ЦИФРОВАЯ КРЕПОСТЬ

Сергей РАЗУМОВСКИЙ

Вопросы кибербезопасности критически важны для наших стран.

НУЖНЫ ЛИ РОБОТУ ПРАВА?

Нет, пожалуй, больше сфер жизни, куда бы не проникли высокие технологии.

Как отмечалось на форуме, лидерами Беларуси и России поставлена четкая задача: создать единое технологическое пространство внутри Союзного государства. По этому пути, собственно, идет весь мир - унификация законов и стандартов в данной сфере. Жить в едином цифровом мире удобно, но это порождает массу проблем. В том числе правовых. Что, в частности, обсуждали эксперты.

- Какой, например, правовой статус у искусственного интеллекта или робота? - задается вопросом **российский сенатор, зампред Комитета по конституционному законодательству и государственному строительству Владимир Полетаев**. - Появляются и новые субъекты права: например, наряду с бумажными банкнотами используются электронные платежные инструменты: цифровые деньги, платформы, экосистемы.

Его поддержал белорусский коллега **Сергей Сивец, заместитель председателя Комиссии ПС по законодательству и Регламенту**:

- Цифровизация несет с собой определенные угрозы, а потому необходимо развивать нормы частного права в киберпространстве и обеспечение информационной безопасности.

Иными словами - в мире блокчейна, криптовалют и цифровых знаков часто не соблюдаются права граждан. Что уж говорить о сознательных кражах и мошенничествах: только в 2020 году ущерб от киберпреступности в России составил 69 миллиардов рублей.

- Все больше проявляется противоречий между национальным правом в цифровой сфере, ограниченным территорией государства, и распространением информации, имеющей глобальный характер, - обратил внимание Полетаев. - В связи с этим возникает проблема осуществления правового суверенитета.

Но есть проблемы и еще более серьезные.

ДОЛОЙ ИМПОРТНОЕ ОБОРУДОВАНИЕ

С докладом «Обеспечение цифрового суверенитета как приоритет государства» выступил **Ренат Лашин, исполнительный директор Ассоциации разработчиков программных продуктов «Отечественный софт»**. Кстати, председателем правления ассоциации является **Наталья Касперская**, одна из самых авторитетных и влиятельных персон в российской IT-индустрии.

54 ПРОЦЕНТА РОССИЯН НЕ ЖЕЛАЮТ ДЕЛИТЬСЯ СВОИМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ.

- Нам нужно противостоять влиянию извне, которое все больше на нас оказывается, - утверждает Лашин. - А для этого необходим цифровой суверенитет. Это возможность самостоятельно определять внутренние и геополитические национальные интересы в цифровой сфере, распоряжаться собственными информресурсами и так далее.

Что эксперт имеет в виду? В России активно идет цифровизация денежно-кредитной системы, транспорта, госуправления, военной сферы, не говоря уже о бытовых сервисах для граждан. Но еще не так давно она проводилась преимущественно с помощью импортного оборудования. **Эксперт Наталья Куликова** писала в 2015 году, что на рынке электронных комплектующих отечественная продукция составляла 31,3 процента, а импортная, соответственно, 68,7 процента. И все это заграничное добро может быть напичкано разными «закладками» (аппаратными и программными), с помощью которых их в нужный момент будет возможно отключить. Погаснет свет в домах, начнут выходить из строя АЭС, оружейные системы превратятся в металлолом. А персональные данные любого гражданина превратятся в открытую книгу.

Лашин считает, что в этом вопросе надо брать пример с Китая. В 2017 году там был принят закон о кибербезопасности, который предусматривает, что все госучреждения и ключевые инфраструктурные операторы должны использовать «безопасные и контролируемые» технологии. Россия тоже пошла по этому пути, приняв несколько аналогичных законов, но о полном импортозамещении, по его словам, речи нет. Например, большинство Государственных информационных систем до сих пор поддерживают работу только с иностранным программным обеспечением.

Эксперт уверен, что нам необходимо создавать свою технологическую линейку.

- Знания передаются от разработчиков процессоров к разработчикам устройств, от них - к разработчикам операционных систем, далее - к создателям приложений и языков программирования. Любая лакуна в цепочке - дыра для влияния, закладок, вторжения, отключения извне.

Полная отечественная технологическая линейка, считает он, позволит удержать талантливых разработчиков, также является средством влияния на другие страны. А Россия в союзе с Беларусью станут неприступными цифровыми крепостями.

Виталий ТИМКИВ/РИА Новости

Чтобы уберечься от хакеров, «Газпром» полностью перешел на отечественные комплектующие для компрессорных установок.

СЕТЕВАЯ ВОЙНА

ДИВЕРСИЯ С НЕБА

В 2019 году, по информации «Нью-Йорк таймс», США пытались проводить кибератаки против российских электрических сетей. Совершалось это путем воздействия на иностранные комплектующие. К счастью, российская электронная защита сработала успешно.

В том же году была заблокирована работа импортных компрессорных установок «Газпрома». Команда была послана из космоса, со спутника. Чтобы избежать таких атак впредь, газовый монополист заменил импортное оборудование отечественным, изготовленным на казанском предприятии.

Член президиума Совета по внешней и оборонной политике Александр Лосев заявил в эфире «Вестей ФМ», что российская армия готовится к противодействию в киберсфере.

- Ушел из информационного поля очень интересный отчет, который подготовили в мае «Ростелеком» и ФСБ, о том, что зафиксированы мощнейшие хакерские атаки на серверы и сайты наших федеральных ведомств. Уровень угроз - очень высокий. Уровень профессионализма хакеров - колоссальный. По уровню подготовки и тому, как это было проведено, можно сделать вывод, что это - не любители, не студенты из Калифорнии или Хельсинки. Это атака враждебного государства. По сути, кибервойна началась.

БелТА

Суперкомпьютер СКИФ-ГЕО-ЦОД входит в ТОП-50 мощнейших машин на территории СНГ.

КОМПОНЕНТЫ СУВЕРЕНИТЕТА

САМИ С УСАМИ

Что требуется для гарантии электронной и информационной безопасности государства.

- **Собственная аппаратная платформа:** Процессоры, микросхемы, цифровые устройства (ПК, смартфоны), сетевое оборудование, чип геопозиционирования.
- **Своя программная платформа:** BIOS, операционная система, браузер, офисный пакет, мессенджеры, бухгалтерия, ERP, шифрование, антивирус, средства разработки и ПО, средства информационной безопасности, мобильные ОС.
- **Автономные системы управления предприятиями и страной:** Электронное правительство, IT в министерствах и ведомствах, банковские системы, инженерные и транспортно-логистические системы, системы управления промышленными объектами и предприятиями, системы проектирования.