# НОВАЯ ЦИФРОВАЯ ЭПОХА: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОЙ ПОЛИТИКЕ РОССИИ

**Аннотация**

В статье рассматривается политизация общественных отношений в цифровой сфере, выделяются ключевые тренды данного процесса, анализируются основополагающие документы государственной политики России в области информационной безопасности — ответной реакции государства на изменения внешней цифровой среды.

**Ключевые слова:** балканизация Интернета, кибератаки, информационная безопасность, цифровая экономика.

**Автор**

**Садов Константин Сергеевич**

Студент кафедры государственной политики факультета политологии Московского государственного университета имени М.В. Ломоносова (Москва, Россия)

В сентябре 2010 г. центрифуги иранского ядерного проекта неожиданно начали оплавляться, выделяя опасную радиацию в окружающую среду. Причиной стал не сбой в автоматизированной системе контроля, а вирус Stuxnet — компьютерный червь, чьи действия оказались первой в истории кибератакой с разрушением физических объектов впоследствии.

Ответственность за проведенную атаку взяли на себя США (инициированная Б. Обамой операция «Олимпийские игры» по сдерживанию Ирана) [1].

Киберпространство сродни ядерной энергетике: с одной стороны, оно позволяет нам выстраивать глобальную экономику, обмениваться информацией в абсолютно разных точках земного шара, автоматизировать и улучшать процессы производства, повышать транспарентность государственных органов, приобретать кредит доверия к институтам власти. Однако в то же самое время именно информационная среда, по словам бывшего министра обороны США Р. Гейтса, становится пятой средой ведения боевых действий — наравне с землей, водой, космосом и воздухом [2].

Особенность кибератак заключается в том, что барьер входа на арену борьбы для них крайне низкий по сравнению с другими сферами: достаточно знания программирования, компьютера и выхода в Интернет. Источники данных атак крайне сложно отследить, а сама архитектура Интернета фактически нивелирует саму идею национально-территориального деления государств [3].

Эти условия предполагают, что информационная структура государства может быть атакована как киберподразделениями другого государства, так и рядом иных акторов: корпорациями, террористическими ячейками и отдельными индивидами.

Сами атаки могут носить характер и кибершпионажа, и уничтожения информационной структуры государства либо общественных институтов с

возможным разрушением физических активов.

Кибероружие, в частности, также предполагает опасность для сил ядерного сдерживания, что особенно актуально в свете последнего обращения Президента РФ В.В. Путина к Федеральному Собранию, на котором были представлены новые системы стратегических вооружений [4].

Исходя из вышесказанного, можно утверждать, что включение информационной безопасности в ряд направлений государственной политики по развитию информационного общества в РФ является насущным требованием сегодняшнего дня.

Адаптирован ли современный стратегический блок, целеполагающий в условиях деятельности государственных органов власти, к указанным тенденциям?

Обратимся к одной из самых инновационных программ российского правительства, являющейся частью общегосударственной политики по информатизации и информационной безопасности — «Цифровая экономика» [5].

Цель информационной безопасности определяется как «достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие РФ в условиях цифровой экономики», что указывает на следующее: государство участвует в обеспечении безопасности не только собственной информационной структуры, но и берет ответственность за сохранность данных граждан, бизнес-структур и всего общества в целом.

При этом данная цель обеспечивается в нормативной (правовая защита владельцев информации), физической и кибернетической среде (обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной структуры России). Также предполагается продвижение продуктов кибербезопасности и национальных интересов в данной области на международную арену.

Программа нацелена на сокращение иностранного сегмента серверов в трафике РФ до 5% и внедрение единых стандартов кибербезопасности для государства и общественных институтов. Данные ориентиры отражают общемировой тренд к «балканизации Интернета», формированию цифрового суверенитета государств и поиска ими моделей снижения рисков в условиях развивающейся глобальной экономики и диффузии регулирующей роли государства.

Следует отметить, что в программных документах подчеркивается определяющая роль взаимодействия государства и общественных структур в области обеспечения информационной безопасности: от совместной разработки программного обеспечения и систем защиты до формирования совета по вопросам безопасности новых технологий из компетентных представителей от общества.

Вместе с тем программа «Цифровая экономика» идет в русле Доктрины информационной безопасности РФ, впервые принятой в 2000 г. и пересмотренной в 2016 г. [6]. Эти документы представляют собой систему базовых принципов, которые закладываются в основу государственной политики информационной безопасности.

Конкретная эволюция взглядов выражается в акцентировании внимания на использовании не только кибератак против России, но также и информационно-психологического воздействия, которое приравнивается к угрозе информационной безопасности в силу способности дестабилизировать внутриполитическую и социальную ситуацию и привести к подрыву суверенитета. Отдельно выделяются

террористические группы как источник потенциальных угроз, что также отражает тенденцию снижения порога совершения киберпреступлений.

В рамках данного документа выделяются основные направления деятельности с целью обеспечения информационной безопасности: противодействие пропаганде экстремизма, защита критически важной информационной инфраструктуры, систем вооружений, разработка собственного программного обеспечения, равно как и спасение традиционных ценностей от размывания.

Особняком среди этих документов стоит «Стратегия развития информационного общества в РФ на 2017–2030 годы» [7], т.к. в ней выделяются наиболее перспективные технологические тренды, которые должны быть созданы в России и для которых уже должна существовать особая инфраструктура безопасности. Вместе с предположением об автоматизации процессов государственного управления и полным проникновением «интернета вещей» в общественную жизнь и государственный сектор данный документ устанавливает необходимые лимиты безопасности.

Особо здесь следует выделить определение «экосистема цифровой экономики», предполагающее широкое взаимодействие государства и общества в вопросах не только внедрения нового технологического уклада, но и в области обеспечения безопасности. И сегодня можно проследить успешное взаимодействие между государственными ведомствами и компаниями, например, «Лабораторией Касперского».

Если стратегический блок целей уже создает пространство для реализации поставленных задач, то на оперативном уровне ведомств продолжается работа над современными системами защиты информации, главной из которых стала созданная в результате принятия ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [8] глобальная система по борьбе с компьютерными атаками (или ГосСОПКА) [9], курируемая ФСБ и представляющая собой поле обмена информацией о всех атаках на критически важные объекты на территории России: от федеральных и региональных органов власти до науки и химической промышленности. Каждый участник данной программы обязан выработать свою систему защиты, а после подключиться к ГосСОПКА.

Уже известно, что созданный на базе ГК «Ростех» КЦОПЛ (корпоративный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак), равно как и ФинЦЕРТ Центрального Банка или НИИАС «РЖД», подключены к ГосСОПКА [10].

Более того, в 2014 г. РФ обрела новый инструмент противодействия потенциальным противникам в области киберпространства в целях обеспечения Доктрины информационной безопасности — войска информационных операций, находящиеся в подчинении Министерства обороны России [11]. Тогда же был подписан указ о создании кибернетического командования, главной целью которого является защита электронных систем управления РФ от вмешательства со стороны потенциальных противников.

Само понятие «информационные операции» предполагает «использование и управление информационными и коммуникационными технологиями для достижения превосходства над противником» [12]. Они включают в себя не только защиту от и проведение кибератак, но также и дезинформацию противника, ведение психологической войны, кибершпионаж и т.д.

В рамках современных министерств происходит создание структур информационной безопасности (например, отдел информационной безопасности Департамента высоких технологий Минкомсвязи РФ [13]), реализуется рынок SafeNet (безопасные и защищенные компьютерные технологии)

в составе Национальной Технологический Инициативы [14], проводятся мероприятия по обеспечению кадрового состава защиты цифровой инфраструктуры будущего (к примеру, серии хакатонов с отбором лучших команд по созданию продукта информационной защиты [15]).

Все это говорит о том, что работа в направлении информационной безопасности сейчас активно ведется — и это не может не радовать, учитывая, что будущее предвещает нам проникновение цифровых технологий абсолютно во все сферы жизни общества, с характерным изменением понятия публичности. В условиях того, что практически каждый дом может быть оборудован «интернетом вещей», а вся активность пользователей в глобальной сети оставляет и будет оставлять после себя цифровой след, вопросы конфиденциальности, защиты информации как для гражданина, так и для всего государства приобретают приоритетное значение. Только та страна, которая сможет обеспечить надежную защиту от кибератак и сопровождающих их «психологических войн», будет вознаграждена и экономическим развитием, и притоком инвестиций из менее стабильных в информационном плане территорий мира (но все же помним, что для Интернета понятие «национальные границы» весьма размыто), равно как и полной свободой использования информации для саморазвития человека.

## Литература

1. *Коэн Дж.* Новый цифровой мир / Пер. с англ. — М.: Манн, Иванов и Фербер, 2013.
2. New DOD cyber command to protect .mil domain/ Washington Technology [Электронный ресурс]. — Режим доступа: https://washingtontechnology.com/articles/2009/06/15/web-dod-cyber-command.aspx (дата обращения: 06.03.2018).
3. *Росс А.* Индустрии будущего / Пер. с англ. — М.: АСТ, 2017.
4. Послание Президента Федеральному Собранию [Электронный ресурс]. — Режим доступа: http://kremlin.ru/events/president/news/56957 (дата обращения: 21.09.2018).
5. Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р.
6. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).
7. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы. Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203.
8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
9. Восхождение на ГосСОПКА [Электронный ресурс]. — Режим доступа: http://www.jetinfo.ru/stati/voskhozhdenie-na-gossopka (дата обращения: 11.09.2018).
10. Ростех потратит на защиту от хакеров 800 млн руб. [Электронный ресурс]. — Режим доступа: https://www.rbc.ru/politics/17/08/2017/599180249a7947963e65f566 (дата обращения: 13.09.2018).
11. Шойгу объявил о создании войск информационных операций [Электронный ресурс]. — Режим доступа: https://rg.ru/2017/02/22/shojgu-obiavil-o-sozdanii-vojsk-informacionnyh-operacij.html (дата обращения: 16.09.2018).
12. Что такое информационные операции [Электронный ресурс]. — Режим доступа: http://tass.ru/info/4046536 (дата обращения: 07.08.2018).
13. Приказ Минкомсвязи России «Об утверждении Положения о Департаменте развития высоких технологий Министерства связи и массовых коммуникаций Российской Федерации» [Электронный ресурс]. — Режим доступа: http://minsvyaz.ru/ru/documents/4940/ (дата обращения: 16.09.2018).
14. SafeNet [Электронный ресурс]. — Режим доступа: http://www.nti2035.ru/markets/safenet (дата обращения: 20.09.2018).
15. AI HACK [Электронный ресурс]. — Режим доступа: http://aihack.ai-hub.ru/ (дата обращения: 17.09.2018).