3. *Wong M., Schlitt W.* Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail // Network Working Group. April 2006.
4. *Allman E., Callas J., Delany M., Libbey M., Fenton J., Thomas M.* DomainKeys Identified Mail (DKIM) Signatures // Network Working Group. May 2007.

Н. В. Гришина

АНАЛИЗ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ С ЦЕЛЬЮ ВЫЯВЛЕНИЯ УГРОЗ ДЛЯ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Коротко суть проблемы можно сформулировать следующим образом: субъектами информационных отношений являются юридические и физические лица, находящиеся в едином информационном конкурентном пространстве. У каждого из них есть свои цели и задачи. Каждый из них решает проблему безопасности информации, необходимой для обеспечения непрерывности бизнес-процессов. Однако часто причины и источники информационных рисков лежат за пределами конкретного субъекта, являются результатом взаимодействия субъектов. А вот эффекту «взаимодействия» должного внимания не уделяется.

Несмотря на важность изучения проблем обеспечения информационной безопасности при различного рода взаимодействиях субъектов информационных отношений, данный объект исследования не выделялся в самостоятельную проблему. Тем не менее исследования, прямо или опосредованно касающиеся данной проблематики, довольно обширны по объему и разнообразны с точки зрения конкретного предмета исследования.

Следует выделить несколько важнейших направлений научно-исследовательской деятельности, в рамках которых затрагиваются отдельные аспекты проблем взаимодействия субъектов информационных отношений:

– анализ понятия, принципов и методов обеспечения информационной безопасности отдельных субъектов информационных отношений;

– анализ подходов к выявлению и нейтрализации информационных рисков субъектов единого информационного поля и угроз информационной безопасности;

– изучение особенностей конкурентной среды как единого информационного пространства, в котором происходит взаимодействие субъектов информационных отношений, нуждающихся в обеспечении защиты информации и информационной безопасности.

Выделенные блоки проблем отчасти смыкаются друг с другом, однако, как правило, рассматриваются отдельно специалистами в разных областях экономики, менеджмента, защиты информации и т. д. Одной из задач данного исследования является объединение ряда таких подходов в рамках интеграции различных научно-исследовательских направлений в целях решения теоретических и практических задач построения модели взаимодействия субъектов информационных отношений.

Выводы

Тематика данного исследования лежит на стыке различных направлений, таких как управление рисками, анализ конкурентной среды, управление информационными рисками, информационная безопасность и др. Изучение выделенного предмета исследования должно представлять собой комплексный анализ экономических, правовых, организационных и технических проблем в различных областях научно-исследовательских знаний.

Имитационное моделирование процессов взаимодействия субъектов единого информационного пространства позволит проанализировать процессы взаимодействия субъектов, определить риск потери информации, риск получения неполной или недостоверной информации, риск получения дезинформации, риск использования информации другим субъектом, а также выявить и исследовать влияние различных факторов, определяющих качество организации и функционирования механизмов, обеспечивающих информационную безопасность субъектов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Андрианов В. В.* Обеспечение информационной безопасности бизнеса. М.: ЦИПСиР: Альпина Паблишерс, 2011. — 373 с.
2. *Астахов А. М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010. — 312 с.
3. *Арямов А. А.* Общая теория риска: юридический, экономический и психологический анализ: монография. М.: РАП. Валтерс Клуверс, 2010. — 208 с.
4. *А. А. Малюк, В. С. Горбатов, В. И. Королев и др.* Введение в информационную безопасность: Учебное пособие для вузов. М.: Горячая линия — Телеком, 2011. — 288 с.
5. *Носова Н. С.* Конкурентная стратегия компании или маркетинговые методы конкурентной борьбы. М.: ИТК «Дашков и К», 2010. — 255 с.
6. *Рубин Ю. Б.* Теория и практика предпринимательской конкуренции: Учебное пособие. М.: Маркет ДС, 2010. — 604 с.

Д. В. Гуров, В. В. Гуров, М. А. Иванов

ИСПОЛЬЗОВАНИЕ МОДЕЛЕЙ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПРОГРАММНОГО КОМПЛЕКСА

Защищенность — это совокупность свойств программного средства, характеризующая его способность предотвращать несанкционированный доступ (НСД), как случайный, так и умышленный, к программам и данным, а также степень удобства и полноты обнаружения результатов такого доступа или действий по разрушению программ и данных [1]. НСД может быть осуществлен при наличии определенных уязвимостей в программном коде. Во многом понятие защищенности перекликается с понятием надежности программного средства, одним из основных свойств которого является устойчивость к ошибке, т. е. способность поддерживать определенный уровень качества функционирования в случаях программных ошибок или нарушения определенного интерфейса.

Вопросы обеспечения надежности программного обеспечения рассматриваются уже достаточно давно и имеют в своем активе большой набор моделей и методик. В то же время проблема обеспечения защищенности возникла гораздо позже. Поэтому интересно рассмотреть возможность использования моделей надежности ПО применительно к оценке его защищенности. Отладка ПО проводится до тех пор, пока интенсивность появления потока ошибок не снизится до приемлемой для данного применения величины, т. е. среднее время наработки на отказ будет достаточно большим. Поэтому многие модели надежности ориентируются на анализ времени появления очередной ошибки (модель Джелинского—Моранды и др. [2]).

В то же время можно утверждать, что если программа попадет в руки злоумышленника на достаточно продолжительное время, то она будет взломана. Поэтому оценка ее защищенности может проводиться по степени ее стойкости, т. е. по длительности периода, на протяжении которого она противостоит НСД. А этот показатель определяется количеством уязвимостей, оставшихся в программе после этапа ее тестирования. Следовательно, использовать модели