КИБЕРБЕЗОПАСНОСТЬ: УГРОЗЫ, ВЫЗОВЫ, РЕШЕНИЯ

***Згоба Артём Игоревич**, г. Москва,*
***Маркелов Дмитрий Витальевич**, г. Санкт-Петербург,*
***Смирнов Павел Игоревич**, кандидат технических наук, г. Санкт-Петербург*

Надежная и защищенная работа сетей передачи данных, компьютерных систем и мобильных устройств является важнейшим условием для функционирования государства и поддержания экономической стабильности общества. На безопасность работы ключевых информационных систем общего пользования оказывают влияние многие факторы: кибер–атаки, нарушения, вызванные физическим воздействием, выход из строя программного и аппаратного обеспечения, человеческие ошибки. Перечисленные явления наглядно демонстрируют, насколько современное общество зависит от стабильности работы информационных систем.

***Ключевые слова**. Сети, кибербезопасность, защита информации, угрозы.*

CYBERSECURITY. THREATS, CALLS, SOLUTIONS

***Zgoba Artem**, Moscow,*
***Dmitry Markelov**, St. Petersburg,*
***Pavel Smirnov**, PhD., St. Petersburg*

Reliable and secure operation of data networks, computer systems and mobile devices is the most im–portant condition for the functioning of the state and for maintaining economic stability. The safe operation of key information systems in common use is influenced by many factors: cyber attacks, disorders caused by physical impact, failure of hardware and software, humane mistakes. These events demonstrate how mod–ern society depends on stability of information systems.

***Keywords**. Network, cyber security, information security, threats.Network, cyber security, information security, threats.*

Введение

Целью исследования данной проблемы стала актуальность вопроса в современном мире, где защита информации в кибер-пространстве стоит крайне остро.

Кибербезопасность все чаще рассматривается, как стратегическая проблема государства, комплексно затрагивающая экономику страны, в том числе взаимодействие национальных разработчиков программного обеспечения и систем управления, производителей оборудования и компонентов для обеспечения ИКТ-инфраструктуры, низкая рыночная конкурентоспособность которых приводит к необходимости использования решения иностранных производителей. На практике данное явление приводит к стремительному росту зависимости от иностранных производителей и снижению уровня информационной защиты в виду вынужденного использования «закрытого» программного и аппаратного обеспечения во всех сегментах инфраструктуры как для специальных государственных ведомств, так и гражданского сектора.

Уже в ближайшее время зависимость от иностранных производителей оборудования и разработчиков программного обеспечения может достигнуть критического уровня. Например, несмотря на созданный виртуальный «железный занавес», власти Китая фактически признали полную зависимость и незащищенность вследствие повсеместного использования программной платформы для мобильных устройств Android (доля платформы на рынке Китая по итогам 2012 года – 86,4%), основанную на «открытом» коде, но подконтрольную специальным службам США. С точки зрения экономики данное явление оказывает положительное влияние на развитие электронной промышленности и реального сектора, использующих «открытое» программное обеспечение для производства мобильных устройств, но при этом создаёт реальную угрозу для национальной безопасности, переводя её под контроль иностранных спец. служб.

Для того чтобы национальная кибербезопасность могла соответствовать уровню ведущих экономических держав, необходимы, в том числе,

последовательные действия со стороны государства, направленные на повышение эффективности и развитие системы взаимодействия участников ИКТ-отрасли.

В свою очередь предприятия разработчики и производители должны уделять особое внимание вопросам информационной безопасности в разрабатываемой/выпускаемой продукции, предъявляя повышенные требования к надёжности и защищенности предлагаемых решений, и только в крайних случаях и при необходимости повышения рыночной ориентированности отдельных продуктов должны использовать решения иностранных вендоров и разработчиков программного обеспечения.

Рассмотрим существующие угрозы для кибербезопасности России с учетом актуальных тенденций развития ИКТ-отрасли в мире.

Технологические и системные проблемы кибербезопаности

Понятие кибербезопасности включает в себя множество проблем различного типа, а также содержит еще большее число решений.

Кибербезопасность является областью активных исследований и разработок в сообществе информационных технологий силами участников со всех частей экосистемы ИКТ. Схематично понятие «кибербезопасность» представлено на рисунке 1.

Многие направления кибербезопасности имеют общую тематику и проблемы, которые требуют комплексного подхода.

На рисунке 2 кратко выделены некоторые из областей основных проблем кибербезопасности, а также показано, где некоторые из указанных проблем удается решать с помощью технических решений, разработанных коммерческими организациями, организациями по стандартизации и пользователями Интернета.

В подавляющем большинстве случаев наиболее успешные атаки хакеров, преступников и других злоумышленников направляются на серверы и компьютеры конечных пользователей, подключенные к Интернету. Среди инструментов, которые используются для атаки компьютеров, – вредоносное ПО, троянские кони, бот-сети, фишинг, распределенные атаки типа «отказ в обслуживании» (DDoS), а также атаки «человек посередине».

Рис. 1. *Темы и направления кибербезопасности*

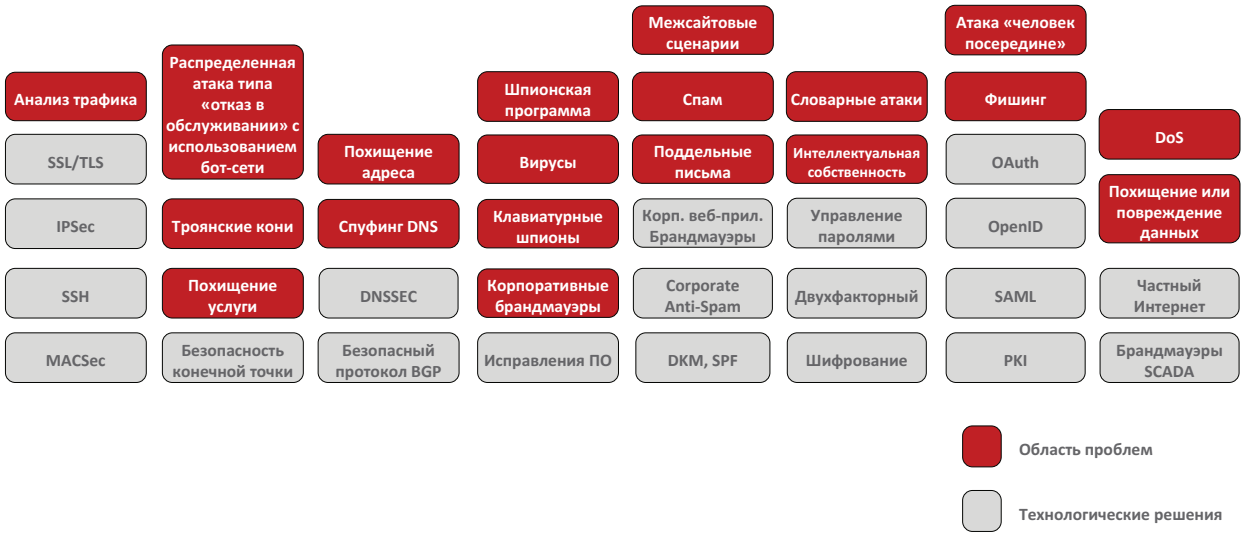

Рис. 2. *Проблемы кибербезопасности и технологические решения*

Таблица 1

Пример специализаций мировых компаний в сфере информационной безопасности.

Организация	Область интересов
Компании-разработчики ПО, такие как Eset, F-Secure, Kaspersky, McAfee, Sophos, Symantec и Trend Micro	Производство программ для борьбы с вредоносным ПО для использования на серверах, пользовательских настольных компьютерах и ноутбуках, а также во встроенных устройствах, таких как брандмауэры
Компании-разработчики брандмауэров, такие как Check Point Software, Cisco Systems, Juniper Networks и SonicWALL	Производство сетевых устройств, брандмауэров для защиты организационных сетей путем разграничения доступа к сети и Интернету
Компании-разработчики оборудования, такие как AMD и Intel	Производство компьютеров со встроенными средствами безопасности (например, с дисками с автоматическим шифрованием доверенными платформенными модулями) для защиты от внешнего вмешательства
Trusted Computing Group (отраслевой консорциум)	Разработка стандартов для защиты устройств конечных систем, таких как жесткие диски с автоматическим шифрованием, устройства аппаратной проверки подлинности, а также системы контроля сетевого доступа
IETF	Разработка стандартов для оценки сетевых конечных точек, которые проверяют безопасность устройств, прежде чем им будет разрешено подключаться к сетям и Интернету

Обеспечение безопасности компьютеров, будь то серверов, настольных компьютеров, ноутбуков или смартфонов, является целью работы самых различных групп внутри ИТ- и Интернет-сообществ. Таблица 1 поможет определить некоторых крупных игроков, а также области их интересов.

Важно отметить, что подавляющее количество компаний, представленных в таблице – иностранные разработчики и производители, в большинстве своём доминирующие на российском рынке.

Тем не менее, даже нахождение технологического решения для проблемы кибербезопасности не означает, что сама проблема исчезает – просто появляется возможность ее решения. Например, комплексное шифрование с использованием алгоритмов SSL/TLS является широко известной технологией, которую можно использовать в качестве решения многих проблем, перечисленных выше. Однако оно не было принято повсеместно. Частично это обусловлено историческими причинами и организационной инертностью, а также неграмотностью или плохой информированностью. Наличие хорошо известных решений хорошо известных проблем имеет небольшую ценность, если эти решения не используются.

Таким образом, вопросы обеспечения национальной кибербезопасности зависят не только от технических способов реализации, но, что более важно, от наличия и реального спроса на данные решения.

Генеральный директор ОАО «Воентелеком» А. Е. Давыдов отмечает, что если задача обеспечения информационной безопасности при передаче по сетям и каналам связи может быть решена преимущественно применением средств криптографической защиты информации отечественного производства, то обеспечение безопасности связи от разрушающих воздействий является проблемой, так как в виду отсутствия собственной инфраструктуры «Воентелеком» вынужден заказывать необходимые услуги у коммерческих операторов связи, сети которых развернуты на импортном оборудовании. Это касается и фиксированной, и мобильной, и спутниковой компонент. Фактически вся единая сеть электросвязи России находится в жесточайшей технологической зави-

симости и по этой причине не может служить доверенной средой и надежной основой для системы управления войсками, так как в любой момент может контролироваться и управляться вероятным противником.

Таким образом, по мнению А. Е. Давыдова, полноценно и гарантированно решать вопросы безопасности связи можно только тогда, когда в стране на сетях будет использоваться российское телекоммуникационное оборудование, а еще лучше – будет создана единая выделенная сеть на его основе в интересах государственного управления.

Обеспечение кибербезопасности с точки зрения инженерного владения инфраструктурой

Правительства многих стран в своих программах развития кибербезопасности уделяют особое внимание инфраструктуре, тесно связанной с вопросами безопасности. Для оценки масштаба проблемы кибербезопасности и возможных угроз важно понимать взаимосвязь между кибербезопасностью, важнейшей инфраструктурой (CI), важнейшей информационной инфраструктурой (CII), защитой важнейшей информационной инфраструктуры (CIIP) и инфраструктурой, не относящейся к важнейшей. Эта взаимосвязь представлена на рисунке 3.

Хотя определения могут незначительно отличаться, важнейшими инфраструктурами (CI), как правило, считаются ключевые системы, услуги и функции, неисправность или разрушение которых оказывает пагубное влияние на систему общественного здравоохранения и безопасности, коммерческую деятельность и национальную безопасность или на их сочетание. CI состоят как из материальных (например, зданий и сооружений), так и виртуальных элементов (например, систем и данных). Каждая страна может иметь свое понимание термина «важнейший», однако обычно это понятие может включать в себя элементы информационно-коммуникационных технологий (ИКТ) (включая электросвязь, энергетику, банковское дело, транспорт, общественное здравоохранение, сельское хозяйство и продовольствие, водоснабжение, химическую промышленность, судоходство, а также важнейшие государственные службы).

Каждый из этих секторов экономики имеет свои собственные материальные ресурсы, например здания банков, электростанции, поезда, больницы и правительственные офисы. Вместе с тем, все эти важнейшие секторы национальной экономики зависят от информационно-коммуникационных технологий.

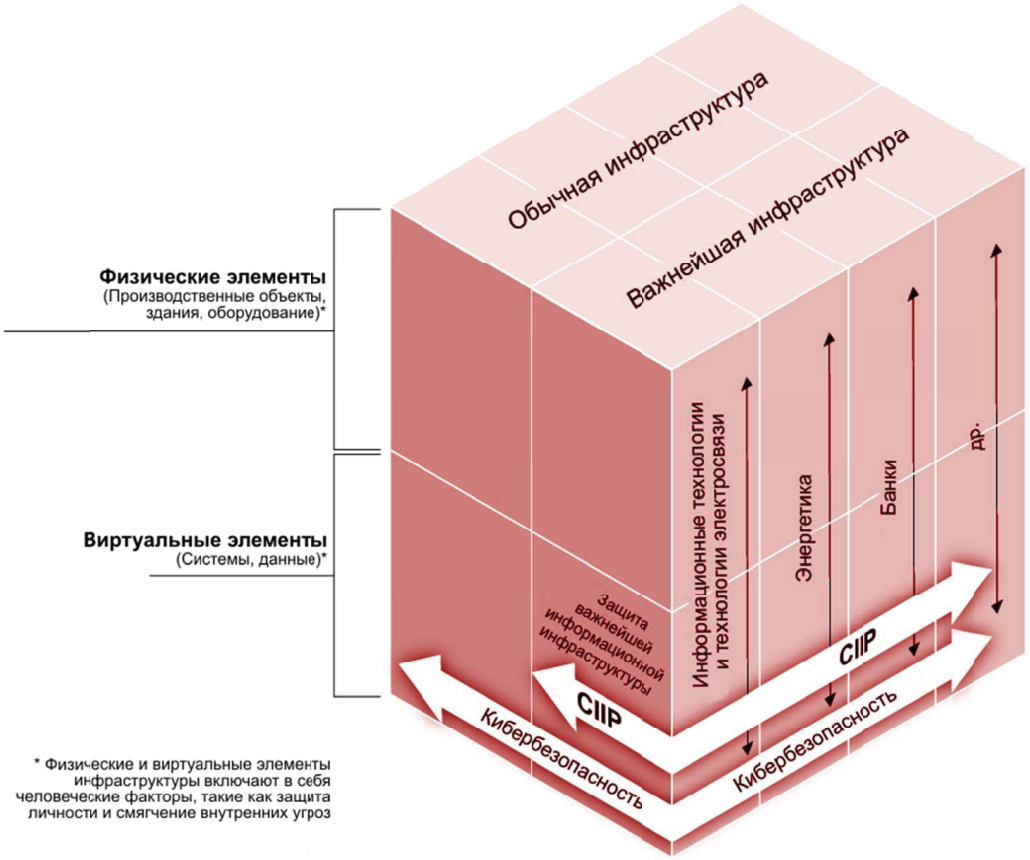

Рис. 3. *Связь между кибербезопасностью и защитой важнейшей информационной инфраструктуры*

Ключевая проблема для России состоит в том, что крупнейшие потребители такой продукции не могут отказаться от продуктов зарубежных вендоров в пользу отечественных решений. При этом большинство государственных ведомств, имея собственные сети и осуществляя ежегодные затраты на НИОКР (в том числе на разработку телекоммуникационного оборудования и средств защиты информации), приобретают импортные решения. Именно благодаря таким тенденциям, по мнению экспертов, для иностранных производителей в России помимо гражданского открывается дополнительный рынок – рынок специального и государственного назначения. В качестве альтернативного решения проблемы может служить создание единой сети с логическим разделением ресурсов.

На каждом из участков ИКТ-инфраструктуры используются решения иностранных производителей с «неизвестной» начинкой. Проверки и анализ свойств данных решений не гарантируют безопасность их использования при наступлении определенных условий.

В настоящий момент сложилась критическая ситуация, при которой на каждом из участков инфокоммуникационной инфраструктуры (чипы, схемотехника, электронные компоненты, транспорт и передача данных, системы управления, программное обеспечение от библиотек до отдельных продуктов, и т.п.) с высокой долей вероятности используются зарубежные решения с «неизвестной» начинкой. Даже после проведения специальных мероприятий для проверки и анализа потенциально-опасных свойств используемых решений, у нас нет оснований полагать, что данные свойства гарантированно не смогут проявиться при определенном наборе условий в дальнейшем.

Проблема инженерного владения на базе решений иностранных вендоров носит системный характер, как с точки зрения обеспечения кибербезопасности, так и с точки зрения текущего состояния российской электронной промышленности.

Разработка и производство электроники как процесс, а также использование электроники на внутренних и внешних рынках (в том числе, на рынке спец.заказчиков) как результат, недостаточно эффективны, что является комплексной проблемой всей отрасли. В России действительно много успешных разработчиков, а на многих предприятиях сохранилась школа по НИОКР. Наряду с компаниями, которые преуспели в разработке, но не продвигают свои продукты на рынок, есть компании, которые разрабатывают и продвигают свои вполне успешные продукты, но взаимодействуют при этом только с зарубежными чип-вендорами. Почему так происходит?

При создании конкурентоспособного продукта основными являются бизнес-задачи, при этом за скобками остается вопрос развития электроники на уровне отрасли. Таким образом, бизнес отказывается от применения дорогого и неконкурентоспособного чипа российского производства, так как использование такого «сырого» чипа несёт в себе огромные риски для бизнеса. Поэтому для создания потребительской электроники, как правило, на этапе технического проектирования выбирают импортные чипы.

Проблема отсутствия взаимодействия российских чип-вендоров и российских разработчиков электроники является системной. С одной стороны, барьеры выстраиваются разработчиками электроники — даже если чип-дизайнеры разработали хорошую микросхему, то ее применение блокируется их коллегами — инженерами-разработчиками электроники — под любым формальным предлогом. С другой стороны, барьеры создаются разработчиками микросхем, которые недостаточно ориентированы на рынок. Зачастую они создают микросхемы только для отчетности по ОКР, на их базе невозможно сделать конкурентоспособный продукт.

Сегодня сложилась ситуация, когда занимаясь ОКР по созданию продукта, гарантирующего соблюдение требований обеспечения кибербезопасности, невозможно получить результат, взаимодействуя только с российскими предприятиями.

В качестве решения может быть выбрана популярная в мире **аутсорсинговая модель производства**, согласно которой разработка и вывод на рынок востребованных продуктов возможны только при условии тесной кооперации с зарубежными и отечественными компаниями. Это позволяет на этапе проектирования сформировать концепцию нового продукта, предъявляя ему востребованные рынком современные требования и передать сторонним специализированным производителям виды работ, не являющиеся профильными для предприятия. Например, такие виды работ, как организация схемотехники устройства, производство

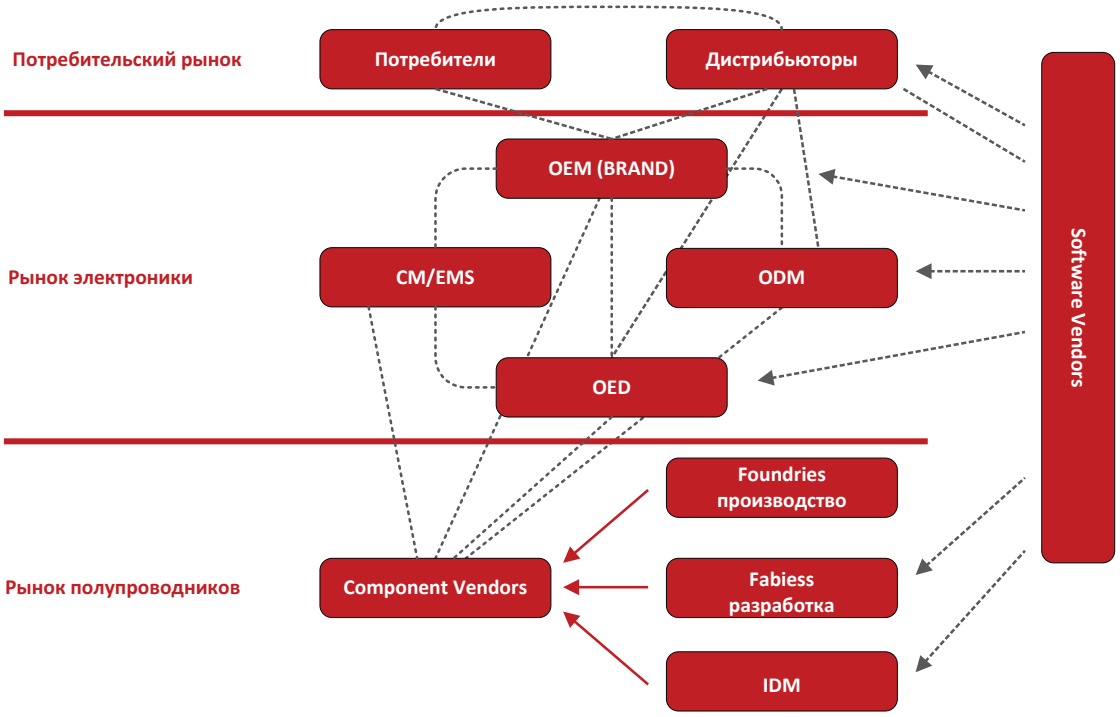

***Рис. 4**. Уровни взаимодействия участников кооперации*

электронных компонентов, промышленное серийное производство устройств, техническая поддержка и дистрибьюция могут быть переданы специализированным предприятиям отрасли. Данная модель позволяет с максимальной экономической эффективностью обеспечить разработку и вывод на рынок решений согласно мировым стандартам производства в условиях ограниченного по времени цикла производства.

Если рассматривать бизнес-модель взаимодействия через аутсорсинговую модель, то можно выделить три основных уровня:

1. Рынок полупроводников, создание компонентной базы, процессоров и СнК.

2. Рынок электроники, разработка и производство электроники.

3. Потребительский рынок, дистрибьюторы.

Приведенная схема формирует общее понимание того, как сейчас происходит разделение рынков по уровням, и как выстраивается схема кооперации в мировой практике при создании продуктов в сфере электроники.

Сужая область деятельности, компании все больше концентрируются на их приоритетных направлениях и получают в них технологические преимущества, позволяющие значительно увеличить долю в выбранном сегменте рынка. Разделение на уровни обусловлено рядом экономических факторов и быстро растущей технологической сложностью каждой отдельной области. Получается, что зачастую сосредоточить определенные компетенции в рамках одного предприятия целесообразнее, чем выстраивать вертикально интегрированную компанию, отвечающую за полный цикл. Такое разграничение зон ответственности позволяет обеспечить экономический эффект от разработки новых продуктов и цикличность производства в условиях постоянно меняющегося рынка, позволяет отрасли электроники развиваться динамично, но при этом каждое из предприятий находится в зависимости от других участников кооперации.

Для развития отечественного производства сертифицированной высокотехнологичной продукции радиоэлектроники и программного обеспечения мирового уровня для рынка специальных заказчиков необходимо внедрение аутсорсинговой модели в систему взаимодействия отечественных производителей и разработчиков внутри отрасли.

Таким образом, системный подход к вопросам кибербезопасности на уровне государства включает в себя не только повышение осведомленности относительно существования рисков в киберпространстве, создание национальных структур, занимающихся вопросами кибербезопасности, но и установление необходимых взаимоотношений

между различными группами участников, в том числе между отраслями экономики, для развития аутсорсинговой модели производства. Комплексная программа по обеспечению кибербезопасности, подкрепленная системным планированием НИОКР, с одной стороны, поможет защитить экономику страны от сбоев, способствуя планированию непрерывности бизнеса в различных секторах и защищая информацию, хранящуюся в информационных системах, и, с другой стороны, поможет стимулировать производство и сбыт для отечественных инфокоммуникационных предприятий, снижая тем самым зависимость страны от иностранных производителей и разработчиков и поставляя на гражданский и специальный рынки полностью безопасные и современные решения мирового уровня.

Мобильная платформа Android как крупнейшая скрытая угроза для кибербезопасности страны

Проблемы кибербезопасности носят комплексный характер и не ограничиваются исключительным инженерным владением. Ситуацию усугубляет использование программного обеспечения (на уровне программного кода и библиотек), операционных системы и систем управления иностранного производства, которое в большинстве своем является «закрытым». Одним из примеров скрытой угрозы для кибербезопасности является повсеместное использование мобильных устройств иностранных производителей, полностью определяющих развитие данного сегмента рынка в России. Китайские власти уже усмотрели национальную угрозу в платформе Android. Свои выводы власти КНР обосновывают итогами исследования Китайской академии телекоммуникационных исследований (China Academy of Telecommunications Research), проведенного по заказу Министерства промышленности и информатизации. По их данным, рыночная доля платформ iOS, Windows Phone, Tizen и Firefox OS, даже в суммарном порядке существенно уступают на китайском рынке платформе Android. Если в 2009 году на долю Android приходилось порядка 0,6% устройств, то ко второму полугодию прошлого 2012 года этот показатель возрос до шокирующих 86,4% китайского мобильного рынка.

В настоящий момент злоумышленники практически полностью сконцентрировались на создании и распространении зловредов для операционной системы Android. 2012 год охарактеризовался взрывным ростом числа вредоносных программ для ОС Android: если за весь 2011 год было обнаружено почти 5300 новых вредоносных программ для всех мобильных платформ, то в некоторые месяцы 2012 года число обнаруживаемых Android-зловредов превысило это число. В таблице №2 представлено общее количество модификаций и семейств мобильных вредоносных программ по данным «Лаборатории Касперского» по состоянию на 1 января 2013 года:

Таблица 2

Общее количество модификаций и семейств мобильных вредоносных программ по данным «Лаборатории Касперского»

Платформа	Модификации	Семейства
Android	43600	255
J2ME	2257	64
Symbian	445	113
Windows Mobile	85	27
Другие	28	10
Всего	**46415**	**469**

Если в конце 2011 года на долю Android приходилось порядка 65% всех мобильных вредоносных программ, то к концу 2012 года доля Android-зловредов практически достигла 94% (рисунок 5). При этом 99% всех обнаруженных в течение 2012 года мобильных зловредов нацелены на Android-устройства.

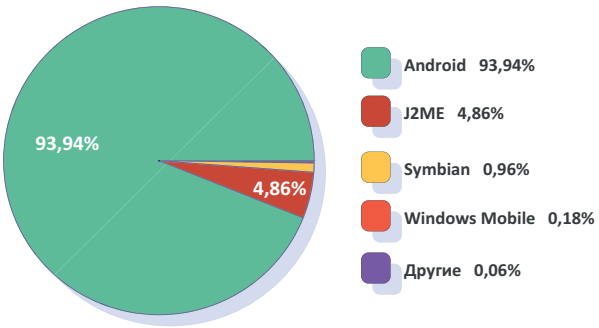

Рис. 5. *Распределение вредоносных программ для мобильных устройств по платформам за период с 2004 по 2012 год*

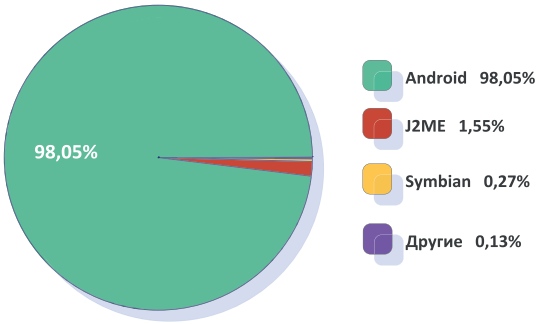

Рис. 6. *Распределение мобильных вредоносных программ по платформам за период с 2004 по 2013 год*

За прошедший 2013 год положение для пользователей мобильных устройств на базе Android только ухудшилось (Рисунок 6).

Таким образом, в настоящее время ОС Android стала самой распространенной операционной системой для мобильных устройств, и это сделало ее основной мишенью для создателей вирусов.

Однако главная и наиболее актуальная для России претензия к данной операционной системе заключается в обманчивом утверждении открытости и доступности платформы. Несмотря на бесплатность и открытость исходного кода, корпорация Google целиком и полностью контролирует все разработки на базе Android. В свою очередь, по данным Wall Street Journal, Федеральное бюро расследований (ФБР) США использует хакерские инструменты для слежки за людьми, пользующимися современными средствами связи, в том числе на базе ОС Android. Речь идет о скрытой установке троянов и другого шпионского программного обеспечения на мобильные устройства и персональные компьютеры посредством вредоносных веб-ссылок и поддельных писем электронной почты – методов, широко применяемых хакерским сообществом.

При этом по данным издания, ФБР располагает технологиями, которые позволяют удаленно включать микрофон на смартфонах и планшетах под управлением операционной системы Android, а также на ноутбуках, и вести запись. Фактически, это превращает в «жучок» устройство, которое пользователи всегда имеют при себе и пользуются повседневно. Как правило, подобные методы ФБР использует для слежки за группами организованной преступности и борьбы с терроризмом, но это не исключает возможность их использования в иностранной разведке.

Таким образом, рассматривая актуальные проблемы кибербезопасности, с которым сталкиваются граждане России каждый день, становится очевидной опасность использования операционной системы Android (а также других мобильных платформ иностранных производителей) с точки зрения обеспечения информационной безопасности. Отсутствие конкурентоспособных отечественных решений на рынке вынуждает использовать импортные аналоги оборудования и программного обеспечения, что ещё раз подчеркивает необходимость комплексного подхода к организации процессов НИОКР, производства электронных изделий и каналов сбыта инфокоммуникационных решений внутри страны.

Таким образом, в настоящий момент инфокоммуникационная инфраструктура России находится в сильнейшей зависимости от иностранных производителей и разработчиков, активно внедряя их решения (от библиотек программного обеспечения до аппаратных платформ и систем управления).

Примером такой зависимости и вытекающих из неё угроз может служить повсеместное использования мобильных устройств на базе операционной системы Android, подконтрольную спец. службам США.

Дальнейшее обеспечение кибербезопасности России напрямую зависит от уровня взаимодействия заинтересованных участников: государство, научно-исследовательские институты, разработчики и производители инфокоммуникационных решений, заказчики и потребители.

В качестве возможного решения предлагается организовать ряд системных НИОКР среди компетентных предприятий, объединенных общими целями и ответственных за вывод на рынок востребованных продуктов мирового уровня. Данная модель позволит государству, с одной стороны, на федеральном уровне формировать защищенную инфраструктуру кибербезопасности, а с другой стороны, обеспечить развитие экономики благодаря увеличению числа рабочих мест и объема производства отечественных инфокоммуникационных решений с высокой добавленной стоимостью.

Литература:

1. Internet Society – общемировая общественная организация под управлением широкого попечительского совета [Электронный ресурс]. http://www.internetsociety.org/sites/default/files/bp-deconstructing-cybersecurity-16nov-update.doc.doc_RU_121712.pdf «Взгляды на кибербезопасность: 2012г.»
2. CNews – [электронный ресурс]. http://www.cnews.ru/top/2013/03/13/android_zahvatil_kitay_vlasti_byut_trevogu_522278 – «Android захватил Китай. Власти бьют тревогу»
3. CNews|безопасность – [электронный ресурс] Сергей Попсулин – http://safe.cnews.ru/news/top/index.shtml?2013/08/02/537614&utm_source=twitterfeed&utm_medium=twitter «ФБР способна удаленно включать микрофоны в смартфонах Android»
4. Гарнаева М.А., Функ К. Kaspersky security bulletin 2013 // Вопросы кибербезопасности. 2014. №3. С.65-68

References:

1. Internet Society is a global cause-driven organization governed by a diverseBoard of Trustees. http://www.internetsociety.org/sites/default/files/bp-deconstructing-cybersecurity-16nov-update.doc.doc_RU_121712.pdf – article on the Internet «Views on cybersecurity: 2012.»
2. CNews – [electronic resource]. http://www.cnews.ru/top/2013/03/13/android_zahvatil_kitay_vlasti_byut_trevogu_522278 – article on the Internet «Android has conquered China. Authorities are sounding the alarm»
3. CNews|security [electronic resource] Sergey Popsulin – http://safe.cnews.ru/news/top/index.shtml?2013/08/02/537614&utm_source=twitterfeed&utm_medium=twitter – article on the Internet «the FBI is able to remotely activate the microphones in Android smartphones»
4. Securelist – [electronic resource] / Maria Garnaeva, Christian Funk /December 11, 2013/ http://www.securelist.com/ru/analysis/208050822/Kaspersky_Security_Bulletin_2013_Osnovnaya_statistika_za_2013_god. part of the report of Kaspersky Security Bulletin 2013 – «Kaspersky Security Bulletin 2013. Key statistics for the year 2013»