ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ, ПУТИ РЕШЕНИЯ НА МАКРОУРОВНЕ

Е.В. Слепцова, *канд. экон. наук, доцент*
Е.В. Красюк, *магистрант*
Кубанский государственный университет
(Россия, г. Краснодар)

Аннотация. *В статье рассматривается понятие информационной безопасности, ее общий смысл, рассмотрены основные направления повышения информационной безопасности на макроуровне.*

Ключевые слова. *Информационная безопасность, информационные технологии, защита информации, экономическая безопасность.*

Относительная новизна проблематики информационной безопасности в экономической системе определяет ее актуальность. Данный вопрос имеет частичную степень проработки и носит несистемный характер самих исследований. Поэтому для понимания специфики информационной безопасности и большого значения информационно-коммуникационных технологий (ИКТ) для развития предприятия, а также страны и общества и в целом необходима разработка данной темы.

Понятие «информационная безопасность государства» включает в себя защиту конституционного строя, суверенитета, территориальной целостности с точки зрения информационных средств. Под информационной безопасностью понимают защиту и обеспечение жизненно важных интересов отдельной личности, социума и государства в информационной среде от внутренних и внешний атак, т.е. состояние защищенности национальных интересов страны [1].

В Концепции национальной безопасности РФ укрепление информационной безопасности заявлено как одна из приоритетных задач. Рассмотрим основные положения, которые обеспечивают информационную защиту:

1) защита информации (охрана персональных данных, государственной и служебной тайны, а также других видов информации ограниченного доступ);

2) . снижение воздействия преднамеренных или случайных атак естественного или искусственного характера;

3) обеспечение и реализация гарантий конституционных прав и свобод человека и гражданина в информационном пространстве.

4) защита потребностей граждан, отдельных групп и населения отдельно взятой страны в достоверной информации для их развития, образования и жизнедеятельности в целом. Данный фактор положительно влияет на информационно психологическую удовлетворенность граждан и общества и их безопасность от негативных воздействий как информационно психологических, так и информационно – технических воздействий [2].

Исходя из вышесказанного можно констатировать, что национальные интересы страны на макроуровне в информационной среде сконцентрированы на соблюдении конституционных прав и свобод граждан в области получения и пользования информацией, в инновационном оснащении телекоммуникационных технологий и защите государственных информационных ресурсов от несанкционированного доступа.

Для достижения государством таких целей необходимо следующее:

1) Предоставление таких условий гражданам, чтобы могли быть обеспечены главные конституционные права и свободы: тайна личной и семейной переписки, телефонных переговоров, почтовых и иных способов передачи сообщений, защита своей чести и своего доброго имени.

2) Внедрение инноваций, для чего необходимо развитие современных отечественных технологий.

3) Повышение безопасности информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами.

4) Обеспечение защищенности информационных ресурсов от несогласованного доступа.

5) Создание инфраструктуры, с помощью которой производители будут обеспечивать отечественный рынок аппаратными средствами защиты информации.

6) Защита сведений, составляющих государственную тайну [3].

Информационная безопасность РФ является одной из главных составляющих безопасности нашей страны в сферах жизнедеятельности общества и государства. Рассмотрим это на примере статистических данных (табл.), и проследим как изменилась конъюнктура использования информационных технологий прошлых лет.

Таблица 1. Удельный вес организаций, использовавших информационные и коммуникационные технологии

	2012	2013	2014	2015	2016
Организации, использовавшие:					
персональные компьютеры	94,0	94,0	93,8	92,3	92,4
серверы[2)]	18,9	19,7	26,6	47,7	50,8
локальные вычислительные сети	71,7	73,4	67,2	63,5	62,3
электронную почту	85,2	86,5	84,2	84,0	87,6
глобальные информационные сети	87,5	88,7	89,8	89,0	89,6
из них сеть:					
Интернет	86,9	88,1	89,0	88,1	88,7
в том числе широкополосный доступ	76,6	79,4	81,2	79,5	81,8
Интранет	14,7	16,7	16,8	19,2	21,6
Экстранет	6,4	7,7	14,3	16,9	15,0
Организации, имевшие веб-сайт в сети Интернет	37,8	41,3	40,3	42,6	45,9

Анализируя динамику периода с 2012 – 2016 г.г. можно увидеть увеличившееся количество организаций, использующих серверы на 31,9%, электронную почту на 2,4%, глобальные информационные сети на 2,1% из них Интернет на 1,8%, Интранет 6,9%, Экстранет 8,6%. Организации, имеющие веб-сайт в сети Интернет также показываю рост на 8,1%. Такая ситуация говорит о том, что велика вероятность роста киберпреступлений, которые оказываю негативное влияние, как на микро-, так и на макроуровне. С приходом инноваций в сферу ИКТ, тенденция на снижения наблюдается в таких статьях как использование персональных компьютеров и локально вычислительных систем.

Таким образом, мы подходим к определяющему моменту данной статьи – проблемам, связанным с информационной безопасностью на макроуровне. В данном аспекте стоит отметить злоупотребление свободой массовой информации, что является одним из главных внутренних источников угроз информационной безопасности России. С одной стороны, в демократическом государстве журналисты должны информировать общественность по всем злободневным вопросам жизнедеятельно-

сти государства. С другой стороны - в то время, когда государство устраняется, журналист или те лица, которые финансируют, а значит, заказывают, сами определяют, что и как печатается в прессе, показывается по телевидению, звучит по радио. При этом в прессе появляется значительный объем информации, которая является объектом спецслужб.

Другая составляющая негативных последствий, бурно развивающихся ИКТ – возникновение новых форм международных конфликтов, включая информационные войны, сетевые войны, хакерские атаки. По мнению Б. Паньшина, в результате распространения информационно-коммуникационных технологий изменяется характер социума, следовательно, изменяется характер возникающих в нем противоречий и их разрешения [4]. Заметно растет количество государств присоединяющихся к разработке программ информационного воздействия, а также ведению информационных войн.

Относительно перспектив развития информационной безопасности, прежде всего можно отметить, что благодаря существенному технологическому росту информационная безопасность в деятельности по защите информации будет использовать современное оборудование, которое будет бесперебойно работать, а также защищать самих пользователей от их некомпетентности. Защита пользователей от их некомпетентности может подразумевать не только советы от самого оборудования или устройства, но и недопустимость выполнения некоторых действий. Помимо этого, большое развитие должна получить сама нормативно-правовая база, в будущем она должна охватывать все новые вопросы, связанные с обеспечением информационной безопасности.

Также необходимо сказать, что информационная безопасность России является базовой составляющей национальной безопасности России. Она напрямую влияет на эффективную работу органов государственной власти, является неотъемлемым фактором в борьбе с организованной преступностью и мировым терроризмом. Внедрение современных технологий и законодательная основа защиты государственной тайны должна стать мощным звеном в укреплении вертикали власти в России и ее становлении как экономически и политически сильного государства на мировой арене.

Библиографический список

1. *Дорофеев А.В.*, Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. №1 (2). URL: https://cyberleninka.ru.

2. *Ахмадиев Ф.В.* Свобода слова и проблемы информационной безопасности общества и личности // Вестник ЧелГУ. 2013. №38 (329). URL: https://cyberleninka.ru/article.

3. *Гобеев Л.Т.*, Гогаева А.Л., Догузова О.Р. Основные направления обеспечния информационной безопасности Российской Федерации // Материалы Всероссийской научно-практической конференции (заочной). 2017. С. 399-401.

4. *Паньшин Борис* Цифровая экономика: особенности и тенденции развития // Наука и инновации. – 2016 – №157. С. 17-20.

INFORMATION SECURITY: PROBLEMS AND SOLUTIONS ON MACROLEVEL

E.V. Sleptsova, *candidate of economic sciences, associate professor*
E.V. Krasiuk, *graduate student*
Kuban state university
(Russia, Krasnodar)

Abstract*. The article deals with the concept of information security, its General meaning, the main directions of improving information security at the macro level.*

Keyword*. Information security, information technology, information security, economic security.*