основы Интернета, но также его глобальное влияние и социальные структуры»*[1].

Любая стратегия решения проблемы кибербезопасности должна начинаться с понимания фундаментальных свойств Интернета, благодаря которым данное средство глобальных коммуникаций становится инструментом для реализации творческих устремлений, совместной работы, создания изобретений, выражения идей, проявления культурной и социальной индивидуальности, коммерческой активности и т. д. Мы описываем эти фундаментальные свойства как «**неизменные ценности Интернета**», поскольку дальнейший глобальный успех Интернета зависит от сохранения этих свойств.

Первыми двумя свойствами являются **глобальный охват и целостность**.

Интернет является глобальным, поскольку любая конечная точка, подключенная к данной сети, может обращаться к любой другой конечной точке. Подобной конечной точкой может выступать ноутбук, смартфон или автомобильная навигационная система, поддерживающая доступ в Интернет, и т. п.

Под целостностью Интернета понимается получение конечной точкой информации отправителя независимо от места и способа подключения получателя к Интернету. Например, независимо от того, где находится пользователь, он должен получить одно и то же содержимое при доступе на домашнюю страницу сайта Internet Society по адресу **www.internetsociety.org**. Безусловно, пользователь может ограничить получаемое содержимое на своем устройстве (например, с помощью подключаемого модуля в браузере, такого как Ghostery), чтобы заблокировать следящие элементы, такие как теги, веб-жучки, пиксели и маяки, которые включаются в веб-страницы для наблюдения за поведением пользователей в сети, например для отслеживания посещаемых ими сайтов. Это не влияет на целостность обмена данными. Однако если бы поставщик услуг Интернета заблокировал доступ на сайт **www.internetsociety.org**, то это отразилось бы на целостности Интернета, поскольку информация исключается или отбрасывается поставщиком услуг Интернета, прежде чем она достигнет конечной точки. Очень важно, что данное действие осуществляется не на уровне конечной точки, а на промежуточном этапе в сети.

Третьим основным свойством Интернета является **поддержка инноваций без необходимости дополнительного разрешения.** Иными словами, это способность каждого создавать новое приложение в Интернете без необходимости получения специального разрешения от кого бы то ни было. В истории Интернета имеется множество примеров потрясающих технологий и услуг, которые появились благодаря возможности создания новых приложений или услуг без разрешения со стороны правительства, поставщика услуг Интернета или кого бы то ни было еще. Возможно, самым известным примером является HTML (HyperText Markup Language — язык разметки гипертекста), который стал началом развития Всемирной Паутины. Данный язык был разработан ученым, который работал в CERN в Швейцарии, и впоследствии данный язык стал доступен для использования любому пользователю. Если бы Тиму Бернес-Ли нужно было просить разрешения, то Всемирной Паутины могло бы и не быть. Если бы идея предоставления ссылок на данные была отклонена, то на этом могли бы прекратиться разработки поисковых служб, таких как Google. Был ли бы в этом случае миллиард активных пользователей в социальной сети Facebook[2]? Существовали ли бы краудсорсинговые службы сбора и визуализации данных, такие как Ushahidi[3]? А как насчет Wikipedia, Twitter, YouTube, мобильных приложений, программного обеспечения для карт, потоковой передачи музыки и сотен других вещей, которые мы используем ежедневно и уже воспринимаем как должное?

Четвертым свойством является **открытость** – Интернет открыто разрабатывался и является открытым для использования любым человеком. Интернет построен на технических стандартах, которые разрабатывались открыто на основе консенсуса, а затем предоставлялись для использования во всем мире. Примерами таких стандартов являются HTTP (для доступа к веб-содержимому), SMTP (для электронной почты), протоколы SIP и RTP (для голосовой связи и передачи аудиоданных).

Пятым свойством, которое мы должны сохранить, является **доступность Интернета**. Это не просто возможность доступа людей к информации и интерактивным услугам. Она включает возможность вносить свой вклад в создание содержимого; взаимодействовать с другими людьми во всем мире; создавать приложения или услуги; подключать сервер или новую сеть при условии их соответствия техническим стандартам Интернета.

Шестым основным свойством, которое мы должны оберегать, является **дух совместной работы и сотрудничества** Интернета. При решении проблем безопасности Интернета мы должны найти способ привлечь к этому процессу все заинтересованные стороны – от пользователей до научно-исследовательского сообщества Интернета, коммерческих компаний, политиков и т. п. Решения, которые вырабатываются отдельной группой людей, либо не смогут решить проблему, либо причинят больше вреда, чем пользы. В некоторых случаях они могут даже создавать значительные проблемы, которые ставят под вопрос устойчивость работы Интернета.

Сложность проблем безопасности

Баланс между достижением целей по обеспечению безопасности и сохранением основных свойств Интернета и является истинной задачей при разработке стратегии кибербезопасности. Очень важно, чтобы решения были совместимы с неизменными ценностями Интернета.

Обеспечение выполнения требований по безопасности в закрытой системе, работающей в ограниченной среде, является относительно простой задачей, и, во многих случаях, простая стратегия “безопасность за счет неизвестности” (стратегия, которая строится на том, что злоумышленник не знает структуры системы) может вполне выполнять свою задачу. В то же время защита открытой системы, такой как Интернет, связана несколько с другими проблемами.

Во-первых, все те же свойства Интернета, которые обеспечивают его успех и его ценность для пользователей, создают новые возможности для разного рода вредоносной деятельности. Например

- Интернет является доступным.
    - *Вместе с тем, это означает, что он также является доступным для атак и проникновения.*
- Интернет процветает благодаря возможности инновационного творчества без дополнительных разрешений.
    - *Однако это свойство также, по сути, разрешает и разработку разного рода вредоносного программного обеспечения.*
- Мы ценим глобальное распространение Интернета.
    - *Однако, с точки зрения кибербезопасности, это означает, что трансграничному злоумышленнику будет проще реализовывать свои атаки и они могут иметь гораздо более далеко идущие последствия.*
- Стандарты Интернета являются добровольными, равно как и их внедрение. Они являются результатом совместной работы. Данная совместная работа является неотъемлемой частью функционирования Интернета.
    - *В то же время, это затрудняет распределение ответственности и выработку решений.*

При решении проблем кибербезопасности очень важно понимать, что, несмотря на то, что злоумышленники используют ту или иную возможность, сами по себе неизменные ценности Интернета не являются ни отправной точкой, ни причиной подобной вредоносной деятельности. Баланс между достижением целей по обеспечению безопасности и сохранение основных свойств Интернета и является истинной задачей при разработке стратегии кибербезопасности. Это означает, что разработка и внедрение решений в области безопасности должны осуществляться с учетом их возможного влияния на фундаментальные свойства Интернета. Как было отмечено ранее, очень важно, чтобы решения в области безопасности были основаны или хотя бы не противоречили неизменным ценностям Интернета, чтобы обеспечить постоянный успех Интернета как средства развития экономики и обеспечения социального благополучия.

Технологические строительные блоки для обеспечения безопасности

С точки зрения технологии, техническое сообщество Интернета имеет длинную историю разработки подобных решений (включая технические протоколы и технологии, а также оптимальные процедуры) и предоставления возможности их использования во всем мире для создания более надежного и безопасного Интернета. Эти решения создаются в различных организациях, занимающихся разработкой стандартов, в ходе открытого процесса и принимаются коллективно на основе общего консенсуса.

Примерами технических стандартов, разработанных Целевой инженерной группой Интернета (IETF) для повышения безопасности инфраструктуры Интернета, являются:

- IPsec (Internet Protocol Security - безопасность протокола Интернета) – обеспечивает комплексную безопасность на уровне Интернета.
- TLS (Transport Layer security - безопасность на транспортном уровне) – обеспечивает безопасность обмена данными через интернет, а также широко используется, например, для защиты обмена данными между веб-сайтами.
- Система проверки подлинности в сети Kerberos – позволяет проверять личность пользователей в открытой (незащищенной) сети.
- DNSSEC (Domain Name System Security Extensions) – обеспечивает целостность аутентичных ответов на DNS-запросы.
- DANE (DNS-based Authentication of Named Entities — проверка подлинности именованных элементов на основе системы DNS) – использует расширения DNSSEC и позволяет администраторам доменного имени указать ключи, которые используются для установления соединения, защищенного с помощью шифрования, с сервером с данным именем.

Примерами разработки технических стандартов при участии Консорциума Всемирной Паутины (W3C) для повышения безопасности Паутины и Интернета являются:

- Политика безопасности содержимого.
- Обмен ресурсами с запросом происхождения.
- Сигнатура XML, шифрование XML и сопутствующие спецификации.
- Криптографические интерфейсы API для JavaScript.

Примерами стандартов в области безопасности данных, разработанных организацией OASIS (Organization for the Advancement of Structured Information Standards), являются:

- Службы цифровых подписей (DSS) - стандарты служб цифровых подписей для XML.
- Протокол KMIP (Key Management Interoperability Protocol) – обеспечивает расширенные функциональные возможности для технологий с применением ключа асимметричного шифрования.
- Язык SAML (язык разметки, предусматривающий защиту данных) – основанная на XML платформа для создания и обмена информацией по безопасности между партнерами в сети.
- Язык XACML (eXtensible Access Control Markup Language) – используется для представления и оценки политик контроля доступа.

Во-вторых, абсолютной безопасности не существует. Всегда будут угрозы и уязвимости, поэтому слово «безопасный» означает просто то, что остаточные риски являются допустимыми в конкретном контексте. Именно поэтому очень важным показателем при определении цели всех усилий в области кибербезопасности является «**устойчивость**». Точно так же как организм человека может подвергаться воздействию вирусов и в результате этого становится сильнее и устойчивее, новые технологии, решения и совместные разработки делают Интернет более устойчивым к различного рода вредоносной деятельности.

Культура общей и коллективной ответственности за риск

Прочные взаимные связи и зависимости в экосистеме Интернета выдвигают новое важное требования для достижения эффективной безопасности: совместное управление рисками, связанными с «входящими» и «исходящими» угрозами.

Традиционные подходы к обеспечению безопасности принципиально были связаны с внутренними и внешними угрозами, а также с тем влиянием, которое они могли оказывать на собственные ресурсы пользователя. Однако среди все большего числа людей растет понимание того, что парадигма безопасности для экосистемы Интернета должна основываться на защите возможностей для обеспечения экономического и социального благосостояния, а не на модели, которая просто предотвращает возможный ущерб. Более того, к проблеме безопасности необходимо подходить с точки зрения управления риском. В рамках этого подхода учитываются угрозы и уязвимости, а также их вероятность и возможный эффект.

Интернет, с его прочными взаимными связями и зависимостями, открывает новый показатель для оценки рисков. Безопасность и устойчивость Интернета зависит не только от того, насколько хорошо удается управлять рисками для организации и ее ресурсов, но также, что очень важно, от признания и управления рисками, которые представляет сама организация (в результате своих действий или бездействия) для экосистемы Интернета — «исходящих» рисков. Например, существование и ненадлежащее обслуживание так называемых «открытых DNS-преобразователей», которые широко используются для осуществления DDoS-атак [4]; недостаточно эффективные политики и практики в области безопасности, которые позволяют зараженным компьютерам подключаться к долговечным ботнетам; центр сертификации PKI с недостаточным уровнем защиты и несоответствующими возможностями распознавания брешей в системе безопасности, что приводит к несанкционированному доступу и задержкам в оповещении об инциденте в области безопасности[5].

Данный конкретный аспект управления рисками необязательно является очевидным, особенно потому что часто он сразу не причиняет ощутимого ущерба для организации и ее ресурсов и поэтому не может являться прямым доказательством, которое можно было бы напрямую связать со снижением «исходящих» рисков. В то же время, если игнорировать данные риски, это приведет к снижению общего уровня безопасности экосистемы.

Кроме того, для устранения некоторых рисков требуется участие нескольких сторон. Это лежит в основе идеи общего управления рисками. Это особенно важно в тех случаях, когда это связано с безопасностью всей инфраструктуры глобального Интернета. Поскольку сети являются взаимно связанными и зависимыми друг от друга, отдельно взятая сеть в одиночку не сможет кардинально решить проблему, даже если ей удастся защитить свои собственные ресурсы. Поэтому коллективная ответственность играет особенно важную роль в обеспечении безопасности и устойчивости глобальной системы маршрутизации Интернета. Например, снижение риска DDoS-атак на регулятора требует широкого внедрения средств фильтрации входящего трафика с целью предотвращения спуфинга IP-адресов[6]. Несмотря на это, даже при наличии средств фильтрации входящего трафика в хост-сети, атака на ее ресурс (например, веб-сервер) все равно возможна, если в других сетях подобная фильтрация не применяется. Тем не менее, мероприятия, проводимые в данной сети, могут благотворно отразиться на всем Интернете в целом, поскольку данная сеть не станет местом для организации подобных атак.

Культура общей и коллективной ответственности хорошо согласуется с сутью «общих интересов» Интернета. В контексте кибербезопасности это означает, что внедрение решений для обеспечения безопасности является долгосрочной инвестицией в экосистему Интернета, от которой выиграют все, а также что все заинтересованные стороны имеют общий интерес в управлении этими ресурсами.

Совместная работа как важнейший компонент эффективной системы безопасности

В конечном счете, именно благодаря людям обеспечивается целостность Интернета. Создание Интернета стало возможным благодаря добровольной совместной работе и сотрудничеству, и мы уверены, что это до сих пор является одним из основополагающих факторов для его процветания и раскрытия потенциала.

Безопасность в целом является очень сложной областью с точки зрения определения средств стимулирования. Безопасность глобальной инфраструктуры Интернета, будь то его система DNS или маршрутизация, создает дополнительные трудности: применение средств безопасности сильно зависит от действий многих других сторон.

Более того, если участники в экосистеме Интернета будут действовать независимо и исходя исключительно из своих собственных интересов, это не только повлияет на безопасность экосистемы, но и приведет к уменьшению общего социального и экономического потенциала Интернета. Подобную ситуацию часто описывают как «трагедию общин» – термин, популяризованный Гарретом Хардином[7] в его одноименной публикации. Действительно для отражения некоторых проблем, особенно в области кибербезопасности, в экосистеме Интернета можно применить аналогию общин.

В области безопасности и устойчивости интернета непросто преодолеть «трагедию общин», поскольку люди по своей природе ищут решения, которые затрагивают, прежде всего, их собственные интересы. Однако данный подход является контрпродуктивным и в долгосрочной перспективе губительным для интересов всех сторон.

Технологические решения являются при этом важным элементом, но одних только технологий недостаточно. Чтобы обеспечить видимые улучшения в этой области, необходимо более четко обозначить проблемную область с точки зрения рисков на основе показателей и тенденций. Также, что более важно, требуются изменения в культуре, предполагающие коллективную ответственность во всех аспектах: политических, юридических, технических, экономических, социальных.

Интернет появился в результате добровольного сотрудничества и совместной работы. В истории Интернета можно найти множество примеров подобного сотрудничества и его эффективности. Ярким примером является рабочая группа[8] Conficker, которая была создана для борьбы с атакой, появившейся в Интернете и осуществляемой вредоносным программным обеспечением под названием Conficker. Еще одним примером являются группы операторов региональных и национальных сетей и их роль в решении рабочих проблем (которые часто охватывают несколько сетей).

Проблемы, связанные с трудностями и возможностями совместной работы вместе с необходимыми культурными изменениями, можно разделить на четыре основные области. По нашему мнению, успех в каждой из этих областей является предварительным требованием для обеспечения положительного эффекта для безопасности и устойчивости Интернета:

1. **Общее понимание проблемы**. Чем ближе друг к другу будут все заинтересованные стороны в понимании проблем, степени их важности и приоритетов их решения, тем более конструктивным будет диалог, тем более согласованными будут усилия, направленные на повышение безопасности и устойчивости.

2. Общее понимание решений. Проблема здесь состоит в том, что имеется целый спектр возможных решений (технических, политических, экономических, социальных) и каждое отдельное из них решает только часть или лишь отдельный набор этих проблем в заданный момент времени. Важно понимать, что «серебряной пули» не существует. Для построения решения по обеспечению безопасности можно использовать постоянно развивающиеся строительные блоки.

3. Понимание общих и индивидуальных затрат и преимуществ. Технологические строительные блоки отличаются по цене и преимуществам, которые они обеспечивают для отдельного участия и общего благополучия глобальной инфраструктуры. Понимание этих факторов и того, как они согласуются с бизнес-целями операторов сетей и других сторон, является очень важным для обеспечения постоянных усовершенствований в области безопасности и устойчивости.

4. Способность оценить риски. Правильный выбор средств и подходов зависит от способности соответствующим образом оценить как входящие, так и исходящие риски. Для этого требуется договориться о показателях и фактах, а также связанных с ними тенденциях. Эти данные также важны для оценки эффективности и влияния подобных инструментов после их развертывания, а также для контроля меняющейся динамики среды.

Практически невозможно добиться всеобщего согласия по сути проблем, а также прийти к согласованному плану действий, который будет принят во всем мире в обозримом будущем. Экономическая конкуренция, политика и личная мотивация также играют свою роль в организации успешного сотрудничества. Однако как показали несколько попыток сотрудничества, все разногласия являются преодолимыми при совместной борьбе с угрозой. Подобное добровольное сотрудничество по мере необходимости, «работа во благо каждого» является чрезвычайно важной для обеспечения масштабируемости Интернета и его способности адаптироваться к изменяющимся условиям и возникающим угрозам, что приводит к беспрецедентной эффективности.

Замечания и пояснения

[1] «Неизменные ценности Интернета: что действительно является важным», http://www.internetsociety.org/internet-invariants-what-really-matters

[2] http://news.cnet.com/8301-1023_3-57525797-93/facebook-hits-1-billion-active-user-milestone/

[3] Ushahidi — это проект с открытым исходным кодом, который позволяет пользователям осуществлять краудсорсинг кризисной информации, отправляемой посредством мобильного телефона.
www.ushahidi.com/

[4] Например, метод, который использовался в атаке, направленной на www.spamhaus.org в марте 2013 г.

[5] Например, нарушение работы сервера голландского центра сертификации Diginotar, полный отчет http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip- update.pdf

[6] Для получения дополнительной информации см. RFC 2827 Фильтрация входящего сетевого трафика: защита от атак с целью отказа в обслуживании с применением спуфинга исходных IP-адресов (http://tools.ietf.org/html/rfc2827)

[7] Хардин, Г. «Трагедия общин». Science 162 (3859): 1243–1248, 1968.

[8] Рабочая группа Conficker, http://www.confickerworkinggroup.org/wiki/

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Тел.: +41 22 807 1444
Факс: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA (США)
Тел.: +1 703 439 2120
Факс: +1 703 326 9881
Электронная почта:
info@isoc.org