Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.738.5:339-025.27

Князькова
Вероника Святославовна

Методика обеспечения информационной безопасности кластеров в электронной экономике

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель

Лыньков Леонид Михайлович
доктор технических наук, профессор

_____

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Современная цивилизация постепенно вступает на новый исторический этап своего развития – к так называемому постиндустриальному или информационному обществу. Отличительными характеристиками информационного общества является доминирующая роль знаний и информации во всех сферах жизни общества, решающее воздействие информационно-коммуникационных технологий (ИКТ) на образ жизни людей, их образование и работу, а также на взаимодействие государства и гражданского общества. Развитие информационного общества является национальным приоритетом Республики Беларусь. К основным его направлениям развития относятся: электронное правительство, электронное здравоохранение, электронное обучение, электронная занятость и социальная защита населения, электронная экономика и т.п.

Электронная экономическая система может быть определена как совокупность распределённых и автоматизированных (в разной степени) социо-технических подсистем, взаимосвязанных через информационные технологии, а также средствами телекоммуникаций и экономическими законами.

В условиях постоянного интенсивного совершенствования технологий, нарастания темпов внедрения и развития Интернет-технологий в повседневную жизнь все большую актуальность приобретают проблемы информационной безопасности. В научной литературе существует обширное разнообразие определений термина «информационная безопасность» (ИБ). Но все они сводятся к достижению и поддержанию конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Оценить ущерб от хищения информации можно с помощью финансовых и нефинансовых показателей. Так, финансовые последствия могут включать в себя снижение доходов, сбои в работе бизнес-систем, штрафные санкции со стороны регулирующих органов и сокращение числа клиентов. К нефинансовым последствиям можно отнести подрыв репутации компании, пиратское копирование продуктов, утечку научно-технической информации, последствия для инновационной деятельности компании, хищение продуктового дизайна или опытных образцов, незаконное копирование бизнес-процессов и производственных процессов, а также утрату такой особо важной конфиденциальной информации, например, планы по осуществлению сделок слияния и поглощения и стратегия развития компании.

Если оценивать финансовые убытки с учетом этих факторов, их общая сумма может оказаться значительно выше по сравнению с расчетами, опирающимися на традиционные показатели.

Ряд исследований подтвердили предположение о том, что финансовые убытки, возникающие в результате нарушений системы ИБ, в значительной степени зависят от формы и размера организации. Крупные компании выделяют обычно больше средств на ИБ. В результате у них более эффективно внедрены соответствующие бизнес-процессы и формируются знания, необходимые для точного расчета финансовых убытков. Поэтому они могут принять во внимание весь диапазон потенциальных последствий, в том числе издержки, связанные с утратой клиентской базы, оплатой услуг юристов, проведением судебной экспертизы и ущерба репутации. Руководство крупных организаций, как правило, хорошо понимают риски третьих лиц и предъявляют базовые требования по безопасности к своим партнерам. Кроме того, в крупных организациях чаще существует развитая корпоративная культура ИБ, которая базируется на программах повышения осведомленности персонала и соответствующих курсах обучения. В этих компаниях руководители высшего звена контролируют и гарантируют кибербезопасность на всех уровнях организации в соответствии со стандартами безопасности.

Организациям малого бизнеса сложно организовать сложную, комплексную систему защиты информации главным образом из-за ограниченности ресурсов; одним из решением данной проблемы может быть формирование их целевого объединения в форме электронных виртуальных экономически взаимосвязанных сообществ (е-кластеров).

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью работы является разработка базовой модели е-кластера и основных элементов реализации обеспечения его информационной безопасности.

Для достижения указанной цели в работе поставлены следующие *задачи*:

1. Проанализировать основные особенности мер по обеспечению информационной безопасности в электронной экономике и электронном бизнесе.

2. Охарактеризовать особенности развития «электронной экономики» и «электронного бизнеса» в Республике Беларусь.

3. Дать определение организационным основам системы обеспечения информационной безопасности в электронной экономике, выделить в ней основные критические точки.

4. Разработать методику обеспечения информационной безопасности кластеров в электронной экономике.

Объект исследования – организации электронного бизнеса, объединяющиеся в процессе развития экономической системы в е-кластеры.

Предмет исследования – информационная безопасность кластеров в электронной экономике.

Положения, выносимые на защиту

1. Предложен алгоритм реализации оценки рисков информационной безопасности е-кластеров, основанный на следующих этапах: составление перечня информационных активов е-кластера и соответствующих им типов среды; разработка актуальных источников угроз информационной безопасности е-кластера с оценкой рисков их реализации; осуществление процедур минимизации рисков информационной безопасности е-кластера; осуществление контроля за формированием и динамическим изменением угроз информационной безопасности е-кластера; оценка последствий нарушения информационной безопасности для каждого типа информационного актива е-кластера. Данный алгоритм позволяет оценить и управлять рисками информационной безопасности е-кластера с учетом их динамического изменения.

2. Методика оценки рисков информационной безопасности е-кластера, основанная на байесовском подходе, позволяющем определить вероятность наступления события при наличии статистических данных. Данная методика

может использоваться для определения вероятности отнесения исследуемых типов ресурсов к группе ресурсов с высокой или низкой степенью защищенности по отношению к воздействию угрозы типа *Y*, что позволяет принимать обоснованные решения по функционированию ресурсов той или иной степени защищенности, а также, при необходимости, конфигурировать систему защиты информации для ресурсов различных групп.

3. Методика обеспечения информационной безопасности е-кластера, основанная на экономико-математическом моделировании (линейное программирование), что позволяет учитывать различные виды ущерба – экономический (финансовый), технологический, ущерб субъекту персональных данных, репутационный, социальный.

Методология исследования

Теоретическую и методологическую базу исследования составили системный подход к моделированию сложных социально-экономических и технических систем, ключевые положения кибернетики, общей теории систем. При решении поставленных задач использовались труды отечественных зарубежных ученых в области информационной безопасности и теории электронной экономики и электронного бизнеса, математического программирования, теории вероятностей и математической статистики, нормативно-правовые документы и стандарты Республики Беларусь.

Научная новизна исследования заключается в исследовании научной проблемы разработки методики информационной безопасности кластеров электронной экономики на методологической базе экономико-математического моделирования.

Личный вклад соискателя

Содержание диссертации отражает личный вклад автора. Он заключается в разработке алгоритма оценки риска и комплекса базовых защитных мер по обеспечению информационной безопасности е-кластера.

Определение целей и задач исследования, интерпретация и обобщение полученных результатов проводились под руководством научного руководителя, доктора технических наук, профессора Л. М. Лынькова.

Апробация результатов диссертации

Теоретические и практические результаты диссертационных исследований докладывались и обсуждались на следующих научных конференциях:

- Международная научно-практическая конференция (в рамках Республиканского научно-практического форума «Дни науки – 2016»), Макеевка, 13 апреля 2016 г.;

- VIII Международная заочная научно-практическая конференция, Институт бизнеса и менеджмента технологий, Минск, 1 – 14 апреля 2016 г.;
- XIV Белорусско-российская научно-техническая конференция «Технические средства защиты информации», Минск, 25-26 мая 2016 г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 6 печатных работ: 4 тезисов докладов на конференциях и 2 статьи.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из трех глав, заключения, библиографического списка и приложения. В первой главе проведен анализ электронной экономики и основных тенденций ее развития, разработана базовая модель кластера в электронной экономике. Во второй главе проведен анализ особенностей обеспечения информационной безопасности в кластерах электронного бизнеса. Третья глава содержит анализ угроз информационной безопасности виртуального кластера «IT-PARK», а также оценку вероятности реализации угрозы безопасности информации и алгоритмы реализации угроз и минимизации рисков информационной безопасности е-кластера. В приложении приведена политика информационной безопасности в «IT-PARK».

Общий объем диссертационной работы составляет 131 страницу, из них 58 страниц основного текста, библиография из 63 наименований на 8 страницах, включая 6 публикаций автора на 1 странице.

ЗАКЛЮЧЕНИЕ

1. Разработана базовая модель кластера в электронной экономике (е-кластера), проведено обоснование ее использования в экономике. Под е-кластером понимаются связанные между собой по технологической цепочке или ориентированные на общий рынок ресурсов или потребителей организации электронного бизнеса, которые имеют сетевую форму управления и в основе конкурентоспособности которых лежат инновации; при этом условие территориальной локализации не является принципиальным. С точки зрения технологии в основе создания кластеров е-кластеров лежат принципы сети Интернет; с организационной течки зрения основой формирования е-кластеров является общность корпоративной культуры. В е-кластерах владельцы информационных ресурсов переносят часть информации различной степени конфиденциальности в открытый доступ; при этом потеря информации зачастую может поставить под угрозу сам факт существования бизнеса.

2. Эволюционное процессы развития ЭБ, в том числе формирование е-кластеров обозначает актуальную проблему формирования методологического подхода для обеспечения ИБ е-кластера, в частности – снижения рисков ИБ в кластерах ЭБ. Предлагаемая в работе методика обеспечения ИБ кластеров в электронной экономике представлена в виде дополнительных требований к обеспечению информационной безопасности и составлена на основе типовых рекомендаций для такого рода документов. Она применена для виртуального, абстрактного кластера электронного бизнеса «IT-PARK». Предлагаемая методика содержит до 11 этапов.

Основной в предлагаемой методике является оценка рисков информационной безопасности в кластерах электронной экономики. Под риском нарушения понимается возможность утраты свойств ИБ информационных активов в результате реализации угроз ИБ, вследствие чего е-кластеру может быть нанесен ущерб. В диссертации представлен и разработан алгоритм реализации оценки рисков ИБ е-кластеров, реализуемый в пять последовательных этапов: составление перечня информационных активов е-кластера и соответствующих им типов среды; разработка актуальных источников угроз ИБ е-кластера с оценкой рисков их реализации; осуществление процедур минимизации рисков ИБ е-кластера; осуществление контроля за формированием и динамическим изменением угроз ИБ е-кластера; оценка последствий нарушения ИБ для каждого типа информационного актива е-кластера.

3. Для оценки риска реализации угроз ИБ в работе была разработана модель нарушителя информационной безопасности е-кластера; приведена модель нарушителя ИБ виртуального кластера – «IT-PARK». В Модели нарушителя выделяются два типа нарушителя – внешние нарушители (тип I) – лица, не имеющие права доступа к ИС, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ ИС; и внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к ИС, ее отдельным компонентам.

К основным видам нарушителей в модель включены: преступные группы (криминальные структуры); внешние субъекты (физические лица); конкурирующие организации; разработчики, производители, поставщики программных, технических и программно-технических средств; лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ; лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру «IT-PARK» (администрация, охрана, уборщики и т.д.); пользователи ИС «IT-PARK»; администраторы ИС и администраторы безопасности «IT-PARK»; бывшие работники (пользователи).

Рассмотрена задача по минимизацию рисков ИБ в е-кластере рассмотрена как решение экстремальной задачи на основе линейного программирования. Это позволяет определить число единиц информационных ресурсов каждого уровня защищенности (низкий, высокий уровень), которые требуются для того, чтобы при воздействии *i*-й угрозы риски ИБ были минимальны.

4. Для оценки угроз ИБ е-кластера в качестве методологической базы в работе предлагается использовать байесовский подход. Для виртуального е-кластера он позволил найти вероятность отнесения исследуемых типов ресурсов к группе ресурсов с высокой или низкой степенью защищенности по отношению к воздействию угрозы типа *Y*. Осуществив подобные расчеты для всех угроз безопасности в соответствии с моделью угроз и зная требования по обеспечению моделей безопасности, можно принимать обоснованные решения по функционированию ресурсов той или иной степени защищенности, а также, при необходимости, конфигурировать СЗИ для ресурсов различных групп.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Князькова В.С. Отрасль информационно-коммуникационных технологий Республики Беларусь: анализ основных тенденций // Электронная экономика: теория, модели, технологии: Т. Н. Беляцкая [и др.] ; под общ. ред. Т. Н. Беляцкой и Л. П. Князевой. – Минск : БГУИР, 2015. – 248 с. : ил.

2-А. Князькова В.С. Оценка эффективности информационной безопасности электронного бизнеса // Экономика и право: становление, развитие, трансформация: материалы Международной научно-практической конференции (в рамках Республиканского научно-практического форума «Дни науки – 2016») (13 апреля 2016 г.). – Макеевка: МЭГИ, 2016. – 383 с. С. 39-42.

3-А. Князькова В.С. Информационная безопасность как основной элемент корпоративной культуры организаций электронного бизнеса // Инновационные процессы и корпоративное управление: материалы VIII Международной заочной научно-практической конференции, 1 – 14 апреля 2016 г., Минск / Министерство образования Республики Беларусь, Белорусский государственный университет, Институт бизнеса и менеджмента технологий, Ассоциация бизнес-образования / [редколл.: В. В. Апанасович (гл. ред.) [и др.]. – Минск : Национальная библиотека Беларуси, 2016. – 296 с. Страницы 104-112.

4-А. Князькова В.С. Информационная безопасность электронного бизнеса // Технические средства защиты информации: Тезисы докладов XIV Белорусско-российской научно-технической конференции, 25–26 мая 2016 г., Минск. Минск: БГУИР, 2016. — 90 С. Страницы 10-11.

5-А. Лыньков Л.М., Князькова В.С. Экономическое обоснование инвестиций в систему информационной безопасности организаций сферы электронного бизнеса // Технические средства защиты информации: Тезисы докладов XIV Белорусско-российской научно-технической конференции, 25–26 мая 2016 г., Минск. Минск: БГУИР, 2016. — 90 с. Страница 11.

6-А. Князькова В.С. Управление информационной безопасностью электронного бизнеса // Вестник Макеевского экономико-гуманитарного института : сб. научных трудов. – Макеевка : МЭГИ, 2016. - №25 (38). – 263 с. Страницы 72-85.