ПЕТЕРБУРГСКИЙ МЕЖДУНАРОДНЫЙ ЭКОНОМИЧЕСКИЙ ФОРУМ

16—18 июня 2016

ВЫЗОВЫ В КИБЕРПРОСТРАНСТВЕ. ВОЗМОЖНО ЛИ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ В СЕТИ?

16 июня 2016 г., 10:15—11:30

Павильон G, Конференц-зал G2

Санкт-Петербург, Россия

2016

Модератор:

Эрик Очард, Главный технический корреспондент по региону Европа, Ближний Восток и Африка, Thomson Reuters

Выступающие:

Йон Фредрик Баксаас, Председатель, GSMA

Александр Жаров, Руководитель, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (Роскомнадзор)

Герман Клименко, Советник Президента Российской Федерации

Станислав Кузнецов, Заместитель Председателя Правления, Сбербанк России

Сан Чжин Пак, Президент, Samsung Electronics

Илья Сачков, Основатель, генеральный директор, Group-IB

Руслан Юнусов, Генеральный директор, Российский квантовый центр

Участники дискуссии:

Томмазо Каларко, Профессор, Institute for Complex Quantum Systems (ICQ)

Тимоти Клау, Партнер, руководитель отдела анализа и контроля рисков, PwC Russia

Хокон Виум Ли, Главный технический директор, Opera Software

Михаил Якушев, Вице-президент по связям с Россией и странами СНГ и Восточной Европы, ICANN

E. Auchard:

That video spelled out a few of the issues we are going to be talking about today. This panel appears to be about cyber crime. I say that, because nothing in this subject is ever what it seems. Things are very murky whenever we talk about cyber crime and try to attribute responsibility for what is happening. The format today is that we are going to have the various panellists give short introductions about their take on this particular issue from their company or regulatory perspective. I will follow up with specific questions from each of the speakers, and then we will open it up for members of the audience to ask questions of the panellists. I just want to make sure to point out that four of our panellists are over there; they are very much a part of the panel, but it is just that our format is such that we have a round table plus four more. With that, I would like Jon Fredrik to get started.

J. F. Baksaas:

Thank you, Eric. I have the luxury of having the “B” in the alphabet. I am ready to start. The question about cyber security is a question that comes to mind through examples, which we just saw. The other side of this coin is that while the world goes digital, we tend to see the opportunities of that digitalization very clearly, and many companies rush for their opportunities. But there is still a whole ecosystem in play here, with lots of elements that form what is perceived or the actual security level of things when they reach the consumer or the user, whether that is a company, a government institution, a bank, or an individual. It is a very complex world out there to be able to say that this is an absolutely secure environment.

My hat today is GSMA. GSMA is the industry organization of mobile operators in the world. Basically, all mobile operators are members of this association. And in this association, cyber security is, of course, a very central point. But we are only

one element of the many elements that need to take part in the security questions around societies becoming more digital.

The first aspect of what we are concerned about in this organization, GSMA, is the network access security element. Who is on the network on any point in time? What is that player in the network doing in the network at all times? That is our number one concern. Here, we are working with industry players in the ecosystem in general, but also with communities of hackers in a kind of friendly setting where the network access element is being put up to special tests, and as such, developing. It is widely known that the 2G protocol that was launched in the late 1980s has been exposed and can be fairly easily penetrated these days. But on the other hand, both the 3G and the 4G protocols are much better. Are they bulletproof? Probably not. But they are at least on a completely different level than the 2G.

The new element that is coming up is the Internet of Things. An Internet of Things is described as a phenomenal opportunity for many players, addressing new needs for everything related both to companies' usage and individual usage. The potential is so strong. But on the other hand, if the Internet of things does not have a security element attached to it that is also very strong, we will have a severe problem, both when it comes to cyber crime and also for many other potential issues. So, one could say that as industry players with network capacities, we are moving slowly in that direction.

That slowness is also a concern and mirrors the need for security on the Internet of Things coming into the world. Because, as an individual, I want my Internet of Things to be secure; I do not want any one of you guys to look into my things. I think that goes without saying; that is normal consumer behaviour. But on the other hand, can network operators and the ones that offer you this Internet of things guarantee this going forward? That is a big question. So let me stop there.

E. Auchard:

Next, German? Maybe you could say some introductory comments?

Г. Клименко:

Спасибо. Я являюсь советником Президента Путина и представляю Институт Развития Интернета, который по его поручению занимается интеграцией Интернета с отраслями экономики. Тема кибербезопасности очень важна, но сначала я хотел бы обратиться к истории. Человечество тысячелетиями занималось своей безопасностью. Оно выработало прекрасные механизмы для защиты дверей (ключи, сигнализация), денег (векселя для их безопасной перевозки) и несколько тысячелетий жило прекрасно. Но в последние десять лет выяснилось, что все его корпоративные и частные тайны вдруг стали открытыми. У нас нет ни квалификации, ни опыта, передаваемого из поколения в поколение, для контроля за имуществом, за информацией, за детьми, даже за мыслями. Справедливо было сказано про Интернет вещей: когда в вашем доме холодильники не только начинают разговаривать, они еще и становятся уязвимыми, от этого делается страшно. Плохо, если скиснет молоко, но гораздо хуже, если ваша личная информация попадет к конкурентам. Беда заключается в том, что органы, которые должны обеспечивать безопасность граждан и предприятий, то есть система полиции и армии, вдруг перестали действовать, опять же за отсутствием нужной квалификации и опыта.

Буквально вчера я был на телевизионном шоу у Петра Толстого, где обсуждались так называемые группы смерти и поднималась та же проблема. Здесь говорили в основном о «железе» и телекоммуникациях, а я бы хотел поговорить об Интернете. Наши граждане наконец-то узнали, что через Интернет можно не только переписываться, влюбляться, но и доводить до самоубийства. Многие почувствовали большое, агрессивное

желание все закрыть. Ведь проблема кибербезопасности, как любой другой безопасности, — это ее стоимость и эффективность. Понятно, что полный контроль за новым явлением, пока что малознакомым, можно получить, воспользовавшись опытом либо Северной Кореи, где вообще все запрещено, либо Китая. Общество — и мы это видим — склоняется к жестким мерам по отношению к самому Интернету. Беда заключается в том, что мы хорошо помним опыт Советского Союза, когда был введен сухой закон, и в результате люди не перестали пить, потому что им не дали заменитель, а стали употреблять другие напитки, что не раз приводило к трагедии.

Наша основная задача, в том числе на этой встрече, не сводится к диагностике проблемы, она очевидна: отсутствие опыта. Я вырос во дворе, у меня был очень ограниченный круг общения, родители были для меня безусловным авторитетом. Современные дети растут в социальных сетях, у них авторитеты совершенно другие, и мы не знаем, какие поставить ограничения, нужны ли эти меры. Мы встретились с новым явлением, а неизвестное пугает. Важно, чтобы испуг общества не превратился в жесткий контроль и санкции, ведь они могут убить новую экономику. С точки зрения интернет-технологий Россия сегодня выглядит настолько хорошо на фоне других стран, что необходимо искать баланс в развитии и ни в коем случае не под видом защиты (иногда это очень выгодно — оперируя вопросами безопасности, жестко ограничивать развитие). Мы и так очень болезненно воспринимаем любые запреты, этому способствует наша наследственная память. Тем не менее мне кажется, что картина развития на данный момент положительная. Нужно только точечно диагностировать проблемы и точечно их решать. С этим прекрасно справляется следующий выступающий. Спасибо.

E. Auchard:

Next I'd like to have Stanislav.

С. Кузнецов:

Добрый день, дамы и господа. Я представляю Сбербанк России. Это крупнейший банк в Центральной и Восточной Европе. Мы, как и другие финансовые кредитные учреждения и крупные корпорации, конечно же, сталкиваемся с проблемой обеспечения кибербезопасности. Я бы хотел продолжить тему, которую обозначил Йон. Он сказал, что мы пытаемся решить эту проблему в течение уже нескольких лет. Мне кажется, активная фаза противостояния киберугрозам насчитывает 12—15 лет. Существуют три основных направления киберпреступлений: блокирование деятельности компаний — формат DDoS-атак всем известен; воровство данных и использование их в криминальных целях; управление различными системами от имени этих компаний. Были попытки управлять аэропортами, самолетами и так далее.

Сбербанк России встречается с подобными угрозами ежедневно и, конечно же, разрабатывает систему противостояния. Эти 15 лет можно разделить на три этапа. В начале 2000-х годов все использовали антивирусы и были довольны. Уже через семь-восемь лет, примерно в 2010 году, стало ясно, что антивирусы не справляются с поставленной задачей, и начался этап так называемых расследований, поисков первопричины происходящего. По этому пути шел весь мир — кто-то быстрее, кто-то чуть медленнее, кто-то вообще топтался на месте. Уже в конце 2015 — начале 2016 года мы оказались на пороге новой эры — эры искусственного интеллекта, когда назрела необходимость полной коллаборации и использования облаков, все должны хорошо это понимать.

Безусловно, нас беспокоят цифры: объем ущерба от киберпреступлений и расходы компаний на защиту, а также число киберпреступников в мире —

сегодня их около 40 миллионов человек. Главная особенность состоит в том, что исчезли границы. Если раньше правоохранительные органы имели представление о размерах преступной группировки, то теперь все это умножилось в сотни раз, потому что границ не существует. Противодействие в странах мира строится по трем направлениям. Первое — законодательное, оно заключается в создании системы законов, нацеленных на борьбу с киберугрозами. Второе — отраслевое, когда целые отрасли создают свои системы правил, обмена информацией, операционных действий. Например, в финансовой отрасли зачисление денег на те или иные счета имеет определенные правила и систему защиты. Третье — корпоративное, когда крупные корпорации строят собственные системы защиты. Развитие этих трех направлений происходит неравномерно. Поскольку в России на сегодняшний день почти не существует законов в сфере кибербезопасности, усилия корпораций переходят в положение номер три, то есть они вынуждены создавать собственные системы, испытывая большую потребность в развитии первого и второго уровня поддержки со стороны государства.

Примерно с декабря Сбербанк начал мониторинг ситуации с вирусами в мире, в самых разных странах. Мы увидели, какие страны находятся в лучшей ситуации, а какие в худшей. Я вынужден с сожалением констатировать, что Россия сегодня — мишень номер один, главный объект внимания хакеров и киберпреступников. Это связано со слабостью, во-первых, нашего законодательства, а во-вторых, правоохранительной системы. По количеству она имеет большие возможности, но сеть противодействия киберпреступникам достаточно небольшая. И в-третьих, зачастую мы не имеем общих правил для обмена информацией. Приведу пример: до сих пор ни банки, ни телекомы не имеют единой базы данных, чтобы обмениваться стоп-листами, дискредитировавшими себя номерами

телефонов, карт и так далее. У каждого есть свой стоп-лист, но они никак не связаны друг с другом.

Что делает Сбербанк? Он идет по третьему пути: создает собственную систему, привлекая внимание государственных институтов, чтобы сделать все возможное для усиления первого, законодательного пути. В частности, в мае прошлого года по инициативе Сбербанка была внесена поправка в статью 187 УК, и теперь за скимминг стали давать шесть лет лишения свободы. Статистика этого вида кражи сразу пошла вниз. Как только государство начинает реагировать, мы видим хорошую статистику.

Не могу не коснуться темы, которую поднял Герман Клименко, — тему беспокойства, испуга. Пришло время серьезно говорить о культуре кибербезопасности, сегодня они имеют большое значение не только для компаний или государственных институтов, но и для общества в целом. Мы уже попали в новую реальность, и должны выработать новые привычки, связанные с соблюдением правил кибербезопасности, подобно привычке выходя из квартиры проверять, есть ли ключи в кармане. Сбербанк двигается по этому пути, работает с сотрудниками, инструктирует, организует лекции, проводит учения. По моему мнению, самый наглядный прием — демонстрация сотрудникам того, что происходит, когда хакеры заражают компьютер жертвы, и каковы последствия. Это достаточно легко показать и очень эффективно. Большое спасибо за внимание.

Э. Очард:

Thank you very much. Ilia, maybe we could have you go next?

И. Сачков:

Спасибо за возможность сказать здесь пару слов. Хотя по образованию я технический специалист, компьютерный криминалист, и Group-IB делает

именно технологии, я хотел бы остановиться на человеческом факторе киберпреступности, потому что за преступлениями стоят конкретные люди.

Средний возраст компьютерного преступника, в том числе в России, — примерно 25—26 лет. Официальная статистика МВД России показывает, что ни одного человека в возрасте до 18 лет к уголовной ответственности за компьютерные преступления не привлекали. В 2015 году была рассмотрена 61 000 дел о подростковой преступности, в марте — 12 000 дел, но ни одного — по компьютерным преступлениям. Таким образом, на этапе формирования этой проблемы мы имеем огромное количество людей, которых никто не мониторит.

Кто же создает преступные технологии? Чтобы понять это, мы проводим совместное исследование с пятью вузами, двумя российскими и тремя американскими. Получается, что гениальные вирусописатели — это чаще всего люди с аутизмом. Сам по себе он не является проблемой, среди наших криминалистов в Group-IB тоже есть люди с аутизмом. Проблема в том, чтобы еще на этапе детских учебных заведений такие люди были детектированы государством и определенным образом воспитаны, потому что недостаточное внимание и агрессия, которую в обществе вызывают личности, не похожие на других, вызывают ответную агрессию, и иногда она проявляется в виде гениальных компьютерных преступлений.

Еще одна проблема связана с политикой. Борьба с киберпреступностью никоим образом не должна быть политизирована, потому что в Интернете нет границ, компьютерные преступления — это единственные преступления в мире, которые можно совершить из одной страны в ста других странах одновременно. Так многие русские хакеры, находящиеся в розыске, уезжают на Украину и оттуда воруют деньги у российских банков, а украинские уезжают в Россию и отсюда воруют деньги в украинских банках. Борьба с компьютерной преступностью должна быть похожа на борьбу с болезнями или глобальным потеплением. Это общая проблема. В этом году

мы стали свидетелями того, как атака на казанский банк поменяла курс рубля, а месяц назад на конференции Positive Hack Days абсолютно реальная модель действующей гидроэлектростанции с действующей системой безопасности была взломана, и виртуальный город затопила вода. К счастью для общества, пока что основная цель компьютерных преступлений — деньги. Но уже у одного только ИГИЛ сейчас есть 12 активных кибертеррористических группировок, преследующих совершенно другие цели.

Я выдвигаю четыре тезиса борьбы с компьютерной преступностью. Во-первых, нужно понимать мотивы и работать с людьми еще в детстве. В обществе должно быть воспитано отношение к киберпреступникам: опросы общественного мнения показывают, что негативного отношения к этому виду преступности в целом у населения России, США и Европы не существует.

Второе: борьба с компьютерным преступлением должна проходить полный цикл — от воспитания до определенных законов, правоприменения и наблюдения по выходе из тюрьмы. Сейчас такая работа не ведется. Многие компьютерные преступники заканчивают карьеру за два года: этого достаточно, чтобы полностью легализоваться в качестве реального бизнесмена. И в России, и во многих других странах есть преступные группы, занимающиеся и ресторанным бизнесом, и кинобизнесом (случай 2015 года). В прошлом этих групп — компьютерная преступность, но сейчас они выглядят как абсолютно легальный бизнес.

Третий важный тезис: в борьбе с компьютерными преступлениями не должно быть никакой политики, иначе все закончится глобальной техногенной катастрофой.

Наконец, я абсолютно согласен с позицией Сбербанка по поводу корреляции данных, единых баз данных и раннего предупреждения атак. Именно это позволит бороться с компьютерными преступлениями

технологически. Но, вернусь к тезису номер один: за компьютерными преступлениями стоят люди, и чисто технологически, без работы с людьми, вопрос компьютерной преступности решен не будет. Спасибо.

Э. Очард:

Ruslan, maybe you could tell us about some new technology developments that may come to bear in this discussion?

Р. Юнусов:

Спасибо. Я представляю Российский квантовый центр. Коллеги подчеркнули несколько аспектов кибербезопасности: технический — важно иметь протоколы шифрования, которые сложно или невозможно взломать, — социальный и так далее. За последние 10—15 лет возросла роль информации и, соответственно, возросли риски. Сейчас, когда мы говорим о кибербезопасности, мы подразумеваем риск потерять деньги. Но в следующие 10—15 лет мы будем рисковать жизнью или здоровьем, потому что это коснется, например, имплантов, и стоимость передаваемой информации вырастет еще раз. Квантовый центр был организован пять лет назад с целью создания квантового компьютера и других квантовых технологий и выпуска их на рынок. Все эти годы в мире над созданием квантового компьютера работает много групп, и эта цель из эфемерной и непонятной становится осуществимой через 10—15 лет. Здесь присутствует профессор Томмазо Каларко, он лучше расскажет, когда этот компьютер появится и как сильно он изменит наш мир.

Я бы хотел сконцентрироваться на одном из результатов появления квантового компьютера, а именно на его возможности дешифровать действующие алгоритмы — тем самым системы шифрования, которые сейчас очень широко применяются, сразу будут дискредитированы. Более того, если, например, в США появится квантовый компьютер, мы можем об

этом не узнать, в статьях об этом не напишут: зачем писать, если можно спокойно его использовать. Все это выглядит плохо, но на самом деле в квантовых технологиях есть и позитивные стороны: на каждый меч находится щит. Ряд проблем решает технология квантовой криптографии, и мы ею активно занимаемся. Конечно, это не универсальное решение, наверное, оно не поможет добиться успеха в решении проблемы групп смерти. Зато оно способно обеспечить безопасную передачу данных из одной точки в другую, чтобы по пути никто не смог перехватить их и дешифровать сигнал. Они гарантируются не сложностью математического шифрования, обратной задачи и так далее, а фундаментальными законами физики: если мы передаем информацию с помощью одиночных частиц — на один фотон записываем один бит, — ее нельзя перехватить, дешифровать и отправить дальше. К сожалению или к счастью, так устроена природа, что незаметное наблюдение квантовых систем невозможно в принципе, каким бы совершенным прибором ни пользовались хакеры.

По совпадению, как раз сегодня мы объявили о том, что нам удалось технически реализовать передачу квантового ключа уже не в лабораторных условиях, а в реальных. Мы запустили линию квантовой связи между двумя офисами нашего партнера — Газпромбанка — и передали по ней квантовые ключи. Конечно же, мы не первые в мире, но я считаю, этот шаг показывает, что мы становимся на уровень ведущих держав, а их немного: Китай, США, Швейцария, некоторые другие страны Европы, Япония, Корея. Нам приятно, что в России заработала такая технология, и, я надеюсь, в течение полутора лет мы выйдем на рынок. К сожалению, это технология первого поколения, и у нее есть технические ограничения: передача происходит по волокну длиной порядка 100 километров, скорость передачи маленькая, поэтому всю информацию дата-центры передавать по квантовому каналу не могут. Но в мире уже существуют решения, когда

квантовые коробочки соединяются с классическими потоковыми шифраторами. В этом гибридном режиме передается только ключ, который очень часто обновляется. Система не абсолютно безопасная, но безопасней, чем предыдущие решения.
Вот то, что я хотел сказать о безопасности информации и месте квантовых технологий в сегодняшнем и будущем мире. Спасибо.

E. Auchard:
Thank you. Mr Zharov, maybe you could throw a new perspective on how the citizens and individuals are affected by these trends?

А. Жаров:
Спасибо, Эрик. Я хотел бы несколько оживить дискуссию. Во вступлении и в презентациях моих коллег достаточно много говорилось о компьютерных преступниках, преодолевающих барьеры, которые ставят на их пути корпорации. Но мне кажется, что вопрос информационной безопасности значительно шире. Попробую это доказать. Количество интернет-зависимых экономик с каждым годом, если не с каждым месяцем, растет. Зависимость личности, общества и корпораций от сети становится всё выше. Мы всё больше времени проводим в сети и совершаем в ней всё больше действий. Количество услуг и товаров, которые мы получаем через сеть, также с каждым днем растет. Сеть эволюционирует, и увеличивается прозрачность личности, корпораций, общества и экономики для транснациональных компаний — я говорю о социальных сетях, поисковых сервисах и других крупных транснациональных корпорациях, которые работают в сети. А ведь очевидно, что вопросы информационной безопасности касаются не только борьбы с преступниками, но и защиты личных и корпоративных данных. Для этого создаются новые рынки

компаний, которые, как компания господина Сачкова, предлагают услуги по защите информации.

Кроме того, принципиально важно, находясь в сети, соблюдать правила жизни в ней. Далеко не все пострадавшие в инцидентах на дорогах стали жертвами преступников: они просто не соблюдали правила дорожного движения…

С точки зрения Роскомнадзора, вопрос информационной безопасности делится на несколько уровней. Во-первых, это национальный уровень. Мы должны говорить о национальном цифровом суверенитете государства как совокупности институтов, представителей общества, представителей бизнеса — мы все должны быть уверены в том, что информация в национальном пространстве распространяется суверенно, инфраструктура распространения этой информации находится под контролем либо бизнес-единиц, которые работают на этой территории, либо государства.

Если мы говорим про общественный уровень информационной безопасности, то в Российской Федерации, например, создан Единый реестр запрещенной информации, который защищает детей от негативных элементов, присутствующих в сети: детской порнографии, информации о распространении наркотиков, информации о самоубийствах, которая в последние месяцы прозвучала достаточно громко (об этом упоминал Герман Клименко).

На корпоративном уровне информационная безопасность контролируется и финансируется каждой корпорацией самостоятельно. Насколько я знаю, в мире доля затрат всех корпораций на кибербезопасность не очень высока, это 4% от общего оборота, но, видимо, в дальнейшем эта цифра будет расти.

На личном уровне информационной безопасности за последнее время произошли фундаментальные сдвиги. Потребитель услуг и товаров перешел с позиции безличного потребителя в объект достаточно

интенсивного изучения. Получив его персональные данные, корпорации формируют индивидуальный профиль пользователя и присылают ему таргетированную рекламу и предложения, которые могут его заинтересовать. Это тоже серьезный вопрос информационной безопасности.

Если говорить более широко про большие данные, big data, которые будут обсуждаться завтра на семинаре в 12.00 (надеюсь, он будет интересным), то совокупность данных, на которые сейчас пользователи дают согласие в сети, — а это и геолокация, и программы распознавания изображений и голоса, видео и фото, которые хранятся в облаках больших корпораций, — делают жизнь каждого человека прозрачной. Где допустимые границы прозрачности, насколько корпорации могут проникать в личное пространство гражданина и насколько он защищен — мне кажется, это вопросы для серьезной дискуссии.

В любом случае, я хочу сделать предложение. После Петербургского экономического форума Роскомнадзор готов открыть на своей площадке постоянно действующий семинар, мы предлагаем назвать его «Цифровой дом» — если переводить на английский, не Digital home, a Digital privacy, — с участием РОЦИТ, РАЭК, ИРИ и всех заинтересованных бизнес-структур. На этом семинаре мы сможем очертить границы, которые должны оставаться личными, комфортными, семейными и неприкосновенными. Я думаю, что эту работу можно включить в систему корпоративной социальной ответственности, а последнюю со временем интегрировать в систему ответственности на уровне международных стандартов отчетности GRI и G3. Благодарю вас за внимание.

E. Auchard:

Thank you. Why don’t we have Mr. Park? Thank you.

S. J. Park:

Ladies and gentlemen, good morning. My name is Sang Jin Park, president of Samsung Electronics. As you may know, Samsung is a mobile phone manufacturer. We cannot imagine our lives without the smartphone these days, but interestingly, it has only been with us for 10 years. Smartphones make our lives safer and faster, but at the same time, our privacy is exposed to the public with the Internet applications and software on our smartphones. This is because the smartphone is an IT platform connecting various types of devices. Moreover, IoT will lead our future lifestyle: smartphones, smart hospitals, smart schools, transport, logistics, you name it. Our reality and social infrastructure is more convenient and easier to process.

Again, the essence and beauty of IoT is connectivity. However, connectivity must come along with security. Although Cisco estimates that the IoT world will consist of 50 billion devices connected to the Internet by the year 2020, we have seen that big-name automobiles were hacked by simple game controllers like a Nintendo. This is only for an automobile. The IoT world will not connect properly without security. Therefore, security is fundamental to the IoT era. It is crucial to have a common policy, collaboration, and technology development to gain security solutions. Government must play a key role in reaching a consensus among international society. And the private sector needs to support technology and innovation development.

Samsung has taken this into consideration very seriously and continues to research and develop how we can contribute to our society with innovations. As a result, we recently unveiled KNOX as a mobile security platform and Tizen as an open operating system for smartphones with enhanced security. KNOX is a defence-grade mobile security platform built into devices. Samsung KNOX protects personal privacy from hardware and software applications by multi-layered security technology. KNOX has been already reflected to mobile devices like smartphones and tablet PCs. We are developing more innovative devices for

the IoT era. Samsung KNOX has a secure partition, or a storage space. The KNOX workspace container is designed to isolate, separate, encrypt, and protect work data from other data. That is a strong point. The user can store their business information and personally sensitive data and applications separately. It is not just an application but the most secure solution. Samsung KNOX has received the highest ratings for a mobile security platform from 22 countries, including the United States, China, and France.

Tizen is open source. That means a particular company does not hold the exclusive rights to it. Anybody can participate in developing that process and adapt their interface and UI to make it as unique as they like. The openness is the biggest advantage of Tizen, as it makes it easier to develop using Tizen software kits. Above all, Tizen is not limited to mobile devices. It has limitless expandability as an IT platform. It has enabled us to connect all products, such as smartphones, smart TVs, fridges, and printers. A great aspect of Tizen smartphones is that it was developed for the friendly smartphone, as it enables diverse functions based on modularized coding. In particular, Tizen's modularized coding structure provides customized security, because Tizen allows a user to add his or her own customized personal security module to the platform security module.

Samsung is committed to promoting freedom and connectivity with Tizen and IoT, and also to protecting against any threat to security with our own and collaborative solutions. In this regard, our collaboration with the Russian government has been very meaningful quite recently, and we look forward to synergy with other governments. Recently in Russia, we launched a Tizen smartphone with KNOX, which got FSTC certification from the authorities. This launch is a humble but very meaningful contribution to the diversity and richness of IT platforms with strong security. Meanwhile, we also believe that accessible regulation of Internet space could damage connectivity, which is a great asset to our Internet. So, for harmonious and balanced solutions on freedom versus

security, creative public-private partnerships are quite crucial. Samsung is committed to making their best effort for IT collaboration to human life and bridging all the related stakeholders to contribute to healthy and strong cybersecurity. Thank you.

E. Auchard:

Thank you, Mr. Park. Tommaso, maybe you could speak now?

T. Calarco:

Thank you. I work on quantum technologies. I am on the board of the Russian Quantum Centre. I was the first acting managing director, and recently I got EUR 1 billion from the European Commission to develop quantum technologies in Europe. Why is that? What are quantum technologies? Well, everybody has quantum technologies in their pocket. At this moment, everything that electronics produces is a first-generation quantum technology. It is based on such devices as transistors and lasers. Facebook and the Internet are based on fibre optic communication, and we would not have that if we did not have quantum mechanics, which was developed in the last century.

Now, this is the first generation. It is not secure. Why is that? It is because we are sending messages that are encoded on a fibre optic signal. Now comes the NSA, or maybe the Chinese. In these signals, per bit, we have many, many thousands, millions, billions of photons. Now they will steal, let us say, a thousand or a million photons. Who can notice that? They can read the information. Of course, we need to have encryption based on software, based on mathematics, but it is not absolutely secure; otherwise, we would not be here discussing these things.

If we go down to the single photon level, I cannot take half a photon, because that is a quantum object. Quantum means that it is not possible to get any smaller. It means that if they try to steal my photon, then we will immediately

notice. So if the photon has arrived, we are sure by the laws of nature that this is secure. This is one of the many applications of quantum technologies.

Another one is quantum computing, which in principle is a threat to current security, but is also a big opportunity in terms of simulating materials and developing new chemical compounds and new materials. Another is sensing. If you use single quantum devices in order to measure, for instance, the field produced by a single neuron, you get unprecedented methods for diagnostics. Now, this is what guarantees absolute security. This was the main argument to convince the European Commission to really go further in this direction a couple of years ago, because this is a very important aspect. As we know, there are now niche companies which sell these things. You can buy a quantum rack, which allows you to do these secure communications over segments up to 300 kilometres. They are currently marketing these in Europe.

Now if you want to go global, you need quantum repeaters. So you need some small quantum computers which make it go over global scales. This is research that we need to develop. In Europe and also in Russia, yesterday's announcement was very exciting, that the Quantum Centre that was started a few years ago has been able to now bring products which are close to the market. We have huge competence here, but the point is that where there may be industrial capacity in terms of investment, it has not yet been developed here. Google, IBM, Intel, and Microsoft are investing hundreds of millions of dollars in this field, and so now the European Commission also wants to bring it further to fruition on our side of the world map. This is something that can be very promising. There is a market around the corner, and I am happy to discuss that later if there is interest.

E. Auchard:

Thank you very much. Tim, could you?

T. Clough:

Good morning, ladies and gentlemen. Obviously, there has been a bit of a spotlight on technology and technology solutions that help companies prevent cyber threats. But I would like to just focus a little bit on the culture, the processes, and the people element, because they are often neglected, but they can be a very efficient and effective way of defending against cyber attacks. If we look at the video that was shown at the start, this clearly is a problem here in Russia. There was a 58% increase in reported cyber attacks in the last year, a tripling of attacks that were targeting intellectual property. So this is not just about personal data, credit card information; it is targeting intellectual property. It is trying to disrupt business.

Actually, most of those attacks are coming from individuals known to the organization: employees, ex-employees, partners, and service providers. And those are the parties where culture, process, and control can have the biggest impact. They can help prevent and reduce the impact of those parties targeting companies. The board of directors absolutely has a critical role to play in establishing the right culture of an organization with regards to cyber. They need to be setting the tone at the top. They need to be treating cyber as a strategic risk issue, one that can have operational, reputational, financial, and business critical impacts on their company. They need to be talking to the executive management about what risks the company faces and how the management team are preparing the company to defend themselves against those risks. They need to be testing their plans. They need to be running simulations. The board needs to be actively involved in building reporting lines and looking at escalation procedures. And with that in mind, the role of the chief information security officer is also absolutely critical. That individual now needs to be someone that can effect change in an organization, somehow who has been empowered by the board to drive change and build defences. It needs to be an individual that not

only has a good grasp of cyber matters but also understands corporate governance, controls, and the ability to change people and cultures.

Why is this important? If you look at some of the incidents that occurred around the world, many of them were already known to those companies. They existed. They had alarms going off, they had red flags, but no one did anything about it. It stayed in the IT department. It was not escalated. People did not know what to do, and as a result those issues got out of control and had a bigger impact than they ever should have. The board and the executive management team need to be talking to their employees about how and when they should be escalating, and if they do that, that will help to prevent and reduce the impact of some of these attacks. Ultimately, when you talk to many board members, they see cyber as a big, scary monster that is hiding in the dark. It is not; it is just another risk. And it is a risk that can be managed by making the right economic decisions and making the right levels of investment. Thank you.

E. Auchard:
Thanks, Tim. Hakon?

H. W. Lie:
My name is Hakon Wium Lie. I am with Opera Software. We make browsers. We have been making browsers since the last century. We have many users in Russia. And, as a browser maker, I feel I need to say something happy about the Internet. The Internet is a fantastic thing. It is truly remarkable that we have this global medium where everyone can participate, contribute, write, read, and communicate. You can just look at the people around here who are communicating right now on their devices. It is incredible.
We have also heard a lot of nice words about how there are threats out there, there are bad guys, there are crooks. And I am happy to see the involvement of

governments in this. We need to work together. We need to stop the bad guys. And browsers have an important role to play there, because browsers are what many people use as their most important tool. They use their browsers for their entire workday, eight hours a day if not more.

At Opera, we have been working very hard at this, and we have recently been adding two new features to the desktop version of Opera where you can turn on VPN, virtual private networks, and you can go anonymous. This could be scary in some ways, but it helps your privacy. We believe in privacy; we believe you should have the ability to surf anonymously. There are times when you do not want to disclose where you are or who you are.

At the same time, we have also added an ad block feature to block advertising. That is a controversial feature in some circles. I am sure some of you live from advertising, and we do too. Opera has a significant advertising business. But ads are troublesome, because they track you. They follow you from one site to the next. And sometimes, there are also bad guys tracking you using advertising-based technology. Advertising is also very heavy for your data quota, the bandwidth that you are using. In the tests we run, we see that 70% to 80% of the bits transferred to your computer are typically ads. And consumers and companies are paying for this. So we need to do ads better. We need to be able to turn them off and on. And we are experimenting with giving users the ability to control their digital presence and their safety and privacy.

E. Auchard:

Thank you, Hakon. Finally, Michael from ICANN can explain how cyber comes into play in the domain name system.

М. Якушев:

Спасибо. Добрый день, уважаемые коллеги. Мне кажется, это прекрасная панель, позволяющая всесторонне обсудить все вопросы, которые

обозначены в ее названии. В первую очередь я хотел бы согласиться с Александром Александровичем Жаровым в том, что вопросы кибербезопасности не сводятся к вопросам борьбы с киберпреступностью. Они намного шире, и пример из правил дорожного движения очень четко это иллюстрирует. Поэтому начать, наверное, нужно с определения киберпространства, чтобы мы все единообразно понимали, что представляет собой та сфера, где мы должны обеспечивать безопасность.

Киберпространство можно описать с помощью многоуровневой модели. В нижней ее части находятся физические системы — это каналы связи, компьютеры, технические устройства. Дальше идет логическая часть, которая связывает их в единую сеть. Наконец, выше располагаются разнообразные услуги, в том числе и финансовые, также являющиеся объектами атак. Сейчас выделяют и четвертый уровень — это контент, информация, циркулирующая по сети. На каждом уровне есть свои особенности и вещи, которые нужно по-особому защищать.

В этой многоуровневой модели наша корпорация отвечает за безопасность, стабильность и отказоустойчивость глобальных идентификаторов, таких как сетевые адреса, доменные имена. Наша деятельность основана на принципе заинтересованных сторон (иногда используют корявое слово multistakeholderism, multistakeholder approach). Это в обязательном порядке правительство, государственные органы, это частный бизнес, это экспертное сообщество, гражданское общество. Без взаимодействия между всеми сторонами процесса эффективной работы не получится, и наоборот, все успехи в развитии Интернета сегодня — следствие использования подхода заинтересованных сторон.

Сегодня еще не был затронут один важный аспект. Понятие безопасности абсолютно коррелирует с понятием доверия. Причем это комплексное доверие — сотрудников организации друг к другу, к тем, кто отвечает за безопасность, к конкурентам в общей ситуации на рынке. Даже такое

явление, как сокрытие информации о кибератаках, возникает потому, что она заключает в себе определенные репутационные риски. Значит, нужно доверие к законодателям, правоохранителям, к тем, кто продает технические устройства защиты информации, и к тем, кто производит расследование. Все вместе создает определенную репутацию, после чего корпорации, граждане, пользователи делают выбор, к кому обратиться, тем самым повышая безопасность как своей организации, так и общества в целом. Мне очень приятно, что за этим столом присутствуют представители организаций, занимающихся безопасностью, для которых доверие имеет большое значение. Это Илья Сачков, это Сбербанк — все мы видим, с какой активностью он занимается безопасностью последние годы, — это корпорация Samsung Electronics. Повышение доверия, безусловно, повлияет на то, чтобы обеспечить максимальную безопасность киберпространства. Спасибо.

E. Auchard:

Thank you. I am now going to ask some questions of the group. I think we need to speed this up. Just a general question, having listened to the discussion of the problem from so many different perspectives: What can be done by industry groups, by regulators, to begin to attack the economics of cyber crime? We know that the costs of cyber crime tools are plunging. It seems like things need to be done at the network and the regulatory levels to address these issues. It is an open question for anyone.

J. F. Baksaas:

I think the first thing is the principle of collaboration. In particular, on the network operating side where the GSMA is working, if there is a challenge in the technology field that comes around in one specific operation, that kind of challenge or problem or issue should be shared with others. Because, generally

speaking, one problem at one point in time can appear in other areas. So, one role is to be more visible about these kinds of issues among the same kind of players. And of course, this is already established in the relationship between operators in Samsung, for example. If there is a mishap in the network, we will collaborate on that issue in order to resolve it and to make sure that what we are there for, namely, to secure peer-to-peer communication, is really working in the trustworthy way that we want to be perceived as.

С. Кузнецов:

Я поддерживаю Йона. Сегодня только в условиях коллаборации можно добиться конкретных и быстрых результатов. Мы имеем тому доказательства. Приведу недавний пример взаимодействия между государственными институтами, правоохранительной системой и частными корпорациями, когда в России была задержана преступная группа Lurk. В течение пяти месяцев ее участники вывели из шести российских банков около миллиарда рублей. Сейчас для суда доказано чуть меньше миллиарда, но, наверное, докажут чуть больше. Проблему решили за два месяца, как только были объединены возможности различного рода частных компаний, крупных корпораций, в том числе занимающихся кибербезопасностью, и возможности государства. Впервые в истории России МВД возбудило дело о киберпреступлении по статье «Организованная преступность», и я думаю, она будет применяться в подобных случаях и дальше.

Второе, что нам может очень помочь и о чем коротко сказал сегодня Илья Сачков, — это кадры и образование. Примерно 20—25% компаний в мире, занимающихся кибербезопасностью, сегодня имеют вакантные должности. Качественных кадров еще меньше, а потребность в их привлечении еще больше. Российские вузы только частично покрывают некоторые аспекты этой сложной отрасли; вузов, которые готовили бы полноценных

специалистов в области кибербезопасности целевым образом, к сожалению, нет. На этом нам всем тоже нужно сосредоточить свое внимание. Александр говорил об организации «Цифрового дома», площадки под зонтиком Роскомнадзора. Мне кажется, это очень важное приглашение и источник новых возможностей для всех институтов, работающих в России и за рубежом. Спасибо.

E. Auchard:

Thank you very much.

И. Сачков:

Я хотел бы очень коротко высказаться о том, что можно сделать для ухудшения экономики преступности. Сейчас преступники часто используют одну и ту же инфраструктуру начиная от регистрации домена, аренды серверов и покупки вредоносного программного обеспечения. Технологически при помощи корреляции данных можно запоминать всю инфраструктуру, которую использовал преступник, чтобы в следующий раз он уже не смог этого сделать. Тогда каждая следующая атака будет для него экономически менее рентабельной.

Вторая вещь связана с обналичиванием денежных средств: если говорить о хищениях денег в интернет-банкинге, то половина преступлений чисто экономическая, она связана не с вирусами, а с тем, как люди в итоге получают наличные. Нужно легально обмениваться информацией о юридических и физических лицах, которые вовлечены в организацию преступного бизнеса. Количество этих единиц ограничено, но из-за отсутствия корреляции данных у нас преступникам удобно снова и снова использовать всех тех же лиц. Например, есть три физических лица, они используются для вывода денежных средств, потом они же открывают компанию, и на нее выводятся деньги. Многие банки этого не замечают.

Если включить элементарные математические методы построения графов между физическими и юридическими лицами, можно значительно усложнить компьютерным преступникам экономику обналичивания. Спасибо.

С. Кузнецов:

Мне кажется, то, о чем сказал Илья Сачков, представляет срочную задачу для России. Единый банк данных поможет нам всем взойти на новую ступень сотрудничества.

Г. Клименко:

Я бы хотел добавить. Преступники пользуются нашими ошибками в двух областях: аппаратной, и ее мы все стараемся развивать, и образовательной, которая тоже делится на две части. Во-первых, это образование населения. Аппаратно вы можете защищаться бесконечно, но компьютерная безграмотность населения, к сожалению, очень усложнит вашу задачу. Мы должны понимать: Интернет пришел к нам недавно, и страна делится на тех, кто еще ездит на бричках, и тех, у кого Феррари. Преступники пользуются тем, что в любой семье есть грамотные дети, но безграмотные родители. С этим надо что-то делать.

Вторая часть — образование правоохранительных органов. Я иногда в частном порядке беседую с судьями, и уровень их подготовки в этой сфере выглядит достаточно экзотично. Если вооружиться понятиями математики — необходимое и достаточное условия, то образование является необходимым условием. Наибольший урон компьютерным преступникам нанесут грамотные люди, которые перестанут попадаться им на крючок. Мы помним, каким образом закончилась борьба с дорвеями, — это была техническая история. А борьба с вирусами, которые рассылались по почте,

закончилась обучением населения. Поэтому образование должно быть поставлено во главу угла. Спасибо.

И. Сачков:

Герман, я могу воспользоваться возможностью задать вам вопрос? Два года назад мы с Сергеем Плуготаренко, директором РАЭК, писали в Министерство образования письмо с просьбой рассмотреть возможность уменьшить в школах количество часов, посвященных ОБЖ, и выделить часы на занятия, связанные с элементарной компьютерной грамотностью и информационной безопасностью. К сожалению, ответ мы не получили. Умение метать гранаты, я надеюсь, детям не пригодится, а вот знать, как правильно пользоваться браузером и какие есть риски в сети, в современных условиях необходимо — это знания будущего. Если можно, я прошу вас спросить у представителей Министерства образования, не ответят ли они на письмо.

Г. Клименко:

Хорошо, я попробую их спросить, где письмо.

Р. Юнусов:

Я бы хотел добавить одно замечание по поводу коллаборации. Она действительна важна, но необходимо отрегулировать один момент. Усложнение сферы кибербезопасности требует сводить вместе людей разных специальностей: физиков и инженеров, которым не так-то просто общаться между собой, а теперь еще и людей с гуманитарным образованием. Нужно реализовать мультидисциплинарный подход и создать такую площадку, где смогут общаться специалисты из разных областей. Это уже социальный вопрос.

А. Жаров:

Я абсолютно согласен, что сотрудничество — залог успеха, и то, о чем говорилось ранее, — кадры, прорывные решения, эффективные действия правоохранительных и надзорных органов в сфере финансов — безусловно, необходимо. Кроме того, необходимо доверие. Между государством, обществом и бизнесом должны быть выстроены доверительные отношения, для этого и нужна та площадка, о которой я говорил, — «Цифровой дом». В сентябре в Сочи проходит форум «Радиочастотный спектр». Он касается связи, но у нас есть опыт организации дискуссии на тему сети с РАЭК, и на сочинском форуме тоже можно создать дискуссионную площадку. Сегодня на нашем сайте будут опубликованы данные для аккредитации, телефон, электронный адрес и прочее. Если такая дискуссия получится, думаю, это будет интересно для всех.

И наконец, должны соблюдаться правила. Каждый человек и каждая корпорация должны четко понимать, по каким правилам они живут в сети, какую информацию следует хранить на бумаге, какую — на флэш-карте, какую — в своем гаджете и какую — в облаке. Чем архаичнее способ хранения, тем менее достижима информация. Спасибо.

E. Auchard:

Go ahead, Mr. Park.

S. J. Park:

As a multinational company, we are quite concerned about industrial espionage. I think the governments of the world must try to build a firewall between the private sector and the common sector through consensus between our governments. Any agency of any government must not try to obtain industrial secrets in the

cyber world from the private sector and overseas. That is our great concern these days.

E. Auchard:

We have heard about the crackdown on Lurk, the group that was said to be responsible for the attacks on the Russian banks. I have also read reports about the immediate impact that has had in the underground on some groups selling ransom and other tools pulling back because of those arrests. What can be done in Russia to extend that? What is the agenda for really going after cyber crime and clamping down on the environment so that young kids and professionals can benefit from this?

А. Жаров:

Я полагаю, что мне нужно ответить первому. В нашей стране работает Единый реестр запрещенной информации. В общей сложности за время его существования к нам поступило 303 000 обращений граждан и организаций по поводу детской порнографии в сети, пропаганды наркотиков и призывов к самоубийствам. В Единый реестр попало 125 000 ресурсов, с большинства из них информация была удалена, на 28 000 она остается, и они постоянно блокируются в Интернете операторами связи. Серьезный шаг был сделан год назад, когда вступил в силу закон о локализации персональных данных граждан Российской Федерации на территории России. На сегодняшний день к нам поступило 45 000 уведомлений от компаний о том, что они хранят персональные данные на территории России. Пользуясь случаем, я хочу поблагодарить господина Пака: компания Samsung одной из первых среди транснациональных гигантов в день вступления закона в силу анонсировала и представила свой дата-центр, где хранятся персональные данные россиян, пользующихся услугами компании.

На сегодняшний день мы проверили более 600 компаний, всего четыре из них не соблюдали правила этого закона. Мы сейчас никого не наказываем, мы проводим аудит. Компании готовы соблюдать закон, мы дали им еще шесть месяцев, чтобы принять необходимые меры. До конца года мы проверим еще 900 компаний. Я думаю, что этот первый, экспериментальный год, когда мы не пресекали ничью деятельность и никого не наказывали, а проводили аудит и давали компаниям советы — достаточный срок, чтобы все научились соблюдать этот важный закон. Мне кажется, в результате IT-бизнес получил стимул к развитию, в том числе с точки зрения информационной безопасности, так как способы хранения информации многообразны — гибридные облака и многое другое.

Сейчас государство предпринимает верные шаги на пути защиты граждан от негативной информации, на пути информационной безопасности, и это движение будет продолжаться в диалоге с бизнесом и обществом.

E. Auchard:

Stanislav, that will be the last comment. Thank you.

С. Кузнецов:

Спасибо. Я хотел бы и поддержать, и немного возразить вам, Александр. Государство действительно предпринимает определенные усилия, но скорость этих усилий очевидно недостаточна, это надо признать.

Отвечая на вопрос, что следует сделать сегодня в обществе, можно выделить четыре направления. Во-первых, надо чаще проводить такие дискуссии, иметь различные площадки для обсуждения, чтобы эта тема становилась публичной и к ней привлекалось должное внимание всех институтов.

Во-вторых, необходимо срочно укреплять российское законодательство, а для этого как можно скорее создать рабочую группу с участием

парламентариев, правительства, бизнеса, чтобы появились законы и было определено само понятие киберпреступления.

В-третьих, среди государственных институтов надо укрепить в первую очередь правоохранительную систему, потому что если сопоставить ущерб и количество киберпреступлений с очень небольшим числом сотрудников Управления «К» и ряда других подразделений, станет ясно, что они не могут даже зарегистрировать всю эту массу преступлений.

И четвертое: очень важно, чтобы Россия и все наши институты, работающие в области кибербезопасности, значительно активнее взаимодействовали с международным сегментом. Международной коллаборации должно придаваться гораздо большее значение. Мы здесь не просто отстаем, мы всегда в положении догоняющих.

E. Auchard:

Thank you everyone for attending. I am sorry I did not get to questions from the audience, but I think the last comment has framed the ideas for further discussion we all need to have on this topic. Thank you.