ВВЕДЕНИЕ[1]

Для современного общества, справедливо названного «информационным», проблемы информационного обеспечения различных сфер экономической и общественной деятельности по своей значимости и актуальности превосходят проблемы дальнейшей индустриализации производства. Появился даже новый термин «цифровая экономика», формирование которой рассматривается как непременное условие обеспечения эффективности современного государства.

Под информационным обеспечением деятельности (в смысле развития цифровой экономики), очевидно, следует понимать предоставление каждому ее участнику всей необходимой ему информации с соблюдением требований доступности, своевременности, целостности, актуальности, релевантности, толерантности и, конечно же, в необходимых случаях конфиденциальности. При этом обостряется проблема обеспечения безопасности и доверия при использовании современных информационных технологий. Компьютеры учреждений, организаций, частных лиц все чаще являются объектами, подвергающимися нападению. Нарастают симптомы развивающейся информационной войны.

В этой связи важнейшим документом, определяющим направления государственной политики в области обеспечения информационной безопасности России, является Доктрина информационной безопасности Российской Федерации. Следует отметить, что первый вариант Доктрины был утвержден Президентом страны еще 9 сентября 2000 г. Основной целью создания этого концептуального документа явилось определение основных направлений деятельности органов государственной власти по обеспечению безопасности государства в информационной сфере, а также конкретизация общецелевых установок по противодействию угрозам информационной безопасности в различных сферах жизнедеятельности личности, общества и государства.

[1] При написании введения авторами использованы материалы сравнения двух вариантов Доктрины информационной безопасности 2000 и 2016 гг., подготовленные в рамках исследовательской работы студентки Национального исследовательского ядерного университета «МИФИ» Я. Валацкайте.

Среди этих основных направлений обеспечения информационной безопасности России в Доктрине 2000 г. были выделены:

- развитие и совершенствование системы обеспечения информационной безопасности;
- совершенствование нормативно-правовой базы обеспечения информационной безопасности;
- разработка федеральных и региональных программ обеспечения информационной безопасности;
- координация деятельности федеральных органов власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности;
- создание систем и средств предотвращения несанкционированного доступа к информации, а также разработка и принятие нормативно-правовых актов, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации или ее неправомочное использование;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие единой системы подготовки кадров в области информационной безопасности и информационных технологий;
- определение порядка финансирования программ обеспечения информационной безопасности;
- совершенствование законодательства, регулирующего отношения в области развития информационных технологий;
- защита конституционных прав и свобод человека и гражданина в процессе обеспечения информационной безопасности.

Вторая редакция Доктрины информационной безопасности Российской Федерации, принятая в декабре 2016 г., является дальнейшим развитием положений Доктрины 2000 г. с учетом реалий современного этапа становления глобального информационного общества. Она представляет собой совокупность официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Таким образом, Доктрина является документом стратегического планирования в области обеспечения национальной безопасности страны, что соответствует основным положениям Стратегии национальной безопасности Российской Федерации, утвержденной Президентом Российской Федерации в декабре 2015 г.

Если анализировать изменения, произошедшие в структуре документа относительно предыдущей его версии, то в первую очередь необходимо отметить, что текущее состояние информационной безопасности, а также направления обеспечения информационной безопасности рассматриваются в разрезе стратегических национальных приоритетов, обозначенных в Стратегии национальной безопасности. Благодаря этому документ является более структурированным и последовательным по сравнению с версией 2000 г. Положения новой Доктрины соответствуют актуальным тенденциям в сфере информационных технологий и информационной безопасности, таким, как импортозамещение, обеспечение безопасности критически важной инфраструктуры, противодействие кибератакам и др.

Несмотря на более чем пятнадцатилетний период, прошедший с момента принятия Доктрины 2000 г., некоторые проблемные вопросы все еще остаются крайне актуальными. Хотя мы констатируем, что уровень развития отечественных информационных технологий постоянно растет, он все еще не достиг достаточных показателей, и сделать в этой сфере предстоит еще очень многое. По-прежнему остро стоят вопросы противодействия враждебному информационному воздействию на массовое сознание, все большую опасность приобретают угрозы компьютерных атак на объекты критической информационной инфраструктуры.

Характеризуя общее содержание новой Доктрины информационной безопасности, необходимо отметить, что значительный ее объем посвящен рассмотрению четко сформулированных национальных интересов Российской Федерации в информационной сфере, основных информационных угроз и анализу в связи с этим состояния ее информационной безопасности. Принципиально важным моментом, отмеченным в Доктрине, является то, что состояние информационной безопасности страны сегодня характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. В качестве угрозы рассматривается высокий уровень зависимости страны от зарубежной компонентной базы и программного обеспечения. Это обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран. Эти положения Доктрины привлекли особое внимание западных аналитиков. В своих комментариях они сразу же отметили, что «Российская Федерация провела широкий анализ слабых мест своей национальной экономики и промышленности, а также

функционирования собственных информационных систем»[1], признала существование проблем в этой сфере, а в качестве решения выбрала разработку собственных ресурсов в секторе информационных технологий и создание преференций для отечественного бизнеса, науки и техники.

Западные комментаторы отмечают, что Доктрина призывает принять все необходимые меры для минимизации влияния иностранных игроков[2]. Со своей стороны дополним, что в Доктрине отмечается и недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий, низкий уровень внедрения отечественных разработок и недостаточное кадровое обеспечение сферы информационной безопасности.

Нельзя не отметить нацеленность государства на «повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации», на развитие кадрового потенциала, что также отмечается в зарубежных комментариях[3]. Особо как серьезная угроза констатируется низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности.

В новой редакции Доктрины сохранились основные взгляды на необходимость безусловного обеспечения информационной безопасности в области обороноспособности нашей страны. Отмечается, что в последнее время заметно выросло количество внешних угроз, связанных с враждебным настроем некоторых иностранных государств и, конечно же, террористических и экстремистских группировок и организаций.

В новой версии Доктрины, по сравнению с редакцией 2000 г., появился новый раздел, касающийся сотрудничества России

---

[1] *Lukasz Olejnik*. Interesting Points in New Russian Information Security Doctrine [Электронный ресурс]: Security, Privacy & Tech Inquiries. 2017, 04 Jan. — Режим доступа: URL: https://blog.lukaszolejnik.com/interesting-points-in-new-russian-information-security-doctrine.

[2] В России утверждена новая доктрина информационной безопасности [Электронный ресурс]: Сайт компании «Аладдин Р.Д.» 2016, 13 декабря. — Режим доступа: URL: https://www.aladdin-rd.ru/company/pressroom/articles/45192.

[3] Анализ положений доктрины информационной безопасности РФ [Электронный ресурс]: Сайт SecurityLab.ru. 2017, 10 февраля. — Режим доступа: URL: http://www.securitylab.ru/analytics/485289.php.

с другими странами в области обеспечения информационной безопасности и развития стратегического партнерства в этой области. Новшеством в документе является и то, что наряду с органами власти активными участниками системы управления обеспечением информационной безопасности признаются собственники объектов критической информационной инфраструктуры и организации, занимающиеся эксплуатацией таких объектов. К числу таких активных участников отнесены и средства массовой информации, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи. Особая роль отводится средствам массовой информации и массовых коммуникаций, поскольку в Доктрине впервые сформулированы задачи доведения до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире. Основные положения Доктрины впрямую затрагивают и интересы организаций, которые занимаются созданием и эксплуатацией информационных систем и сетей связи, разрабатывают, производят и эксплуатируют средства обеспечения информационной безопасности, оказывают услуги в этой области, организаций, занимающихся образовательной деятельностью, а также соответствующих общественных организаций.

Резюмируя отметим, что новая Доктрина информационной безопасности России наиболее полно учитывает все изменения, произошедшие в сфере информационной безопасности за последние годы, но в то же время существенно не меняет концептуальные взгляды на проблему по сравнению с Доктриной 2000 г.