Г.А. Воробьев

Новая доктрина информационной безопасности России: приоритеты, задачи, перспективы

6 декабря 2016 г. Президент Владимир Путин утвердил новую доктрину информационной безопасности Российской Федерации. Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Предыдущая доктрина от 2000 г. утратила силу как устаревшая.

В новой Доктрине на основе анализа основных информационных

угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации. Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности и **затрагивает широкий спектр угроз и вызовов, стоящих перед Россией, от хакерских кибератак до давления на российские СМИ за рубежом и определяет такие положения как:**

- национальные интересы в информационной сфере;
- основные информационные угрозы и состояние информационной безопасности;
- стратегические цели и основные направления обеспечения информационной безопасности;
- организационные основы обеспечения информационной безопасности.

Среди национальных интересов России в информационной сфере первым пунктом указаны обеспечение и защита конституционных прав и свобод гражданина, получающего и использующего информацию, неприкосновенность частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизм взаимодействия государства и гражданского общества, а также применение информационных технологий в целях сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа России.

Далее следует обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры РФ, развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, содействие формированию системы международной информационной безопасности.

Причины необходимости обновления доктрины информационной безопасности России можно разделить на 2 основные группы:

- прогресс в сфере информационно-коммуникационных технологий;
- политическая ситуация в стране и в мире.

Если в документе 2000 г. говорится о возрастающем влиянии ин-

формационных технологий на национальные интересы страны, то в новой Доктрине они рассматриваются уже как неотъемлемая часть всех сфер жизни. Новая доктрина отражает изменившиеся обстоятельства – проникновение мобильной техники в повседневную жизнь практически каждого гражданина и практически полное поглощение пользователей интернетом.

Политические условия, которые повлияли на обновление доктрины приведены в самой доктрине в качестве угроз информационной безопасности России.

Одним из главных негативных факторов, влияющих на состояние информационной безопасности, указано наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную структуру в военных целях. Одновременно усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

Иностранные спецслужбы «информационно-психологически» воздействуют на другие государства в попытках «дестабилизировать внутриполитическую и социальную ситуацию в различных регионах мира».

Российские средства массовой информации, при этом, зачастую подвергаются за рубежом откровенной дискриминации, а в иностранных СМИ наблюдается тенденция к увеличению количества материалов, содержащих предвзятую оценку государственной политики России.

В то же время наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание.

Возрастают масштабы компьютерной преступности, в том числе в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина.

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети Интернет, не позволяет реализовать совмест-

ное справедливое, основанное на принципах доверия управление ими.

В доктрине также отмечается, что отечественная промышленность находится в сильной зависимости от зарубежных информационных технологий, что делает социально-экономическое развитие страны зависимым от геополитических интересов других государств. При этом научные исследования по созданию перспективных информационных технологий недостаточно эффективны, внедрение отечественных разработок находится на низком уровне, а сфера информационной безопасности недостаточно обеспечена квалифицированными кадрами.

Стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий, обозначено в качестве одного из основных направлений обеспечения информационной безопасности в области обороны страны. Среди других целей упомянуты повышение конкурентоспособности российских IT-компаний, ликвидация зависимости от зарубежных информационных технологий, развитие национальной системы управления российским сегментом Интернета, нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества, проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности; развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий. В частности, глава Минкомсвязи России Николай Никифоров заявил, что России необходимо в настоящее время более миллиона специалистов в сфере информационных технологий, подчеркнув, что для них уже есть рабочие места.

В связи с тем, что текущее положение характеризуется низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности, одним из основных направлений информационной безопасности в области образования также должно стать формирования культуры личной информационной безопасности граждан.

Доктрина информационной безопасности, утвержденная главой государства, будет сопровождаться законодательными актами, над которыми уже работают профильные комитеты и комиссии Федерального Собрания.

Документы, подобные Доктрине информационной безопасности России, были приняты и в других государствах. К примеру, политику Соединенных Штатов Америки в информационной сфере определяет утвержденная в 2011 г. Бараком Обамой «Международная стратегия в киберпространстве». Она включает вопросы информационной безопас-

ности в экономике, защиты национальных сетей, правопорядка, военной отрасли, интернет-правительства.

Об усилившемся внимании к кибернетическому противостоянию в НАТО говорит и тот факт, что работу над усилением кибервойск ведут не только страны, лидирующие в альянсе, но и государства, занимающие второстепенные позиции. К примеру, Министерство обороны Польши заявило о намерении потратить на создание и развитие киберармии 1 млрд злотых.

Председатель думского комитета по информационной политике, информационным технологиям и связи Леонид Левин выступил со следующим комментарием: «Понятие „кибервойна» стало не игрушкой подростков и футурологов, а фактором международных отношений».

Снова встал вопрос о не раз высказывавшихся в России предложениях создать международный институт регулирования интернета на уровне и по принципам ООН. Спектр угроз расширился и все более смещается в сферу коммуникационных сетей и бытовых цифровых технологий. Самый важный момент – это признание того, что Интернет является таким же пространством международной политики, как любая другая среда, соответственно, в Сети также возможны военные угрозы и военные конфликты, заявил глава думского комитета.

Советник президента во вопросам развития Интернета, глава ИРИ так прокомментировал утверждение доктрины: «Есть три типа проблем, с которыми мы сталкиваемся в информационном пространстве, – это программное обеспечение, это «железо», это смыслы, которые приносят на нашу территорию, формируя общественное мнение... Они все равновесны, они все очень важны. Нельзя закрыть одну проблему, не победив другую. Только комплексные мероприятия позволят каким-то образом обезопасить нашу экономику и население от недружественного нам влияния».

Следует отметить, что концептуальные, научные и образовательные подходы нашего университета к информационной безопасности и защите информации, реализуемые нами на протяжении уже довольно долгого времени, очень схожи с принципами новой доктрины информационной безопасности.

Мы убеждены, что в современных технологических, социальных, геополитических условиях обучение информационной безопасности должно носить комплексный характер как в содержательном плане, так и в плане методологической и инструментальной базы. Современный специалист в сфере защиты информации, безусловно, должен владеть техническими и технологическими профессиональными компетенциями, но не менее важно для него иметь глубокие знания гуманитарных

аспектов информационной безопасности, которые, зачастую, наносят не меньший, а иногда и больший урон безопасности государства и личности.

Но, по нашему глубокому убеждению в современных условиях чрезвычайно важным является обучение основам информационной безопасности каждого студента, вне зависимости от направления подготовки или специальности, по которым он получает образование, в связи с чем мы убеждены в целесообразности включения таких курсов во все образовательные программы вуза.

В этом контексте актуально высказывание вице-спикера Государственной Думы Петра Толстого: «Надо понимать, что никакие доктрины не помогут, пока мы сами не начнем отдавать себе отчет о грозящих опасностях, пока не начнем соблюдать информационную гигиену и не приучим к этому своих детей».

В этой сфере Пятигорский государственный университет также ведет активную общественно-просветительскую работу, реализуя на постоянной основе ряд проектов по обучению культуре информационной безопасности в повседневной жизни как школьников, так и людей старшего возраста (Тимуровцы информационного общества, Дни информационной безопасности, Дни информационной культуры и др.). В качестве преподавателей в этих проектах выступают, в том числе, и сами студенты ПГУ.

Библиографический список

1. Воробьев Г.А. Информационная культура в развитии информационного общества // Инновационные информационные технологии. 2012. № 1. С. 514-516.
2. Воробьев Г.А. Культура информационной безопасности в современном обществе. В сборнике: Информационные технологии в гуманитарном образовании. Материалы V-VI Международных научно-практических конференций. 2013. С. 77-81.
3. Воробьев Г.А., Павленко И.И. Ситуационный центр в обучении техническим и гуманитарным аспектам информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 117-122.
4. Горбунов А.П. Преобразовательный (креативно-инновационный) университет как ответ на вызовы новой эпохи // Высшее образование в России. 2013. № 8-9. С. 48, 44-46, 49.
5. Депутаты поддержали доктрину Путина об информбезопасности: нужна «информационная гигиена» и институт регулирования Интернета. URL: http://classic.newsru.com/russia/06dec2016/deputat_doktrina_print.html
6. Доктрина информационной безопасности Российской Федерации. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.
7. Павленко И.И. Социальное управление в условиях информатизации общества // Вестник Пятигорского государственного лингвистического университета. 2012. № 2. С. 303-307.