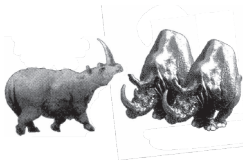

ВЫСОКОТЕХНОЛОГИЧНАЯ ПРЕСТУПНОСТЬ: НОВЫЕ ВЫЗОВЫ ДЛЯ ОБЩЕСТВА, ГОСУДАРСТВА И БИЗНЕСА

Экспоненциальное развитие и распространение интернет-технологий привело к возникновению нового феномена — высокотехнологичной преступности. В интернете совершаются как традиционные правонарушения — мошенничество, шантаж, кражи — так и преступления нового типа, противодействие которым зачастую выходит за рамки возможностей силовых структур. Интернет вещей, блокчейн, атрибуция — в лексикон полицейских и судей постепенно входят новые термины и понятия. Без тесного взаимодействия государства и общества, законодательной и исполнительной власти, а также скоординированных усилий всего мирового сообщества противодействовать новым вызовам вряд ли удастся.

Что такое высокотехнологичная преступность и как с ней бороться, обсуждалось на заседании круглого стола, проведенного Комитетом гражданских инициатив совместно с ПИР-Центром. Модератором дискуссии выступил председатель КГИ Алексей Кудрин. В мероприятии приняли участие члены Рабочей группы по международной информационной безопасности и глобальному управлению интернетом при Экспертном совете ПИР-Центра и эксперты КГИ: директор некоммерческого партнерства Информационная культура *Иван Бегтин, председатель Общественного Совета при МВД России Анатолий Кучерена, эксперт расширенной рабочей группы по реформированию МВД Елена Ларина, бизнес-консультант по информационной безопасности компании Cisco Алексей Лукацкий, советник министра внутренних дел Владимир Овчинский, генеральный директор компании Group-IB Илья Сачков, вице-президент по взаимодействию с заинтересованными сторонами в России, странах СНГ и Восточной Европы Корпорации Интернета по присвоению имен и номеров (ICANN) Михаил Якушев, руководитель стратегических проектов в России, странах Закавказья и Средней Азии* Лаборатории Касперского *Андрей Ярных и эксперт по вопросам управления бизнес-системами Алексей Яцына.*

АЛЕКСЕЙ КУДРИН: Наша сегодняшняя тема — *Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса*. Проблема преступлений с использованием высоких технологий, которую мы будем сегодня обсуждать, относительно нова, и государство не успевает на нее реагировать, правоохранительные органы и спецслужбы не готовы иметь дело с преступлениями

нового типа. Именно об этом и сегодня и поговорим. Наш первый докладчик — Илья Сачков, генеральный директор Group-IB, фирмы, занимающейся в том числе расследованием киберпреступлений, член Рабочей группы по международной информационной безопасности и глобальному управлению интернетом при Экспертном совете ПИР-Центра.

ИЛЬЯ САЧКОВ: Постараюсь очень кратко рассказать о трендах развития высокотехнологичной преступности, которые мы видим на территории Российской Федерации. Часть нашей работы — экспертно-криминалистическая деятельность по сопровождению особо сложных и резонансных уголовных дел против компьютерной преступности.

Самая большая проблема компьютерной преступности состоит в том, что общество в целом не совсем понимает, о чем идет речь, и не совсем верит в реальность высокотехнологичных правонарушений.

Есть потрясающий пример мошенничества против Московской биржи. В апреле мошенники от лица *Энергобанка* отправили на биржу заявку в размере 300 млн долл. и получили деньги. Банк обратился к нам за помощью, мы провели компьютерную криминалистическую экспертизу и нашли на компьютере, на котором находился брокерский терминал, вредоносное программное обеспечение. После этого мы получили запрос из Центрального банка России с требованием предоставить все материалы по делу, которые, между прочим, являются тайной следствия, что мы и ответили Центральному банку. В ответ получили штраф в 500 тыс. рублей за нарушение закона об инсайдерской деятельности. В итоге Центральный банк не верит в то, что заявку мог отправить вирус, в отношении *Энергобанка* ведется проверка, мы заплатили штраф 500 тыс. рублей, уголовное дело продолжается.

Когда мы говорим о компьютерной преступности, важно понимать, что общество знает лишь о верхушке айсберга. Возьмем пример *кардинга* — воровства денег с кредитных карточек — несложное и очень популярное преступление. Преступники пользуются специализированными интернет-магазинами, в которых продаются *дампы* кредитных карточек — копии магнитной полосы и PIN-коды, то есть то, что необходимо, чтобы снимать деньги с карточки. Набор дампов стоит порядка 10 долларов. В одном магазине продается около 5 млн валидных кредитных карточек. Принято думать, что теневой интернет — это что-то очень технически сложное, зеленые буквы на черном экране. Ничего подобного. У таких магазинов очень удобный интерфейс, они вообще мало чем (кроме товара) отличаются от обычных интернет-магазинов.

Когда правоохранительные органы видят подобные сайты в интернете, они пытаются их блокировать. Проблема в том, что, закрывая что-то в интернете без понимания, какие есть тенденции, с которыми надо бороться, правоохранители просто запускают гонку вооружений: поверьте, люди, которые создают кардинговые магазины, из-за того что закрыли один веб-сайт или ликвидировали домен, который стоит 20 долларов, не расстроятся и не скажут «пора, наверное, отходить от дел». Напротив, они станут умнее, хитрее, используют новые средства анонимного доступа.

Это, кстати, уже произошло с торговлей наркотикам. Изначально сайты, на которых их продавали, находились в обычных доменных зонах, и идентифицировать продавцов было достаточно легко. После принятия закона о блокировке их начали закрывать тысячами, а наркоторговцы ушли в теневой интернет. Но проблема никуда не делась, преступники стали изобретательнее, и теперь есть случаи (ФСКН, естественно, в курсе), когда наркотики заказывают с доставкой на дом через *Почту России*.

Сталкиваясь с преступлениями в интернете, очень важно анализировать всю цепочку. В случае с кардингом надо начинать с вопроса, каким образом похитили данные 5 миллионов карточек? В магазине, о котором я говорил, продавали дампы, полученные с зараженных терминалов в двух американских торговых сетях, *Target* и *Home Depot:* в одной похитили данные 70 млн карточек, в другой — 56 млн. Это очень важная информация, ведь если мы знаем точку компрометации, понятно, что делать дальше: любой человек, который был в этих торговых сетях в определенный промежуток времени, должен свою карточку заблокировать.

Также важно понимать, что владелец сайта, торгующего дампами, на комиссии с покупок заработал 6 млн долларов и в случае юридического преследования обеспечит себе первоклассную юридическую защиту. Кстати, появляется целый класс адвокатов, которые специализируются на защите компьютерных преступников, потому что это достаточно просто и очень прибыльно.

Что происходит сейчас на рынке компьютерной преступности, какие цели у злоумышленников? В первую очередь, деньги. Есть случаи, когда компьютерные преступники охотятся за информацией, но это сотые доли процента. Благодаря развитию платежных систем, интернет-банкинга для физических и юридических лиц процветает и воровство денег в платежных системах. Технически это относительно несложно, а если добавить в уравнение сверхприбыль и чувство безнаказанности, получается привлекательная картина. Надо иметь в виду, что компьютерный преступник не вызывает в обществе негативных эмоций — в отличие, например, от наркодилера.

Кроме того, законодательство не успевает за развитием высокотехнологичных преступлений, в нем много лакун. Компьютерные преступления можно за одну секунду совершить с территории одной страны через территорию другой страны в ста странах одновременно. Поэтому, несмотря на то что государство, общество, бизнес, люди тратят на информационную безопасность с каждым годом все больше, атак меньше не становится.

Отношение общества — это отдельный вопрос. Приведу старый, но показательный пример. Господин Аникин из Новосибирска в составе организованной преступной группы украл 9,5 млн долларов. В этот же год господин Блинников взломал щит на Садовом кольце и крутил там порнографию, а господин Гаврилов украл у своей соседки с дачного участка два куста роз и два куста лилий. Приговоры: Аникин — пять лет условно, Блинников — шесть лет колонии, Гаврилов — два года строгого режима.

В сознании людей кража электронных денег — это какая-то игра. В день оглашения приговора Аникину *Первый канал* выпустил новость про *талантливого моло-*

дого программиста, обхитрившего службу безопасности банка. Мы мониторим хакерские форумы, так вот, в этот день количество регистраций на них увеличилось на 400%.

Появляется целое поколение преступников, которые не обладают специальными знаниями, а используют готовые, понятные инструменты. Они, как правило, очень молоды, большинству нет 30 лет. Программы, которыми они пользуются, предельно просты и, что самое поразительное, имеют лицензионную политику, а создающие их злоумышленники тратят время на борьбу с пиратством и на защиту своей собственности. Эти сайты предлагают круглосуточную техподдержку на нескольких языках, которой могут позавидовать некоторые производители программного обеспечения. Работа с ними не требует никаких технических знаний. Есть, конечно, в составе преступных групп очень умные люди, но есть и те, у которых IQ в районе 40–60.

Члены преступной группы зачастую живут в разных регионах не только России, но и мира, что создает массу юридических проблем. Если преступная группа находится в трех — четырех странах, то о расследовании и кооперации правоохранительных органов можно забыть. Сейчас многие люди, которые в России подпадают под подозрение в совершении компьютерных преступлений, уезжают на Украину, а многие хакеры из Украины приезжают в Россию. Русские с территории Украины воруют деньги в российских банках, украинцы с территории России воруют деньги в украинских банках, и все остаются безнаказанными. Политика используется для того, чтобы скрывать компьютерные преступления. Есть и другие факторы. Кроме технической возможности заразить компьютеры, преступники ищут страны, где нет проблем с обналичкой. В России с этим все относительно просто, поэтому компьютерная преступность процветает. Решение вопроса с обналичкой нанесло бы очень эффективный удар по компьютерной преступности.

Мобильные устройства. Благодаря тому, что Android занял 80% мирового рынка устройств и телефоны на базе Android продаются за 20 долларов, идет огромное количество разработок вредоносного ПО под мобильные устройства. С телефоном можно сделать все, что угодно, начиная от кражи денежных средств и кончая прослушкой телефона, когда он просто лежит на столе. Стоимость заражения телефонов на черном рынке — приблизительно 100–200 долларов за тысячу аппаратов. Мы регулярно с 2006 г. выпускаем памятки по компьютерной гигиене, но есть ощущение, что их читают только наши сотрудники. В прошлом году мы выходили с инициативой в Министерство образования, предлагали часть часов ОБЖ выделять на правила компьютерной гигиены. К сожалению, не получилось. В то же время в США дети 6–8 лет изучают основы компьютерной грамотности. В 6–8 лет они знают, что такое фишинг, кардинг. Я считаю, что то же самое необходимо в России, потому что вчерашние школьники становятся сотрудниками предприятий и, не зная базовых вещей, становятся легкой мишенью для атак.

АЛЕКСЕЙ КУДРИН: А кроме вашей компании кто-то в России занимается похожей экспертизой?

ИЛЬЯ САЧКОВ: *Лаборатория Касперского* и мы.

АНДРЕЙ ЯРНЫХ: *Лаборатория Касперского* занимается подобными расследованиями, но в значительно меньшей степени, оперативно-разыскные мероприятия, в основном, проводятся правоохранительными органами.

Мы своей основной задачей видим выпуск программного обеспечения для защиты пользователей, а также стараемся максимально широко их информировать и повышать компьютерную грамотность. Несмотря на то, что все бесконечно повторяют, что интернет является агрессивной средой, пользователи зачастую проявляют беспечность и становятся жертвами злоумышленников.

Это несложно, даже в основе создания ботнет-сетей лежит обычное заражение компьютера троянской программой, после чего компьютеры объединяются в ботнет-сети, и уже под управлением злоумышленников происходят атаки на инфраструктуру, кражи денег, формирование финансовых баз украденных данных. То есть в основе проблемы — элементарная безграмотность пользователей.

АЛЕКСЕЙ КУДРИН: Какой вывод мы можем сделать? Нужно обучать детей в школах, создавать дополнительные системы защиты и выявления преступлений?

ИЛЬЯ САЧКОВ: Российские вузы не выпускают специалистов по цифровой криминалистике. У нас практически все самоучки. Мы проводили олимпиаду по компьютерной криминалистике, в ней участвовало 50 тысяч студентов, задания решили два человека. При этом по уровню сложности это был восьмой класс математической олимпиады.

Кроме того, надо развивать законодательство и обучать следователей и судей. Следователей, которые могут вести серьезные дела, в России можно пересчитать по пальцам. Серьезные сложности с судьями: человек, который выносит решение по компьютерному преступлению, должен понимать специфику.

Еще одна фундаментальная вещь. Интернет — глобальный феномен, требующий тесного взаимодействия между правоохранительными органами разных стран, а если законодательство не гармонизировано, общение между правоохранительными органами занимает не секунды, а часы, дни, а чаще всего месяцы и годы, при том что компьютерные преступники общаются в режиме реального времени, совершают преступления буквально за несколько секунд.

АЛЕКСЕЙ КУДРИН: Получается, нужна международная компьютерная разведка?

ИЛЬЯ САЧКОВ: Необходимо выработать единую конвенцию по борьбе с компьютерными преступлениями на базе ООН. Сейчас есть только Европейская конвенция, к которой Россия не присоединяется, потому что в ней есть статья, которая ущемляет наши национальные интересы. Это логично, но в результате уже много лет реального сотрудничества между нашими правоохранительными органами нет.

Кроме того, было бы полезно, чтобы в отделениях полиции были шаблоны заявлений по компьютерным преступлениям. Когда человек, ставший жертвой компьютерного преступления, приходит в районное отделение полиции и пытается

подать заявление, он встречает непонимание. У полиции нет единых баз данных по расследуемым преступлениям, поэтому бывает, что в разных регионах России ведется одно и то же уголовное дело и следователи не подозревают, что охотятся на одну и ту же преступную группу.

В правоохранительных органах работают очень серьезные профессионалы, но их категорически недостаточно. Сейчас они могут работать только против самых крупных организованных групп, но мелкими преступлениями, например кражами 300 рублей с мобильного телефона, никто не будет заниматься.

АЛЕКСЕЙ КУДРИН: Наш следующий докладчик — Иван Бегтин.

ИВАН БЕГТИН: На протяжении многих лет в России неэффективное использование бюджетных средств мешало государству внедрять давно разработанные информационные технологии. Теперь на помощь чиновникам могут прийти бизнес-круги, которые могут поделиться с ними своими наработками.

Однако государство должно активно стимулировать диалог с гражданами по вопросам информационной политики и формировать институты доверия. Граждане должны, например, иметь право требовать установки видеокамеры на перекрестке рядом со своим домом, где, по их сведениям, совершаются преступления, требовать от правоохранительных органов, чтобы те направляли патрульные машины в определенные районы, пользуясь необходимой информацией. Я давно говорю о том, как важно с правовой точки зрения обеспечить открытость данных, кроме разве что имеющих совсем личный характер. На мой взгляд, это должно быть внедрено в самые краткие сроки: от полугода до ближайших трех лет. Обратной стороной медали или фактором сдерживания распространения этих технологий является готовность российских органов внутренних дел вторгаться в личную жизнь граждан.

Современный уровень технологического развития позволяет хранить данные пользователей практически вечно. Когда в Германии пользователи Facebook на законных основаниях запрашивали свои персональные данные, им предоставляли все, что они когда-либо размещали, включая удаленный контент. Если люди старшего поколения прожили часть жизни без активного использования интернета и соцсетей, то все подробности жизни наших детей и внуков можно будет обнаружить и использовать в тех или иных целях.

В Великобритании и США, например, общественность начинает выражать недовольство тем, какой объем данных собирает полиция. В ближайшие 10–20 лет эта тенденция будет только усиливаться. Представьте себе, что у каждого полицейского будет при себе камера и данные, записанные с ее помощью, будут храниться вечно. Кроме того, камерами будут оснащены дроны самых разных типов. В итоге каждое преступление будет зафиксировано на видео, причем с нескольких ракурсов. Человек, совершивший преступление, будет находиться под постоянным наблюдением, причем с помощью не только камер, но и датчиков, закрепленных на его теле. С технологической точки зрения это осуществимо уже сейчас, просто в большинстве стран общество к такому не готово. Поэтому когда я слышу про неудачи внедрения автоматизации в МВД, я испытываю противоречивые чувства.

АЛЕКСЕЙ КУДРИН: Мне кажется, что США и другие страны с высоким уровнем развития компьютерных технологий в этом плане опережают нас лет на 15. Возможно, и вопросы использования и обработки этих данных, вмешательства в частную жизнь там продуманы более тщательно?

ИВАН БЕГТИН: По моим ощущениям, США в настоящее время — это гибрид тоталитарного и демократического государства. Просто, когда в распоряжении государства появляется эффективный инструмент, каким бы добрым, либеральным, демократичным оно ни было, ему очень трудно избежать соблазна им воспользоваться. А инструмент этот очень удобен для осуществления тотального контроля.

Количество информации в интернете не безгранично. В сутки человек способен создавать ограниченный объем контента, поэтому рано или поздно можно будет отследить действия каждого человека, что, собственно, и происходит. Именно поэтому АНБ стало подвергаться огромному давлению со стороны правозащитных организаций еще до того, как начало осуществлять массовую слежку. Можно даже вспомнить случай, когда американская правозащитная организация *Electronic Frontier Foundation* обнаружила, что некоторые модели принтеров оставляют специальную маркировку, позволяющую узнать, где был напечатан тот или иной документ.

АЛЕКСЕЙ КУДРИН: В Советском Союзе КГБ вел учет всех пишущих машинок, чтобы иметь возможность выяснить, на чем печатается запрещенная литература.

ИВАН БЕГТИН: Это разные традиции. У нас чаще всего прибегают к запретам, у них все разрешено, но находится под наблюдением. Мне трудно сказать, какой вариант хуже. Доподлинно известно, что большая часть операционных систем — Android, последние операционные системы от Microsoft — следят за пользователями. Появление систем в духе *Большого брата* тесно связано с вопросами компьютерной грамотности и культуры как рядовых граждан, так и государственных органов. Хотелось бы, чтобы при внедрении любой новой системы, которая затрагивает наши права и свободы, существовали какие-то площадки для диалога, где вырабатывалось бы взаимопонимание и создавались механизмы ограничения и контроля над теми людьми, которые этими системами управляют, потому что злоупотребления обязательно будут.

АЛЕКСЕЙ КУДРИН: А как бороться с *Большим братом*?

ИВАН БЕГТИН: В этой борьбе хорошо помогает коррупция в правоохранительных органах, но этого я советовать не стану. Поэтому, наверное, власти нужно повышать осведомленность граждан и вступать с ними в диалог.

АЛЕКСЕЙ КУДРИН: Следующий докладчик — Владимир Овчинский.

ВЛАДИМИР ОВЧИНСКИЙ: Сегодня мы говорим о полиции и преступности будущего. В нашем обществе обсуждение этих проблем с политической, социальной и криминологической точек зрения только начинается. Уже примерно пятнадцать лет правоохранительные органы ведут работу по предупреждению преступлений, по борьбе с компьютерной преступностью, с новыми типами преступлений,

возникающими на базе технологических инноваций. Но фактически обсуждения последствий внедрения новых технологий еще не было.

В этом году были опубликованы две очень интересные книги по этой теме — *Будущие преступления* М. Гудмана, бывшего старшего советника Интерпола, который сейчас консультирует один из проектов Google. Еще одна интересная работа — *Будущее насилия* Б. Уиттиса и Г. Блум, которая посвящена тем же вопросам. Так вот, в книге *Будущее насилия* приводятся результаты исследования Стюарта Бейкера, который до недавнего времени был руководителем Департамента политики министерства внутренней безопасности США. Этот ученый с помощью компьютерного анализа, в основу которого было положено два параметра — снижение цены коммерческого использования новой технологии и масштаб ее распространения — исследовал взаимосвязь применения новых технологий и изменения уровня преступности за последние 120 лет и сделал прогноз на ближайшее будущее. Он доказал, что в ближайшие годы мир захлестнет волна высокотехнологической преступности, с которой действующая государственная, банковская система и гражданское общество не смогут справляться. Многие либерально настроенные американские и европейские ученые приходят к неожиданному для них самих выводу о том, что, чтобы противостоять этой волне компьютерной преступности (и речь идет не просто о хищении банковских средств, но о терроризме и других формах насилия), надо будет отказаться от многих привычных ценностей, поступиться своими правами, даже в ряде случаев допустить правоохранительные органы в свою личную жизнь.

Вы знаете, что после атак 11 сентября на *башни-близнецы* в США был принят *Патриотический акт*, сейчас во Франции принят целый комплекс законодательных изменений, которые тоже касаются контроля за сетевым пространством, в Великобритании ужесточено законодательство и расширены права правоохранительных органов в этом плане. Мы должны быть готовы к тому, что придется чем-то поступиться. Ведь кибератака может закончиться и военным нападением, взрывом ядерной станции, взрывом энергосетей, выводом из строя всей технологической инфраструктуры.

Теперь о масштабах. Дело в том, что новая преступность, как раковая опухоль, уже успела пустить метастазы. Я приведу данные, которые были озвучены на 13-м Конгрессе ООН по предупреждению преступности и уголовному правосудию, который проходил в апреле этого года в Катаре. ООН провела исследования по виктимизации в 21 стране, и результаты такие, что если обычный уровень виктимизации, связанный с кражами, грабежами, разбоями, преступлениями против личностями — традиционной преступностью — равен от 1 до 5%, то виктимизация, связанная с киберпреступностью — мошенничеством с банковскими картами, похищением личных данных и прочим — составляет в этих странах до 17–18%.

То есть уже сейчас уровень виктимизации, число потерпевших почти в 4 раза выше, чем при традиционной преступности. При этом мы должны понимать, что традиционная преступность никуда не уйдет. Продолжаются кризисные явления в мировой экономике, продолжаются волны миграции беженцев. Любые потоки вынужденной миграции сами по себе всегда порождают преступность. Сейчас эти потоки идут и через Европу, и через евразийское пространство. Никуда

не уйдет обычное бытовое насилие, которое дает 80–90% всех убийств и нанесений тяжкого вреда здоровью. Правоохранительным органам придется с этим иметь дело. И при этом мир накрывает та волна, о которой я уже говорил, волна совершенно новой высокотехнологичной преступности.

Возникают новые формы преступности, а правоохранительная система, банковская система и общество в целом еще обращены в прошлое. Это проявляется во всем — в подготовке кадров, в выработке мер противодействия, в материально-техническом и кадровом обеспечении. На основании решения Совета Безопасности за последние три года МВД с огромным трудом на треть увеличило численность экспертов, которые занимаются киберпреступностью. Но этого совершенно не достаточно. На сегодняшний день эксперты загружены настолько, что расследования по киберпреступлениям длятся от одного года и дольше. Такая загруженность на 80–90% превышает установленные нормативы.

У государства никогда не будет достаточно средств для борьбы с новыми видами преступлений. Такие выводы делаются в последнем докладе Европола, опубликованном летом этого года. Европейцы прямо указывают, что государство будет вынуждено делегировать некоторые свои функции коммерческим структурам. Некоторые детективные функции, все, что касается экспертизы, защиты, предотвращения преступлений. При этом важно избежать коммерциализации правоохранительной деятельности.

Допустим, существует известное соглашение МВД с Ассоциацией российских банков 1995 г. Сейчас необходимо составить дополнительный протокол к этому соглашению, где должны быть четко регламентированы все действия банковского сообщества, скажем, по обмену информацией и созданию единого банка данных нападений, какие уже созданы в США, Китае, Великобритании. В Великобритании за него отвечают органы МВД. Может быть, возможно создание какого-то агентства, которое будет заниматься такими расследованиями и проведением экспертиз в рамках закона *О частной детективной и охранной деятельности*. Но на это нужны деньги. Банковское сообщество должно решить этот вопрос, потому что возлагать эти обязанности только на экспертные подразделения МВД и ФСБ нереально в условиях дефицита денег и той военно-политической ситуации, в которой мы находимся, и, думаю, что еще целый ряд лет будем находиться.

И, конечно, нужно укреплять международное сотрудничество. Я хотел бы немного поправить Илью Сачкова: ведется большая работа по международному сотрудничеству в рамках Интерпола. В этом году в Сингапуре был создан центр по борьбе с киберпреступностью, его открывали совместно Интерпол и Европол. Россия активно в этом участвует, идет обмен информацией в рамках Интерпола. Само участие в организации предполагает, что обмен оперативными данными должен происходить в режиме реального времени, без сложных согласований. Поэтому нужно расширять центральное бюро Интерпола в России, ведь там тоже произошло сокращение — вы знаете, недавно все структуры МВД были сокращены на 10–15%. Сейчас мы сталкиваемся с парадоксом, когда полиция сокращается, а объемы борьбы и с традиционной, и нетрадиционной, новой преступностью все время возрастают. Из такого положения надо выходить. Первый

путь — прекратить сокращения. Второй — делегировать часть функций коммерческим структурам.

АЛЕКСЕЙ КУДРИН: Но ведь в тех странах, которые вы ставите в пример, численность полиции на сто тысяч жителей значительно меньше, чем у нас.

ВЛАДИМИР ОВЧИНСКИЙ: Даже при имеющемся уровне учета преступлений число убийств на сто тысяч жителей в России где-то в 6–8 раз превосходит этот показатель в средней европейской стране. И тенденций к снижению не видно. Поэтому сокращать полицию никак нельзя.

АЛЕКСЕЙ КУДРИН: Какие структуры государственной власти занимаются этой проблемой концептуально?

ВЛАДИМИР ОВЧИНСКИЙ: При Совете Безопасности есть комиссия по информационной безопасности, и распоряжения об увеличении количества экспертов, приобретении новых аппаратных комплексов для экспертиз, получении новой техники для наших оперативных подразделений были приняты как раз на основе последних решений Совбеза.

АЛЕКСЕЙ КУДРИН: Спасибо. Слово Елене Лариной.

ЕЛЕНА ЛАРИНА: Хочу кратко обратиться к зарубежному опыту взаимодействия между государством (в данном случае полицией), обществом и бизнесом. Начну с опыта США. Как здесь уже правильно отмечали, их цифровое настоящее — это наше ближайшее будущее, поэтому, изучив то, что у них происходит сегодня, мы можем почерпнуть полезный опыт и в некоторых местах подстраховаться, чтобы избежать в будущем повторения их ошибок.

Сейчас в Америке и других технологически продвинутых странах практически нет различия между виртуальностью и реальностью. В наш обиход пришли такие термины, как *интернет вещей*, *интернет людей*, уже сейчас появились *интернет игрушек*, *интернет денег* и такой всеобъемлющий термин, как *интернет всего*. Это значит, что в самом ближайшем будущем практически все будет подключено к интернету, включая устройства и предметы, которые человек носит с собой и на себе. Возникнет единая цифровая среда.

Кроме того, существует проблема разрыва поколений. Современная молодежь с младенчества умеет обращаться с новыми технологиями, у них есть знания и опыт, который наращивается буквально с каждым днем. Людям старшего поколения, которые осваивали компьютеры уже в зрелом возрасте, сложнее адаптироваться в этом быстро меняющемся мире.

К чему все это ведет? По данным полиции крупных американских городов, раскрываемость компьютерных преступлений в настоящий момент в пять-шесть раз ниже, чем традиционных преступлений. Если при традиционных видах преступлений потерпевшие обращаются в органы правопорядка в 80–90% случаев, то при компьютерных преступлениях обращаются где-то в 15–20% случаев. Соответственно, пока показатели раскрываемости низкие, для киберпреступника соотношение потенциальной выгоды от преступления и риска быть пойманным и наказанным значительно меньше, чем при традиционной преступности. Скажу боль-

ше: мы все еще делим преступность на компьютерную и традиционную, в то время как в ближайшем будущем, учитывая, что интернет подключен ко всему, практически любой преступник, за исключением самых отпетых маргиналов, будет компьютерным преступником, и почти вся противозаконная деятельность перейдет именно в эту плоскость.

В условиях такого расцвета высокотехнологичной преступности большое число западных стран изменило свою стратегию и тактику борьбы с ней и ее профилактики. С принятием в США в 2015 г. Стратегии национальной безопасности, Стратегии кибербезопасности, а также с внесением некоторых изменений в законодательство ряда штатов подход к киберпреступности в Америке изменился.

Суть изменений в следующем. Предполагается гораздо более широкое участие общества и бизнеса в борьбе с киберпреступностью. На сегодняшний день федеральным органам власти, включая ФБР, разрешено создавать различные государственно-частные партнерства (ГЧП). То есть за государством остаются системообразующие функции, а все, что менее важно, отдается на откуп бизнесу. При этом такие партнерства создаются не только с крупными корпорациями, но и с более мелкими динамично развивающимися компаниями, иногда даже со стартапами.

В нашей стране на сегодняшний день тоже заложены законодательные основы подобных процессов. Я имею в виду закон ФЗ-224 от 13 июля 2015 г. *О государственно-частном и территориально-частном партнерстве*, который вступил в силу с 1 января 2016 г. К сожалению, пока действие этого закона распространяется только на материальные активы, то есть с помощью механизма ГЧП можно строить дороги, но нельзя оказывать услуги по обеспечению безопасности.

Отдельная тема — взаимодействие государства, бизнеса и общества. В Америке, например, в отдельных штатах на смену полицейским участкам приходят выборные шерифы. В Калифорнии власти могут привлекать к борьбе с преступностью своеобразные высокотехнологичные ЧОПы. Конечно, в России этот опыт сейчас неприменим, потому что у нас нет ни законодательной базы, ни соответствующих традиций, но интересно проследить, в каком направлении развиваются страны мира.

Австралийское правительство устанавливает налоговые вычеты для компаний, которые покупают мощное сертифицированное программное обеспечение для собственной информационной безопасности. Таким образом они побуждают предприятия бороться с киберпреступлениями и предотвращать их. Кроме того, власти Австралии компенсируют частным лицам половину затрат на покупку этих защитных программ.

Очень интересен опыт Голландии. Чтобы противодействовать киберпреступности, нужны современные инструменты и мощное техническое оснащение, приходится закупать ПО и оборудование. Более десяти лет назад в Нидерландах было принято решение о создании центра по расходованию бюджетных средств всех уровней. Комиссия, которая принимает от организаций заявки на участие в тендере, должна информировать общественность о его условиях и о компаниях,

которые подали заявки на участие. Эта информация публикуется в определенной базе, доступной для любого гражданина. В ней можно найти информацию о компании, которая участвует в тендере, о ее учредителях, о том, есть ли у нее какие-то проблемы с правоохранительными и судебными органами. Более того, там даже есть раздел, где каждый гражданин страны может разместить известные ему негативные сведения о той или иной компании. Не принимаются только анонимные сообщения, кроме того, каждый несет за предоставленные данные ответственность вплоть до уголовной.

Таким образом, компании, у которых есть какие-то проблемы с правоохранительными, судебными органами или даже общественными организациями, не могут стать победителями тендера. В результате, если раньше до трети тендеров выигрывалось компаниями, так или иначе связанными с криминалом, то сейчас абсолютно во всех сферах конкурсы проводятся совершенно прозрачно, и ни одна компания, к которой есть претензии даже у гражданского общества, не получила тендер. Использовать этот опыт в России было бы очень полезно.

АЛЕКСЕЙ КУДРИН: Наш следующий докладчик — Анатолий Кучерена.

АНАТОЛИЙ КУЧЕРЕНА: Тема, которую мы затронули, периодически возникает у нас в обществе, особенно в контексте вторжений в частную жизнь. Владимир Овчинский сказал о том, что мы вынуждены будем делиться информацией или предоставлять возможность вторжения в нашу личную жизнь. Я категорически с этим не согласен, потому что считаю, что сейчас давать возможность такого вторжения нельзя, нужно понимать, кому мы даем на это право и как этой информацией могут воспользоваться те или иные структуры.

Из общения с Эдвардом Сноуденом я понял, что мы должны обучать население, проводить информационно-просветительскую работу. Необходимо помнить, что, пользуясь любыми программами или устройствами, мы в первую очередь должны думать о том, как обезопасить себя.

Универсальной технологии, которая могла бы защитить нас с вами, не существует, и вряд ли она появится в ближайшее время. При всей осторожности полностью защитить нашу информацию, нашу частную жизнь на сегодняшний день невозможно.

Существуют специалисты, которые предлагают разные виды защиты, но все омрачает недоверие к правоохранительным органам в обществе и высокий уровень коррупции. Пример тому — *вбросы* закрытой информации по уголовным делам, которые происходят в интернете. Во многих случаях это делается для того, чтобы опорочить или оскорбить человека. Создать имидж сегодня проще простого, в том числе используя новые технологии и утечки информации, хищение данных, например из смартфонов. Поэтому позаботиться о том, как себя защитить, должны мы сами.

Кроме того, необходимо проводить работу среди молодежи. Было правильно сказано, что информация, которая появляется в интернете, остается там навечно. Сегодня она никому не нужна, а завтра может быть использована против человека, чтобы оказать на него давление.

Принципиально важно, чтобы каждый сотрудник полиции был профессионально пригоден к той работе, которой он занимается. Мы понимаем и знаем имеющиеся трудности. К сожалению, надо признать, что сегодня сотрудник полиции вынужден больше 50% своего рабочего времени заниматься отчетностью, ему не хватает времени на повышение профессиональной квалификации, а это необходимо, когда речь идет о борьбе с высокотехнологичными преступлениями.

АЛЕКСЕЙ КУДРИН: Следующий докладчик — Алексей Лукацкий.

АЛЕКСЕЙ ЛУКАЦКИЙ: Хотел бы сказать несколько слов по поводу культуры информационной безопасности. Два года назад при Совете Безопасности была сформирована рабочая группа по разработке документа под названием *Основы государственной политики в области формирования культуры информационной безопасности*. В проект этого документа было включено все то, о чем сегодня упоминали. Это и введение различных образовательных дисциплин, начиная с самого раннего возраста, и обучение преподавателей и воспитателей в детских садах, школах и вузах, и просвещение в вопросах информационной безопасности и грамотности. К сожалению, финальный вариант документа пока так и не увидел свет, и те важные вещи, о которых сегодня говорили, пока не нашли отражения в основополагающем документе, которым руководствовалось бы государство.

Все это время мы говорили о традиционных преступлениях, которые совершаются с помощью высоких технологий, таких как кража денег. Это неприятно, но не смертельно. А бывают киберпреступления, которые могут привести к смерти человека, например атаки на подключенные к интернету кардиостимуляторы, инсулиновые помпы, специальное медицинское оборудование для больных астмой, автомобили, которые практически все оснащены достаточно серьезной электроникой. Прецеденты уже были.

Необходимо предпринять серьезные усилия на уровне взаимодействия различных органов исполнительной и законодательной власти для того, чтобы при выпуске такой продукции на рынок она оценивалась не только с точки зрения медицинской или промышленной безопасности, но и с точки зрения безопасности информационной. Внимание этому сегодня не уделяется по вполне понятным причинам — это совершенно новые угрозы, с ними мало кто сталкивался, поэтому никто не закладывает их в будущие модели угроз и существующие нормативные документы. Через несколько лет эти технологии прочно войдут в нашу жизнь, и если сейчас, скажем, сантехника или бытовая техника, подключенная к интернету, — нечто из области фантастики, то в будущем все будет гораздо серьезнее, и если сейчас к этому не готовиться, то через несколько лет СМИ могут начать сообщать о киберпреступлениях, повлекших человеческие смерти или нанесение вреда здоровью людей.

АЛЕКСЕЙ КУДРИН: Слово Михаилу Якушеву.

МИХАИЛ ЯКУШЕВ: То, что я сейчас скажу, я говорю регулярно уже многие годы: ситуация медленно меняется к лучшему, но, к сожалению, преступность нас все равно обгоняет. Значит, проблема комплексная и отношение к ней должно быть именно комплексное. Мне не совсем понятно, почему тут упоминаются только МВД и полиция, как раз там медленно, но стабильно происходят изменения

к лучшему, в то время как в других правоохранительных органах проблема борьбы с киберпреступностью фактически не решается никак. Поэтому, если мы говорим об улучшении работы правоохранительных органов, то нельзя ограничиваться только МВД или Федеральной службой безопасности, где есть специалисты, адекватно понимающие ситуацию, — нужно брать шире.

Что касается законодательства, решение правовых вопросов очень важно — это первый компонент комплексного подхода к проблеме. На экспертном уровне вопросы, связанные с разработкой законодательства, не поднимаются, то есть опыт тех же Сачкова и Касперского, как мы видим, не сильно используется. В связи с этим, когда речь шла о международном опыте, упоминалась Будапештская конвенция. Госорганы поддерживают неучастие в ней России, эксперты занимают противоположную позицию. Действительно, Россия в этом плане изолирована, Интерпол, к сожалению, не способен решить все проблемы, и поэтому ситуация не исправляется. На международном уровне действительно нужно ставить вопросы о конкретных инициативах, о решении конкретных проблем, а не просто говорить о доминировании одной организации или одной страны.

Второй компонент проблемы — технологический. Почему-то считается, что чем больше запретить в интернете на уровне провайдеров, тем меньше будет проблем. На самом деле доказано, что чем ближе к устройству пользователя происходит фильтрация, тем эффективнее результат. В качестве примера можно привести так называемый *родительский контроль*. Возникает вопрос: где проекты продвижения программных, аппаратных средств, которые позволили бы такой контроль осуществлять? Что-то делают на коммерческой основе операторы мобильной связи или *Лаборатория Касперского*, но это организации коммерческие, их интересует уровень продаж. В то же время государство и общественность хотят, чтобы программные продукты были недорогими, но в то же время известными и надежными.

Третий момент — образовательный, про который тоже много говорили. В этом плане не происходит практически ничего. Давайте себе представим, что в детских садах и школах на вопрос ребенка, что там на улице горит красным и зеленым цветом, ему отвечали бы: «не обращай внимания, тебе нужно перейти дорогу — переходи». Нет, ему объясняют, что означают красный, желтый и зеленый цвета и так далее, это вкладывается человеку в голову *с младых ногтей*.

Последнее, о чем, как я понимаю, пока еще не говорили, — это проблема доверия. Доверия друг к другу и к правоохранительным органам. Это опять-таки часть общей, комплексной проблемы. Существует значительная разница между тем, что такое законность, эффективность и качество с точки зрения гражданина и с точки зрения того, от кого требуют отчетов по показателям раскрываемости, законности и эффективности. Или мы, как коллеги из ФСКН, считаем главной задачей закрыть как можно больше сайтов и тем самым лишить себя возможности поиска людей, которые занимаются торговлей наркотиками, или наша цель — поймать и наказать этих преступников. Еще один аспект в плане повышения доверия — так называемый *пиар*. Нужно рассказывать о конкретных случаях, когда благодаря деятельности правоохранительных органов, российских и зарубежных экспертов выявленные банды привлечены к ответственности, а те, кто занимались педо-

филией или продажей наркотиков, — наказаны. К сожалению, чаще можно услышать об обратных примерах.

Поэтому давайте друг другу доверять. Прозвучали правильные слова про государственно-частное партнерство: бизнес наш патриотичен, население обладает достаточно хорошими знаниями и гражданской позицией, и нужно работать сообща.

АЛЕКСЕЙ КУДРИН: Выступающие более-менее обрисовали состояние дел на сегодня. Но что нас ждет через 15–20 лет? Хотел бы попросить Алексея Яцыну, модератора проекта *Форсайт-флот,* кратко высказаться об этом.

АЛЕКСЕЙ ЯЦЫНА: *Форсайт-флот* этого года, как известно, был посвящен Национальной технологической инициативе, мы стояли у истоков ее проработки, сейчас это официальная государственная программа.

Надо понимать, что уже в следующем году на дороги общего пользования Российской Федерации выйдет первый беспилотный *КАМАЗ*. Это означает, что пройдет пять, семь, десять лет, и беспилотный транспорт будет ездить по нашим дорогам. Не в Америке, не в Англии — у нас. Это означает, что уже сегодня надо формировать дорожно-транспортное законодательство, рассчитанное на беспилотный транспорт. Кто будет виноват, если беспилотник собьет человека? Это к вопросу техноэтики ближайшего будущего, о чем пока думают мало, а думать пора. Завтра в воздух поднимутся тысячи, десятки тысяч дронов. Сегодня маленький дрон с фотовидеокамерой является самым популярным подарком ребенку на Новый год, он стоит уже две-три тысячи рублей, послезавтра эти устройства будут выполнять десятки, а то и тысячи задач. Каким образом они будут помогать полиции обеспечивать безопасность? Готовы ли полицейские работать по профессиональным стандартам не участкового, который обходит дома, а участкового-программиста, способного запрограммировать дронов на облет территории, контроль и вызов оперативной группы?

Был приведен пример того, что людей, имеющих достаточную квалификацию для анализа киберпреступности, крайне мало. В то же время в Лондоне в рамках чемпионата World Skills, где соревнуются представители различных профессий, криминалистика — одна из дисциплин. То есть туда приезжают не только сварщики, штукатуры, ландшафтные дизайнеры, CAD-инженеры, специалисты по 3D-моделированию, но и криминалисты. Известно, что в нашей стране развивается кружковое движение, мне кажется, что МВД и другие органы безопасности должны подключаться к этому процессу со своими задачами, и тогда сегодняшние 12–15-летние дети вырастут и захотят работать в области обеспечения безопасности и решать задачи, в том числе связанные с борьбой с киберпреступностью. Сегодня граждане иногда могут самостоятельно провести расследование быстрее, лучше, эффективнее, чем МВД. Наши граждане готовы в этом смысле сотрудничать с органами правопорядка. Запрос на безопасность есть, и он будет расти.

И последнее. Я уже говорил про снятие законодательных барьеров. Самый яркий пример — это технология блокчейн. Она связана с контролем и криптозащитой транзакций. На днях Герман Греф говорил в своем выступлении, что снимать

законодательные ограничения на блокчейн надо было год назад. В этом плане Российская Федерация отстает, а, значит, наши финансовые институты не имеют доступа к самым современным способам защиты.

Основные предложения, которые у меня сформировались, пока я слушал уважаемых докладчиков: снятие барьеров, формирование перспективного законодательства, проведение конкурсов для младшего поколения. Я считаю, что органы безопасности должны входить в группу *Национальная технологическая инициатива*, туда должны входить разнообразные кружки, и они должны вырабатывать совместную повестку дня.