Ключевые вопросы кибербезопасности информации

Т. Ю. Дьякова
Финансовый университет при Правительстве Российской Федерации (Финуниверситет), Financial University
diakovat@mail.ru

***Аннотация*. На сегодняшний день ведущие государства мира и общество в целом все в большей степени полагаются и, соответственно, зависят от беспрепятственного функционирования пятого места - киберпространства, под которым предлагается рассматривать совокупность взаимосвязанных информационных ресурсов, программного обеспечения, баз и банков данных, обрабатываемых в компьютерных сетях и связанной с ними инфраструктуры, вместе с объектами, подпадающих под их контроль и управление. Защита интересов государств и граждан в киберпространстве становится жизненно важной задачей, которая превращает беспрепятственное использование ИТ-сетей на вопросы безопасности и обороны. Потенциальная опасность может угрожать системам государственного и военного управления, экономики и промышленности.**

Ключевые слова: кибербезопасность; системы обеспечения; безопасность предприятий; программирование

I. Введение

Россия интегрирована в мировое киберпространство и соответственно испытывает различные угрозы и негативные воздействий, связанные с его развитием (в частности от последствий соперничества США и ЕС с РФ и КНР), остро актуализирует проблемы кибербезопасности на общегосударственном уровне. Это приводит к необходимости концептуального понимания новой реальности, благоустройство внутреннего нормативно-правового поля, определение полномочий ведомств и организаций, задействованных в обеспечении кибербезопасности государства и решения комплекса проблем, связанных с развитием национальной системы кибербезопасности.

Наиболее эффективным путем решения указанных вопросов является построение национальной модели кибербезопасности и разработка первоочередных направлений деятельности государственного и частного секторов в сфере кибербезопасности.

Цель исследования – изучить модель безопасности функционирования систем информационных.

Задачи:

- Формирование систем информационно-аналитического обеспечения.
- Модель информационной безопасности функционирования систем.

II. Формирование систем информационно-аналитического обеспечения

Информационно-аналитическое обеспечение финансово-экономической безопасности предприятия – это комплексная система, состоящая из управленческих, организационных, технических, действий безопасности и инструментов, основанный на данных оперативного, бухгалтерского, управленческого учета, статистической, производственной и иной информации, направленной на принятие обоснованных управленческих решений для обеспечения развития предприятия.

Ведущие компании в своем составе создают отдельные аналитические подразделения, занимающиеся сбором, обработкой и интерпретацией необходимой информации о внутренней и внешней среде. Однако из-за ограниченности ресурсов украинских предприятий, особенно малых и средних, возникает проблема оценки эффективности и целесообразности функционирования таких систем.

Опыт ведущих компаний показывает, что создание системы информационно-аналитического обеспечения на предприятии сопровождается как определенным увеличением его материальных активов (например, аппаратного обеспечения), так и, в первую очередь, нематериальных активов. Ведь такая система представляет собой комплекс инструментов и средств для получения данных, аналитических методик, организационного подразделения предприятия и также нематериальных ценностей, на которые распространены права собственности. Этот комплекс по истечении определенного периода времени и может приносить прибыль, а также влиять на уровень финансово-экономической безопасности предприятия.

Рассматривая системы информационно-аналитического обеспечения как нематериальный актив предприятия, для ее оценки можно использовать классические для теории экономики предприятий подходы: затратный; сравнительный; оценка на основе доходности; оценка на основе уровня финансово-экономической безопасности.

С позиций предприятия система информационно-аналитического обеспечения позволяет достигать высокий уровень финансово-экономической безопасности, как результат от внедрения и применения информационных ресурсов. Одним из индикаторов эффективности системы

информационно-аналитического обеспечения является коэффициент ее эффективности (ЕИАЗ). Входным потоком для систем являются затраты на ее содержание и функционирование. Исходным потоком системы информационно-аналитического обеспечения является объективная оценка удовлетворенности уровнем финансово-экономической безопасности, то есть результатом ее работы, лицом, принимающим управленческие решения. Подход, согласно которому уровень финансово-экономической безопасности предприятия рассматривается как исходный поток системы информационно-аналитического обеспечения, обусловливает необходимость рассмотрения основных методов оценки финансово-экономической безопасности.

Используется такие методы количественной оценки уровня финансово-экономической безопасности: индикаторный, ресурсно-функциональный, программно-целевой, подход на основе теории экономических рисков.

При построении на предприятии системы информационно-аналитического обеспечения в центре внимания находится генеральная стратегия предприятия - основное направление работы, стратегические цели. Отсюда вытекают основные задачи системы информационно-аналитического обеспечения. Генеральная стратегия оказывает влияние на все фокус-группы – на финансовую зону, в зону мониторинга потребительского сектора, на сам процесс функционирования информационно-аналитической системы и на процессы совершенствования, модернизации и обучения.

Основные задачи системы информационно-аналитического обеспечения финансового блока проявляется в определении финансовых потребностей и финансовых результатов, а также альтернативного выбора источников финансирования с целью минимизации стоимости капитала и максимизации прибыли, обеспечении высокого уровня финансово-экономической безопасности предприятия, подготовке и ведении стратегических финансовых операций.

Информационно-аналитическое обеспечение мониторинга потребительского сектора играет одну из решающих ролей в формировании его взаимосвязей с потребителями, от эффективности которых зависят объемы реализации, прибыли и, как результат, – финансовое состояние предприятия, предоставляет предприятию преимущества, проявляющиеся в повышении конкурентоспособности предприятия и его продукции.

Также особое место имеет информационно-аналитическое обеспечение формирования кадровой политики предприятия с учетом особенностей трудового потенциала предприятия, заключается в обеспечении системы подготовки специалистов в соответствии со спецификой деятельности и направлений развития предприятия; формировании эффективных коммуникаций в процессе управления персоналом; разработке планов и программ развития персонала предприятия.

Все блоки зоны внимания информационно-аналитических систем взаимосвязаны и позволяют учитывать особенности внутренней и внешней среды, сильные и слабые стороны предприятия, есть почва для принятия обоснованных управленческих решений. Выгоды, которые будут получены в результате функционирования системы информационно-аналитического обеспечения и, как следствие, лучше осведомленность управленцев, наиболее заметно, проявляться на уровне финансово-экономической безопасности предприятия.

1. На уровне предприятия ожидаемые эффекты от внедрения системы информационно-аналитического обеспечения можно условно разделить на стратегические и тактические. К стратегическим – относятся те аспекты, влияние которых имеет долгосрочный характер.

2. К тактическим – оперативные эффекты, которые будут заметны в ближайшей, краткосрочный период. Так, к стратегическим можно отнести генерацию новых стратегий, если в результате аналитической работы могут быть выявлены новые рыночные ниши, что позволит получить высокие прибыли в случае переориентации или диверсификации предприятия на эту новую стратегию.

Выводы по целесообразности существующей стратегии – случай, когда в результате исследования будет доказано, что на данный момент эта стратегия является оптимальной и при ее соблюдении будет гарантировано максимальная прибыль при заданных условиях (конъюнктуре рынка). Повышение уровня финансово-экономической безопасности предприятия может иметь как тактические последствия, так и стратегические.

Повышение конкурентоспособности является наиболее общим, комплексным эффектом, который может проявляться как результат всех. Выявление, минимизация и избегания рисков – не самая главная задача системы информационно-аналитического обеспечения на предприятии. Также в тактических эффектах системы информационно-аналитического обеспечения можно отнести следующие: повышение качества информационного оборота – эффект, который позволит значительно эффективнее использовать имеющиеся информационные ресурсы предприятия, а также привлекать новые, и, в возможно короткий срок, внедрять их в информационно-аналитический процесс.

Таким образом, правильно построенная система информационно-аналитического обеспечения позволяет достичь высокого уровня финансово-экономической безопасности предприятия, используя новейшие и учитывая целый ряд факторов, вытекающих из вышеперечисленных эффектов.

Итак, как показывает передовой опыт – использование информационно-аналитического обеспечения финансово-экономической безопасности может иметь преимущества, относиться к разным сферам: маркетинга, менеджмента, текущей производственной, сбытовой деятельности. Спектр положительных эффектов от функционирования

системы информационного обеспечения на предприятии достаточно широким и зависит от отрасли промышленности, специфики предприятия. Он может проявляться в лучшей осведомленности лиц, отвечающих за принятие управленческих решений, как стратегических, так и тактических, оперативных. Это приводит к тому, что повышается конкурентоспособность как предприятия, в частности, и уровень его финансово-экономической безопасности.

III. Модель информационной безопасности функционирования систем

Все более широкое использование в последние 30–40 лет в различных сферах жизнедеятельности общества компьютерных и телекоммуникационных технологий, в том числе Интернет-технологий, вместе с большим количеством преимуществ привнесло также и большое количество угроз. Реализация этих угроз может нанести значительный ущерб как на микро, так и на макроуровне в рамках суверенных государств, а также и в мировом масштабе. Это привело к пониманию необходимости решения проблемы нейтрализации или минимизации этой новой совокупности угроз. Одновременно с этим возникает термин «кибербезопасность».

Считают, что впервые он возник в середине 1990-х годов, когда правительство США стал исследовать эту тему. С того времени прошло достаточно много международных и национальных форумов, конференций, семинаров на различных уровнях, опубликовано много научных работ, посвященных разным аспектам кибербезопасности. Большое количество стран приняли или разрабатывают стратегии кибербезопасности (США, Германия, Франция, Канада и многие другие). В этих условиях актуальной является проблема определения содержания термина «кибернетическая безопасность».

Некоторые ученые считают, что в последнее время термин cybersecurity все чаще и чаще используется, но при этом многие руководители служб безопасности и просто эксперты по информационной безопасности до сих пор путаются в том, когда и как использовать этот термин, поэтому предлагаю проанализировать некоторые из существующих доктринальных и законодательных дефиниций категории, и представляет научный интерес нашего исследования.

Подчеркиваю, что среди ученых отсутствует единое толкование «кибербезопасности», а также на законодательном уровне нет унифицированной дефиниции. Кибербезопасность – это некоторое состояние систем, при котором нейтрализуются угрозы доступности, целостности или конфиденциальности данных, циркулирующих в информационных системах. По моему мнению, данная дефиниция непонятна, прежде всего, из-за отсутствия объяснения, состояние которой именно системы, конечно, можно предполагать, что системы, которая существует в киберпостори, но, в случае науки, нужна конкретика.

Также под «кибербезопасностью» предлагается понимать отдельный случай информационной безопасности, появление которого обусловлено использованием компьютерных систем и / или телекоммуникационных сетей. В таком случае сформулировано определение: кибербезопасность - информационная безопасность в условиях использования компьютерных систем и / или телекоммуникационных сетей. Развернутое определение: кибербезопасность - это такое состояние защищенности жизненно важных интересов личности, общества и государства в условиях использования компьютерных систем и / или телекоммуникационных сетей, при котором минимизируется задачи им вреда через: неполноту, несвоевременности и недостоверность информации, используемой; негативное информационное влияние; негативные последствия функционирования информационных технологий; несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации. То есть, сквозной категорией данной дефиниции является «информация», которая и является основным объектом информационных правоотношений, что могут иметь место в киберпространстве.

Стоит отметить, что среди основных признаков информации выделяют системность, селективность, субстанциональную несамостоятельность, преемственность, неисчерпаемость, массовость, способность трансформироваться, способность к ограничению, универсальность, качество. Развитие национальной системы кибербезопасности должен сопровождаться соответствующими коррективами в процессе реформирования сектора безопасности и обороны. Целью закона является создание национальной системы кибербезопасности как совокупности политических, социальных, экономических и информационных отношений вместе с организационно-административными и технико-технологическими мероприятиями путем комплексного подхода в тесном взаимодействии государственного и частного секторов и гражданского общества.

В Положении о Национальном координационном центре кибербезопасности закреплены его задачи и, среди других, осуществления анализа состояния кибербезопасности и результатов проведения обзора национальной системы кибербезопасности, состояния обеспечения кадрами национальной системы кибербезопасности и подготовка предложений по ее совершенствованию, а вот нормативно-правовой акт, в котором бы объяснялись все аспекты данной системы, до сих пор отсутствует.

Национальная система кибербезопасности как прежде система взаимодействия субъектов кибербезопасности должна объединить спецслужбы, правоохранительные органы, государственные органы, осуществляющие регулирование в сфере информатизации, телекоммуникаций и защиты информации, для своевременного выявления, предупреждения и пресечения киберугроз, устранение предпосылок к их наступлению и минимизации негативных последствий их реализации.

Функционирование указанной системы невозможно без тесного сотрудничества с частным сектором - операторами и провайдерами телекоммуникаций, владельцами и распорядителями критических объектов информационной инфраструктуры государства, компаний, деятельность которых связана со сферой информационной безопасности.

Для обеспечения кибербезопасности чрезвычайно важно понимать угрозы киберпространства.

Угрозы (киберугрозы) – имеющиеся и / или потенциально возможные явления и факторы, создающие опасность жизненно важным интересам человека и гражданина, общества и государства, реализация которых зависит от надлежащего функционирования информационных, телекоммуникационных и информационно-телекоммуникационных систем. При этом можно выделить следующую типологию кибернетических угроз: кибервойна; кибертерроризм; кибершпионажем; киберпреступность.

Поддерживаю мнение по целесообразность выделения в системе кибернетической безопасности Украины следующих основных элементов: общегосударственная система противодействия киберпреступности и кибертерроризма; общегосударственная система кибернетической защиты объектов национальной критической инфраструктуры.

При этом, под общегосударственной системой противодействия киберпреступности и кибертерроризма понимается совокупность специальных субъектов противодействия киберпреступности и кибертерроризма, средств и методов, используемых ими, а также комплекс соответствующих взаимосвязанных правовых, организационных и технических мероприятий, которыми осуществляются. Например, в Европейском Союзе в связи с пониманием важности проблемы кибербезопасности в 2014 году было создано Европейское агентство по сетевой и информационной безопасности, миссией которого является помощь Сообществе в обеспечении особенно высокого уровня сетевой и информационной безопасности; помогать Комиссии, государствам-членам и бизнес-сообществам в выполнении требований сетевой и информационной безопасности, в том числе настоящее и будущее законодательство Сообщества.

Основными задачами агентства является информирование общественности о новых вирусах, атаки хакеров и проблемы с безопасностью информационного пространства Европы, а также расследование эпидемий электронных вирусов и электронных атак. Особо подчеркивается, что ENISA не собирается играть роль киберполицейских, поскольку для силовых операций есть другие структуры, а послужит консультативным органом, оказывает посильную помощь как в задержании преступников, так и в предотвращении совершении преступлений. Агентство планирует разрабатывать и распространять учебные пособия, а также проводить обучение персонала информационным рискам и способам защиты данных. Планируется и проведение научно-исследовательской работы в области защиты информации.

IV. Заключение

Можно сделать вывод, что введение системы информационно-аналитического обеспечения позволяет повысить эффективность работы предприятия в целом.

Подход, согласно которому информационно-аналитическую систему предприятия отнесены к нематериальным активам предоставляет возможности ее оценки за использование классических подходов, выработанных практикой управления предприятиями. Результат рассмотрения эффектов от функционирования системы информационно-аналитического обеспечения доказывает ее чрезвычайную актуальность для предприятия. Построение действенной системы обеспечения кибернетической безопасности требует от государственных органов России четкого определения государственной политики в этой сфере и опережающего реагирования на динамические изменения, происходящие в мире в сфере обеспечения кибернетической безопасности. В системе кибернетической безопасности России целесообразно выделение следующих основных элементов: общегосударственная система противодействия киберпреступности и кибертерроризма; общегосударственная система кибернетической защиты объектов национальной критической инфраструктуры. Развитие национальной системы кибербезопасности должен сопровождаться соответствующими коррективами в процессе реформирования сферы национальной безопасности, а функционирование указанной системы невозможно без тесного сотрудничества с частным сектором.

Список литературы

[1] Айда Т.Ю. Информационные основы внедрения бизнес-разведки на предприятиях / т айда // Вестник Тернопольского национального экономического университета. Тернополь, 2012. Вып. 4. С. 77-83.

[2] Айда Т.Ю. Проблемы измерения эффективности систем информационно-аналитического обеспечения предприятий // Эффективная экономика. 2014. № 9. С. 39-43.

[3] Васильцив Т.Г. Финансово-экономическая безопасность предприятий России: стратегия и механизмы обеспечения: монография / Васильцив Т.Г., Волошин В.И., Бойкевич О.Г., Каркавчук В.В., [под ред. Т.Г. Васильцива]. Львов: Издательство, 2012. 386 с.

[4] Звягин Л.С. Метасистемный подход в современном маркетинге и управлении // Экономика и управление: проблемы, решения. 2018. Т. 5. № 5. С. 151-155.

[5] Звягин Л.С. Методологические подходы имитационного моделирования в рамках управления инновациями и социально-экономическим развитием // Экономика и управление: проблемы, решения. 2018. Т. 6. № 12. С. 4-11.

[6] Звягин Л.С. Методологические подходы имитационного моделирования в рамках управления инновациями и социально-экономическим развитием // Экономика и управление: проблемы, решения. 2018. Т. 6. № 12. С. 4-11.