Роль информационной безопасности в цифровой экономике

Бондарь Алина Константиновна,
студентка 122Б группы очной формы обучения факультета государственного и муниципального управления Дальневосточного института управления – филиала РАНХиГС

Троценко Алина Андреевна,
студентка 121Б группы очной формы обучения факультета государственного и муниципального управления Дальневосточного института управления – филиала РАНХиГС

Аннотация. В статье рассматривается понятие информационной безопасности в цифровой экономике, способы ее укрепления. Обозначаются способы защиты личных данных, рассмотрено понятие защиты информации. Даны некоторые советы рядовым пользователям. Представлены основы формирования информационного общества и цифровой экономики. Дается теоретический анализ понятийного аппарата и основных признаков цифровой экономики, благодаря которым она существенно отличается от других экономических моделей.

Ключевые слова: информационная безопасность, цифровая экономика, информационные технологии, защита информации.

Базовые идеи цифровой экономики зародились относительно недавно – в конце XX века. Исследователи до сих пор не пришли к

единому мнению насчет того, что же такое цифровая экономика, однако в большинстве случаях в определение данного понятия вкладывают следующий смысл: это виртуальная среда, дополняющая реальность системы производственных отношений. В 2016 году на заседании Всемирного банка она была определена как парадигма ускорения развития экономики и ее систем на основе использования современных цифровых технологий.

В науке существует два подхода к пониманию сущности цифровой экономики. Классический подход рассматривает цифровую экономику как экономику, в основе которой лежат цифровые технологии. При этом, данное понятие отождествляется понятиям электронных товаров и услуг, среди них медиа-контент, дистанционные образовательные технологии и другие. Расширенный подход определяет цифровую экономику как экономическое производство, связанное с использованием цифровых технологий.

Сегодня растут не только объемы виртуальных продаж, но и масштаб повсеместного распространения сферы on-line-платежей: интернет-банкинг, электронные платежные системы, распространение криптовалют. Информационные технологии заполоняют все сферы общественной жизни людей, не без исключения экономической. Они не только ускоряют и облегчают процесс обмена информацией, но и значительно повышают производительность труда. В то же время информатизация неизбежно влечет за собой киберриски, опасность возникновения информационных угроз, что также требует более детального изучения методов информационной безопасности.

Таким образом, цель данной работы - характеристика роли информационной безопасности в цифровой экономике как инструмента ее устойчивого функционирования.

Задачи:

1. Охарактеризовать информационную безопасность в условиях цифровизации экономики в контексте защиты национальных интересов Российской Федерации;

2. Описать и оценить эффективность инструментов информационной защиты;

3. Обозначить ключевые направления государственной политики в области информационной безопасности цифровой экономики.

Объектом исследования является информационная безопасность.

Предметом - методы информационной безопасности в цифровой экономике.

Гипотеза исследования заключается в следующем: в условиях цифровизации экономики Российской Федерации государственная политика должна учитывает новые угрозы информационной безопасности.

На общенациональном уровне, информационная безопасность может быть рассмотрена как состояние, обеспечивающее защиту национальных интересов страны в информационном секторе, которые определяются совокупностью государства, общества в целом и личности [1].

На законодательном уровне информационную безопасность определяют как состояние защищенности информационной среды общества, при котором она формируется, используется и развивается в интересах государства, общества и личности.

В узком смысле, на уровне субъектов экономики, информационная безопасность обозначает защищенность информации и инфраструктуры от воздействий, способных привести к ущербу сторон информационных отношений, включая владельцев и пользователей информации. Характер

данных воздействий может быть случайным или преднамеренным, естественным или искусственным.

Цифровая экономика состоит из трёх основных элементов:

1. Элементы инфраструктуры (аппаратура и программы, телекоммуникационные устройства и другое).
2. Направление электронного бизнеса.
3. Направление электронной коммерции (торговля товарами в режиме онлайн).

Это определение, как и некоторые другие, не отражает существо протекающих процессов, не показывает их единство с технологическими новшествами и так далее. Определение цифровой экономики, принятое в России, было представлено в стратегическом плане развития информационного сообщества:

Цифровая экономика – это хозяйственная деятельность, в которой основным производственным моментом выступают информационные данные, выраженные в цифровом формате, а их переработка и применение в существенных количествах, иногда прямо во время их сбора, даёт возможность значительно увеличить уровень эффективности в разных областях производственной и торговой деятельности.

Это определение тоже не совсем полное, но всё же ближе к истине. Прежде всего, цифровую экономику необходимо рассматривать в аспекте применяемых технологий, которые заложены в её основание и определяют качественные показатели произошедших изменений.

Новые информационные технологии способствуют расширению производственной и непроизводственной деятельности человека, его повседневной сферы общения. Для современной экономики все меньшую значимость составляют материальные блага, а наибольшее значение придается информационным продуктам и услугам.

Процессы информатизации связаны с использованием различных информационно-телекоммуникационных средств и систем. Растет потребность в создании и использовании эффективных решений в области информации.

Развитие инновационных технологий в области информации делает уязвимым любое общество. Интеграция национальных экономик привела к экономическим войнам, которые являются убыточными и слишком опасными, межгосударственное противоборство на современном этапе относится к разряду информационного.

Под информационной войной понимается информационное противоборство, цель которого состоит в нанесении ущерба важнейшим структурам второй стороны, подрыве его социальной и политической системы, дестабилизации общественной жизни.

Суть информационного противоборства состоит в межгосударственном соперничестве, которое реализуется при помощи информационного воздействия на ключевые управленческие системы другого государства и общество в целом.

Под информационной преступность подразумевается осуществление воздействий информационного характера на информационное пространство или же его элементы с противоправными целями.

Информационное воздействие – это применение информационного оружия. Информационным оружием является такой комплекс технических средств, технологий и методов, которое предназначено для:

1. контроля информационных ресурсов потенциального противника;
2. вмешательства в процессы управленческих систем и сетей информации, систем связи с целью нарушения их работы;

3. распространения дезинформации или же выгодной информации в обществе;

4. воздействия на сознание и психику различных социальных групп.

Из приведенных выше терминов можно сделать вывод, что информационная безопасность – это невозможность причинения вреда объекту безопасности и его свойствам, которые обуславливаются информацией и инфраструктурой информационного типа.

Основные угрозы нарушения информационной безопасности следующие:

1. Непрофессиональные действия;
2. Преднамеренные действия;
3. Шпионаж, терроризм, преступные группы, хакеры;
4. Стихийные бедствия и аварии;
5. Сбои и отказ технического обеспечения системы;
6. Нелегальное копирование и использование информации;
7. Заражение вирусами информационных систем и др.

При этом объектами информационной безопасности могут быть информационные ресурсы и системы информатизации (Рис. 2).

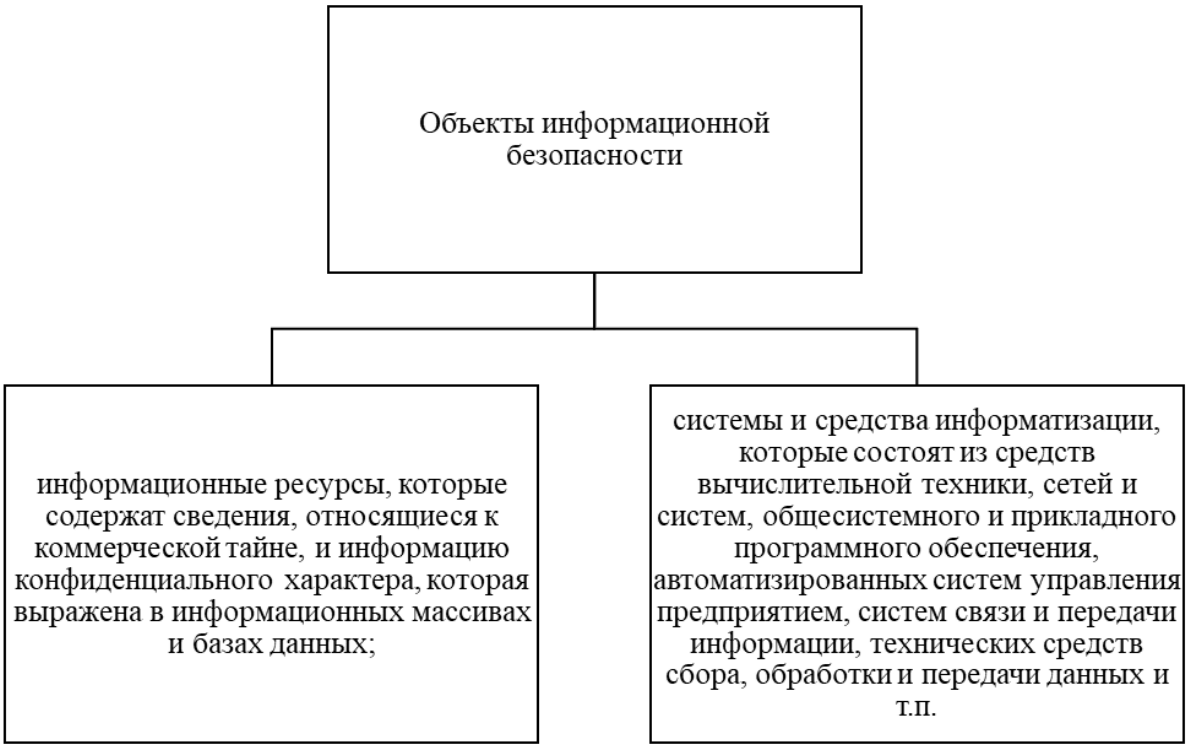

Рисунок 2. Объекты информационной безопасности

Цифровизация, информатизация экономических процессов требуют повышения уровня ее безопасности. Решением данных вопросов занимается государство.

Рынок в России сегодня демонстрирует десяток успешных сервис-провайдеров и фирм, деятельность которых направлена на производство и интеграцию современных информационных технологий. Однако эта же деятельность увеличивает необходимость усиления технологий защиты.

К инструментам обеспечения информационной безопасности цифровой экономики относят [3]:

1. Защита веб-сервисов от хакерских атак, DDoS-атак, мошеннических действий;
2. Биометрия;
3. Введение и распространение электронных цифровых подписей;

4. Развитие систем искусственного интеллекта для решения определенных задач и др.

Биометрические технологии защиты – один из наиболее ярких примеров обеспечения информационной безопасности в экономической сфере. Касание пальца идентифицирует и подтверждает личность человека. Банковская сфера наиболее широко применяет данные технологии в своей отрасли. Вскоре она планирует разработать и внедрить систему кредитования, в основе которой будет лежать распознавание личности клиента по голосу. Все его данные (в т.ч. кредитная история) будут занесены в единую базу.

Еще одним, не менее успешным примером, служат электронные цифровые подписи, содержащие в себе определенные цифровой код. Подобные технологии используются и в системе государственных закупок и электронных торгов, при сдаче отчетности в контролирующие органы.

Кроме того, существуют элементарные правила «цифровой гигиены», которые могут обеспечить информационную безопасность многим компаниям, передавшим эти знания сотрудникам:

1. Регулярно обновлять ПО и антивирусы;
2. Не открывать непонятные вложения;
3. Не переходить по ссылкам в письмах от неизвестных адресатов;
4. Не пользоваться сайтами с сомнительной репутацией;
5. Применять отдельные ноутбуки (планшеты) для работы и развлекательного серфинга в интернете;
6. Не вставлять в ПК непроверенные внешние носители информации и проч.

В целях формирования культуры информационной безопасности нужно регулярно проводить тренинги и семинары по повышению осведомленности работников, а корпоративные службы ИБ должны быть максимально открыты для взаимодействия с коллегами из других подразделений [2].

Информационная безопасность в России в программе «Цифровая экономика», принятая 28 июля 2017 года (Распоряжение Председателя Правительства РФ Д.А. Медведева от 28 июля 2017 года №1632 - р), выделена в отдельный – пятый – раздел, который сегодня активно обсуждается в экспертных группах.

Данные обсуждения позволили сделать несколько выводов о состоянии информационной безопасности в РФ:

1. Информационная безопасность в России является зрелой и вполне успешной отраслью экономики, понимающей свои задачи и методы их решения.

2. Информационная безопасность затрагивает многие отрасли, так или иначе связанные с информационными технологиями.

Соответственно, решая проблемы своей отрасли, экспертное сообщество решает и проблемы экономики в целом. Вместе с тем, вопросы технологий сегодня неотделимы от кадровых вопросов: кто-то должен создавать и обслуживать эти технологии, обеспечивать их безопасность. В этом случае задача подготовки высококвалифицированных кадров в сфере ИТ-инфраструктуры стоит не ниже, чем вопрос обеспечения информационной безопасности [2].

В ходе данного исследования было выявлено, что цифровая экономика существовать без информационной безопасности просто не сможет, а значит, информационная безопасность – это не дело узких специалистов-антихакеров, а забота всех проектировщиков,

разработчиков, тестеров и самих пользователей, под непосредственным руководством государства. Таким образом, гипотеза была подтверждена.

Также можно сделать вывод, что в эпоху повсеместной автоматизации, цифровизации всех сфер общественной жизни обеспечить защиту огромных объемов данных государства, общности и отдельно взятой личности – приоритетная задача цифровой экономики.

Литература:

1. Гэлбрейт Дж. К. Экономические теории и цели общества. - М., 1976.
2. Гэлбрейг Дж. К. Новое индустриальное общество. - М.: АСТ,2004.
3. Белл Д. Грядущее постиндустриальное общество. - М.: АСТ, 1999.
4. Тоффлер Э. Шок будущего. - М: АСТ, 2003.
5. Тоффлер Э. Третья волна. - М.: АСТ, 1999.
6. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» // «Собрание законодательства РФ», 04.01.2016, N 1 (часть II), ст. 212
7. Что дает искусственный интеллект системам кибербезопасности? [Электронный ресурс] URL: https://www.forbes.ru/tehnologii/338971-robot-strazhnik-chto-daet-iskusstvennyy-intellekt-sistemam-kiberbezopasnosti (дата обращения 14.11.2019)