*УДК 351.863.1*
*ГРНТИ 81.93.29*

# ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*С.В. ПОПОВА, кандидат экономических наук, доцент*
*ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)*
*В.Е. ФЕДОРИНОВ, доктор политических наук, профессор*
*ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)*

В современном мире противоборство между государствами перемещено в информационное пространство. Информация воздействует на все сферы жизни общества и может стать причиной как бурного развития, так и банкротства. Поэтому защита информации от несанкционированного доступа является одной из главных проблем поддержания национальной безопасности. Основным документом, раскрывающим важные направления в области обеспечения информационной безопасности в экономической сфере, является Доктрина информационной безопасности Российской Федерации.

*Ключевые слова*: киберпреступления; утечки; доктрина; экономическое развитие; информация; безопасность.

## ECONOMIC ASPECTS OF THE INFORMATION SECURITY DOCTRINE

*S.V. POPOVA, Candidate of economic sciencesш, Assistant Professor*
*MESC AF "N.E. Zhukovsky and Y.A. Gagarin Air Force Academy" (Voronezh)*
*V.E. FEDORINOV, Doctor of political sciences, Professor*
*MESC AF "N.E. Zhukovsky and Y.A. Gagarin Air Force Academy" (Voronezh)*

In today's world, confrontation between states is moved to the information space. Information affects all spheres of society and can lead to both rapid development and bankruptcy. Therefore, the protection of information from unauthorized access is one of the main problems of maintaining national security. The main document that reveals important directions in the field of ensuring information security in the economic sphere is the Doctrine of Information Security of the Russian Federation.

*Keywords*: cybercrime; leaks; doctrine; economic development; information; safety.

**Введение.** Современное постиндустриальное (информационное) общество базируется на знаниях, которые находятся в диалектической взаимосвязи с уровнем развития культуры, образования, средств массовой информации и экономики в целом. Информационная сфера оказывает прямое влияние на систему международных экономических отношений. Информация является объектом на рынке информационных услуг. Потери основного капитала в результате форс-мажорных обстоятельств без соответствующей информации практически невосполнимы, но наличие информационного капитала в форме знаний, навыков и опыта позволит восстановить утраченное, однако утечка информации сопоставима с физической утратой капитала. Для крупнейших государств, претендующих на мировое лидерство, становится необходимостью поддержание информационной безопасности. Эта проблема усугубляется в условиях глобализации. Этим объясняется выбор информационного пространства в экономической сфере как объекта исследования. Предметом исследования являются экономические отношения в информационной сфере. Среди наиболее эффективных методов при



СОДЕРЖАНИЕ

изучении данной проблемы были выбраны методы анализа и синтеза, диалектический и статистический методы.

**Актуальность.** Противоборство в информационной сфере в конце XX века между СССР и США привело к распаду первого государства и биполярный мир сменился гегемонией США. Сегодня, повсеместно происходят кардинальные изменения структуры средств массовой информации, появляются новые пути передачи информации и доступа к ней (интернет, сотовая связь). В этих условиях с целью поддержания информационной безопасности многие государства все больше склоняются к процессу деглобализации.

Создаются локальные и региональные интернет сети, изолированные от глобальной сети, для усиления защиты от кибератак и кибервойн. Например, в Китае не используют поисковую систему Google, так как с ее помощью США могут вести информационную войну, слежение, воздействовать на китайскую аудиторию. Диджитальное пространство становится местом краж и обмана, зомбирования людей опасной информацией, которая уничтожает моральные устои у детей и формирует террористов. Страх и неуверенность в безопасности создают предпосылки для изоляции. На сегодняшний день рамки информационной безопасности не ограничиваются только борьбой с киберпреступлениями, внедрением компьютерных вирусов и шпионских программ. Они охватывают сферы юридических, экономических и геополитических интересов.

Цель работы – анализ экономических аспектов доктрины информационной безопасности РФ и оценка с выявлением возможностей и угроз в сложившихся условиях.

Использование информационных ресурсов приводит к ускоренному развитию всех составляющих НТП (созданию инновационных разработок, повышению производительности труда, автоматизации производства). Информация сопровождает вовлечение всех видов ресурсов в воспроизводственные процессы. Чем она достовернее, тем выше шансов у субъектов на получение своей выгоды, и тем выше уровень социально-экономического развития [1].

Экономические инструменты требуются при решении большинства стратегических задач в области обеспечения информационной безопасности, реализация которых требует привлечения и использования значительных размеров финансовых ресурсов, наличие которых определяется уровнем развития экономики. Среди таких задач можно выделить:

1. Совершенствование средств связи и передачи данных, что требует производства высокоточного и инновационного оборудования.
2. Затрат энергетических ресурсов.
3. Развитие обрабатывающей, машиностроительной, оптико-волоконной отраслей,
4. Разработки и создания передаточных устройств с целью обеспечения доступа к информации всех членов общества
5. Совершенствование информационных услуг в сферах науки, образования, здравоохранения и культуры.

Многие страны, в том числе и Россия, в XXI веке в процесс воспроизводства повсеместно вовлекают инновационные факторы, требующие постоянного обновления и защиты информации. Увеличивается масштаб применения информационных технологий в военно-политических целях.

Объем располагаемой информации, а также наличие средств ее преобразования и использования определяет потенциальные возможности развития производства и конкурентоспособность национальной экономики на внешнем рынке. Неравенство в уровнях развития развитых и развивающихся стран сказывается и на возможностях использования информационных ресурсов. Такие последствия от использования ин-



СОДЕРЖАНИЕ

формационных ресурсов требуют принятия на государственном уровне мер и инструментов обеспечения информационной безопасности.

Впервые вопрос о международной информационной безопасности был поднят Россией в 1998 г. на уровне ООН, а 2 декабря 2009 г. Россия предложила резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Первым документом, предусматривающим и анализирующим эти условия, стала принятая 9 сентября 2000 г. Доктрина информационной безопасности Российской Федерации (в дальнейшем Доктрина). В ней представлены основные факторы обеспечения информационной безопасности (ИБ) нашей страны.

В настоящее время основные направления развития информационного общества в нашей стране определены Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года [2], Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденная указом Президента Российской Федерации от 9 мая 2017 г. и Доктриной информационной безопасности РФ в новой редакции от 5 декабря 2016 г. [3]. В этих документах главной целью государства провозглашается противодействие угрозам использования потенциала информационно-коммуникационных технологий (ИКТ) для нанесения ущерба национальным интересам России, а также снижение зависимости во внешней торговле от экспорта сырья. Реализация стратегии должна позволить увеличить экспорт продукции отрасли информационных технологий до 11 млрд долларов США.

Доктрина определяет основные стратегические цели в экономической сфере, среди которых:

- «сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности,

- разработка и производство конкурентоспособных средств обеспечения информационной безопасности,

- повышение объемов и качества оказания услуг в области обеспечения информационной безопасности» [3].

Этот документ подчеркивает, что деятельность всех компаний, связанных с информационными технологиями должна быть направлена на обеспечение информационной безопасности страны.

Следует отметить, что невозможность самостоятельной разработки информационных технологий слаборазвитыми странами относит их в группу потребителей информации и порождает информационно-коммуникационную технологическую зависимость [4]. Это провоцирует развитые государства к поддержанию дальнейшего цифровой дифференциации. Подтверждением этому служит то обстоятельство, что почти 60% населения мира проживает в условиях бедности, следовательно, они не могут воспользоваться даже примитивными на сегодняшний день информационными технологиями.

С начала XX века в России удельный вес организаций, применяющих ИКТ, непрерывно увеличивается. Оснащение производственного процесса компьютерами увеличилось с 2003 по 2016 на 8,5% (рисунок 1).

Применение сервисного программного обеспечения с помощью специализированного оборудования – серверов – увеличилось за тот же период на 39,8%. Количество пользователей, использующих электронную почту, возросло на 41%. По данным статистики, доля организаций передающих информацию, осуществляющих расчеты и оказывающих услуги через глобальные информационные сети, возросла на 55,9%, а

имеющих свой сайт – на 70,6%. Как видим, такой активный переход на информационные технологии требует высокой степени защиты информации.

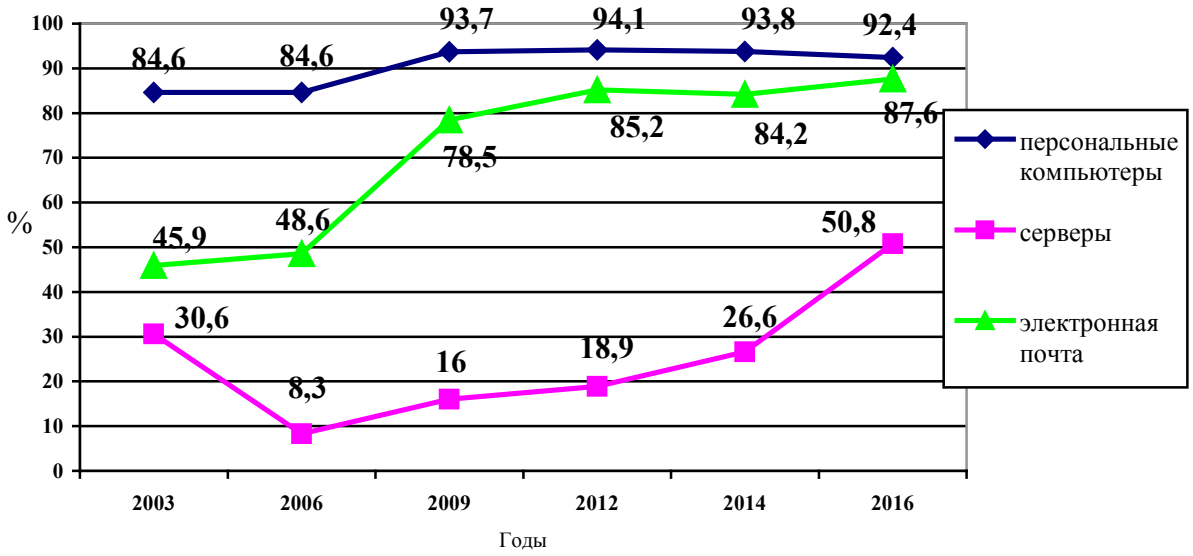


Рисунок 1 – Удельный вес организаций, использующих ИКТ

Все экономические процессы в хозяйственной жизни общества сопровождаются созданием, обработкой, передачей и преобразованием информации. Способы и методы преобразования информации в фактор производства и ее обработка может повлиять на устойчивость экономической системы. Использование информации с целью дестабилизации экономики, основанное на искажении фактов, устранении конкурентов, желании на основе этого максимизировать прибыль, может привести к возникновению как локальных, так и региональных конфликтов.

Состояние международной информационной безопасности усугубляется тем, что «граница», и «территория государства» стали легко проницаемыми и транспарентными для современных информационных технологий. По расчетам Allianz Global Corporate & Specialty, наибольший вред (относительно ВВП страны) действия хакеров принесли Германии. За последний год эта страна потеряла 59 млрд долларов, или 1,6% ВВП. На втором месте США – 108 млрд долларов (0,64% ВВП), третье место занял Китай (60 млрд долларов и 0,63% ВВП). Россия с 0,25% ВВП вышла на пятое место.

Вовлечение России в международные экономические отношения вызывает зависимость экономических субъектов страны от мировых экономических процессов (колебания цен на энергоносители, появление высокотехнологичных отраслей). Поэтому модернизация производства и результаты деятельности таких компаний должны отражать увеличение доли информационной продукции в ВВП и в экспорте. Сегодня российские компании осуществляют поставки средств защиты информации на Кубу и во Вьетнам, в ближайшее время планируется наладить такое сотрудничество с Венесуэлой и Никарагуа.

Эффективность современной стратегии экономического развития страны зависит от государственной информационной и экономической политики. Мы уже упоминали, что как важный фактор производства информация требует применения информационных технологий и увеличения объемов инвестиций. Для производителей владение соответствующей информацией дает очевидные преимущества, позволяет выработать гибкие механизмы управления хозяйственной деятельностью [5]. Для потребителей, дает возможность приобретения новых высокотехнологичных товаров, оплаты услуг,



СОДЕРЖАНИЕ

осуществления заказов и заключение договоров через глобальные сети, создания и использования криптовалют. Одновременно нужно учесть, что параллельно с легальными инструментами и методами использования и передачи информации, создается обширное поле деятельности для всевозможных махинаций [6].

В рейтинге стран по индексу развития ИКТ, в котором оценивается такие факторы как доступность, использование и навыки использования ИКТ. Россия занимала в 2016 году 43 место из 175. Если рассматривать доступность и использование ИКТ, то непреднамеренные ошибки пользователей ИС, операторов, системных администраторов и других лиц, обслуживающих информационные системы представляют реальную угрозу безопасности субъектов на всех уровнях, т.к. они имеют доступ к огромному объему различной информации, знают пароли и секретные коды, но в силу их профессионализма они могут оставаться «невидимками» долгое время. А недостатком навыков работы у 25.3% населения становятся ошибки, в результате которых потеря информации составляет 67%.

В общей численности населения, использующего персональные компьютеры в возрасте от 15 до 72 лет только 53,4% могут работать с текстовыми редакторами, с электронными таблицами – 29,9%. Доля населения, не использовавшего компьютеры, в России в 2016 г. составила 22%, самые низкие показатели 2% в Дании. Удельный вес финансовых операций, проводимых через интернет, составляет 22,5%.

В целом в мире по прогнозам экспертов ущерб от утечки информации к 2020 году составит 1 трлн долларов. По количеству утечек информации на 2017 г. первое место принадлежит США – 451 утечка в год. Россия занимает уже несколько лет стабильное второе место (110 утечек в год), третье место – Великобритания 39 утечек в год [7].

В России наиболее уязвимыми отраслями считаются сфера высоких технологий (14,9%), финансовый сектор (7,9%), торговля (5,8%). Ущерб, наносимый кредитно-финансовой системе в ходе компьютерных атак на финансовые организации, непрерывно растет. В общей сложности доля утечек в коммерческих организациях составляет 79,9%.

Растет число целевых атак на объекты критической информационной инфраструктуры, усиливается разведывательная деятельность спецслужб иностранных государств (14,9% утечек).

На сегодняшний день данные официальной статистики свидетельствуют о том, что ущерб от киберпреступлений в России за первое полугодие 2017 года составил более 18 млн долларов – 40 тыс. преступлений за рассматриваемый период. Использование современных ИКТ и их слабая защищенность, в первую очередь, вызвали увеличение количества преступлений с 11 тысяч в 2013 году до 66 тысяч в 2016 году. За 9 месяцев 2017 года количество утечек информации составило 925 случаев, наибольший интерес представляют персональные данные 65,8%. Раскрываемость в сфере киберпреступлений очень низкая, всего 3-4% за год в среднем в мировой экономике [8].

В научной и образовательной деятельности количество утечек 14,9% и 13,6% соответственно. В следствие, результативность новых научных разработок, обеспечивающих безопасность отечественных информационных технологий, снижается.

Выход из этой ситуации эксперты видят в полной автоматизации процесса передачи информации, строгом контроле за отбором персонала, эффективном его обучении и четком соблюдении положений предусмотренных политикой информационной безопасности. Несмотря на достаточно большое количество утечек из-за человеческого фактора полностью заменить его на техническую составляющую производственного процесса не представляется возможным. На сегодняшний день информационной сфере требуется около 1 млн. специалистов, которые после окончания вуза должны профессионально работать в реальных условиях.



СОДЕРЖАНИЕ

Отсутствие инструментов защиты информации создает угрозу, как для развития отдельного предприятия, т.к. слабая защищенность субъектов экономики от кибератак может привести к усилению зависимости от киберпреступников, за чем следует снижение эффективности национальных научных разработок и сокращение темпов экономического роста, так и для всей экономики в целом. Неправильно введенные данные, ошибки в самой программе, при ее установке, отсутствие надежных паролей, кодов доступа, увеличивает вероятность взлома информационной системы и может поставить деятельность субъекта на грань банкротства, стать причиной утечки капитала и секретной информации, в том числе и в военной сфере.

Сложная геополитическая обстановка вокруг России усугубляется зависимостью отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности и противоречит национальным интересам Российской Федерации, указанным в Доктрине.

Даже высокоразвитые в техническом смысле страны сталкиваются с проблемой утечки информации и уязвимостью программно-аппаратного обеспечения, что порождает реальную угрозу безопасности страны. В этих условиях только собственные средства защиты информации могут с большей долей вероятности обеспечить сохранность и конфиденциальность информации [10].

Согласно статистике, не смотря на представленные выше угрозы информационной безопасности, население, сталкивающееся с несанкционированной рассылкой (спамом) и доступом, заражением вирусами, сократилось с 2014 по 2016 гг. в среднем почти в 2 раза. Население, использующее средства защиты информации увеличилось незначительно (на 1,8%). Таким образом, информация как «гуманное оружие» может стать важным инструментом в руках киберпреступников в рамках ведения экономических войн. По своей результативности информационное оружие сопоставимо с оружием массового поражения. Спектр действия информационного оружия может простираться от нанесения вреда психическому здоровью людей до внесения вирусов в компьютерные сети и уничтожения информации [11].

**Выводы.** На сегодняшний день в любой отрасли экономики используются информационные ресурсы, начиная с процесса производства и заканчивая процессом потребления. Информация стала товаром, ее можно купить и продать. Этим пользуются кибертеррористы, поэтому важно обеспечить надежную систему ее защиты Информационно-коммуникационные технологии определяют степень развития общества, следовательно, информационная политика, проводимая государством, влияет на каждого человека. К сожалению, исходя из проведенного анализа, приходится констатировать тот факт, что на сегодняшний день положения доктрины информационной безопасности России в современной цифровой экономике сфере реализуются недостаточно эффективно экономические цели, определенные в ней не достигнуты, а потенциальные возможности для их достижения на сегодняшний день очень незначительны. Ориентирами государственной политики должны стать рост информационных потребностей населения, темпы и уровень воспроизводства информации.

Информационная политика сегодня не устраняет те угрозы информационной безопасности, которые существуют и все субъекты должны стремиться максимально обезопасить свою деятельность, следуя основным положениям доктрины информационной безопасности РФ в экономической сфере. Особое внимание нужно уделять решению проблем утечки информации, подготовки высококвалифицированных трудовых ресурсов в области защиты информации и финансовым возможностям принятия соответствующих мер.



СОДЕРЖАНИЕ

## СПИСОК ЛИТЕРАТУРЫ

1. Белл Д. Социальные рамки информационного общества. М.: Прогресс, 1986. С. 330.

2. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года Реж. доступа: http://minsvyaz.ru/ru/documents/4084 (дата обращения 05.12.2017).

3. Доктрина информационной безопасности Российской Федерации 5 декабря 2016 г. Реж. доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (Дата обращения 02.12.2017).

4. Поликарпов В.С. Войны будущего. От ракет «Сармат» до виртуального противостояния. М.: Алгоритм, 2015. 368 с.

5. Саитгараев А. Р., Гареева Г. А., Григорьева Д. Р. Эффективность использования информационных технологий в экономической системе России. Реж. доступа: https://moluch.ru/archive/132/36970/ (дата обращения: 02.12.2017).

6. Поткина Е. С., Холопова Л. А. Развитие информационных технологий. Реж. доступа: http://e-koncept.ru/2014/14612.htm.(дата обращения 02.12.2017).

7. Беляев И.И., Грибков Д.Г О проблемах формирования системы международной информационной безопасности // Информационные войны. 2017. № 1 (38). С. 23-29.

8. Киберпрокурор. Реж. доступа: https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html (Дата обращения 05.12.2017)

9. Панарин И.Н. Информационная война и геополитика. М.: Поколение, 2006. 560 с.

10. Андреев В.А., Кравченко Д.А. Информационная война и информационная безопасность // Международный журнал прикладных и фундаментальных исследований. 2016. № 11-4. С. 392-393.

11. Катасонов В. Сталинский ответ на санкции Запада. Экономический блицкриг против России: хроника событий, последствия, способы противодействия / В. Катасонов. М.: Книжный мир, 2015. 288 с.

## REFERENCES

1. Bell D. Sotsial'nye ramki informatsionnogo obshhestva. M.: Progress, 1986. S. 330.

2. Strategiya razvitiya otrasli informatsionnykh tekhnologij v Rossijskoj Federatsii na 2014-2020 gody i na perspektivu do 2025 goda Rezh. dostupa: http://minsvyaz.ru/ru/documents/4084 (data obrashheniya 05.12.2017).

3. Doktrina informatsionnoj bezopasnosti Rossijskoj Federatsii 5 dekabrya 2016 g. Rezh. dostupa: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (Data obrashheniya 02.12.2017).

4. Polikarpov V.S. Vojny budushhego. Ot raket «Sarmat» do virtual'nogo protivostoyaniya. M.: Algoritm, 2015. 368 s.

5. Saitgaraev A. R., Gareeva G. A., Grigor'eva D. R. EHffektivnost' ispol'zovaniya informatsionnykh tekhnologij v ehkonomicheskoj sisteme Rossii. Rezh. dostupa: https://moluch.ru/archive/132/36970/ (data obrashheniya: 02.12.2017).

6. Potkina E. S., KHolopova L. A. Razvitie informatsionnykh tekhnologij. Rezh. dostupa: http://e-koncept.ru/2014/14612.htm.(data obrashheniya 02.12.2017).

7. Belyaev I.I., Gribkov D.G O problemakh formirovaniya sistemy mezhdunarodnoj informatsionnoj bezopasnosti // Informatsionnye vojny. 2017. № 1 (38). S. 23-29.

8. Kiberprokuror. Rezh. dostupa: https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html (Data obrashheniya 05.12.2017.



СОДЕРЖАНИЕ

9. Panarin I.N. Informatsionnaya vojna i geopolitika. M.: Pokolenie, 2006. 560 s.

10. Andreev V.A., Kravchenko D.A. Informatsionnaya vojna i informatsionnaya bezopas-nost' // Mezhdunarodnyj zhurnal prikladnykh i fundamental'nykh issledovanij. 2016. № 11-4. S. 392-393.

11. Katasonov V. Stalinskij otvet na sanktsii Zapada. EHkonomicheskij blitskrig protiv Rossii: khronika sobytij, posledstviya, sposoby protivodejstviya / V. Katasonov. M.: Knizhnyj mir, 2015. 288 s.



Попова Светлана Владимировна, кандидат экономических наук, доцент, доцент кафедры гуманитарных и социально-экономических дисциплин, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, vaiu@mil.ru

Федоринов Вадим Евгеньевич, доктор политических наук, профессор, профессор кафедры гуманитарных и социально-экономических дисциплин, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, vaiu@mil.ru