УДК 364.043.4+338.2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УПРАВЛЕНИИ БИЗНЕСОМ

INFORMATION SECURITY IN BUSINESS MANAGEMENT

Козлов А.Э.
Следственная часть по расследованию организованной преступной деятельности Следственного управления УВД по ВАО ГУ МВД России по г. Москве
Заместитель начальника отдела
Россия, Москва

e-mail: Andrey1988.15@mail.ru
тел.: +7 (919) 767-02-02

Andrew E. Kozlov
The deputy head of Department of Investigative section of investigation organized criminal activity of the Department of Internal Affairs of East administrative district of Ministry of Internal Affairs in Russia Head department in Moscow.
Russia, Moscow

Аннотация

Статья посвящена системе обеспечения информационной безопасности современных предприятий. Рассмотрены требования при выборе наиболее подходящей системы информационной безопасности предприятия, значение оценки информационной безопасности, цели проведения информационной безопасности предприятия и процесс данной оценки. Рассмотрены вопросы влияния информационной безопасности на выполнение стратегических целей и тактических задач организации, финансового и оперативного планирования, а также вопросы необходимости поддержания высокого уровня информационной безопасности на предприятии.

Abstract

The present article is devoted to system of ensuring information security of the modern enterprises. Requirements are considered at a choice of the most suitable information security system of the enterprise, value of an assessment of information security, the purpose of carrying out information security of the enterprise and process of this assessment. The impact of information security on performance of strategic objectives and tactical tasks of the organization, financial and operational planning, and also issues of need to maintain the desirable level of information security at the enterprise are considered.

Ключевые слова: информационная безопасность, защитные меры, внутренние и внешние риски, бизнес-процессы, система обеспечения информационной безопасности

Keywords: information security, protective measures, internal and external risks, business processes

Сложность и противоречивость в хозяйственно-управленческих процессах в РФ за последние два десятка лет потребовали организовать быстродействующие информационные технологии для того, чтобы обеспечить высокую степень устойчивости производства, управления системами безопасности национального богатства и экономики. Информация стала глобальным продуктом, товаром, в качестве эквивалента которого выступают качественная информация и натуральные композиты компьютерных систем. Это объясняет причину, по которой закон возвышения потребностей в данной ситуации работает, как никогда точно и разрушает постулат о тенденциях нормы прибыли к понижению.

В качестве нового рабочего класса выступают – информационщики, которые используют в своей деятельности гибкие технологии, что способствует замене грубых силовых методик воздействия на производство, обмену, распределению и потреблению продуктов потребительской корзины и информации на контрольно-координационные. Мировое сообщество вместе со своими региональными альянсами стали испытывать информационное оружие для того, чтобы, как можно точнее оказать воздействие на человека до момента блокирования его энергетики. На фоне этого разные структуры управления бизнесом не способны быстро приспособиться к системе диверсий и помех при помощи электронно-вычислительных машин (ЭВМ), поэтому они практически в равной мере зависят от влияния «информационного оружия».

Российской Федерации, в отличие от ряда других государств, повезло в том смысле, что в процессе управления бизнесом не имеется каких-то явных противоречий, несмотря на то, что такие доминанты, как Япония и КНР, ощущаются практически повсеместно.

На данный момент имеется множество нюансов, оказывающих влияние на степень эффективности системы маркетинговой информационной безопасности (СМИБ). Разделы безопасности и риск-менеджмента включают в себя организационную безопасность, управление активами, физическую безопасность, безопасность персонала, функционирования и коммуникаций, а также разработку и закупку информационных технологий, что может способствовать обеспечению непрерывности в бизнес-процессе. К примеру, подразделы управления доступом – это доступ на пользовательском уровне, на уровне сетевой инфраструктуры, на уровне компонентов операционной системы. При этом доступ на уровне сетевой инфраструктуры может состоять из политики сетевого доступа, аутентификации пользователей, удаленной диагностики, управлением сетевыми соединениями, управлением маршрутизацией в сети и пр.

Большое количество компонентов, у каждого из которых будут иметься собственные особенности, способны привести к возникновению существенных сложностей. Для избежания этого, существует необходимость разработки структуры, которая будет определять вопросы, которые потребуют решения, что можно сделать при помощи СМИБ.

Предприятия, бизнес которых находится в прямой зависимости от информационной сферы, для того, чтобы достичь собственных бизнес-целей должны поддержать систему обеспечения информационной безопасности (СОИБ) на высоком уровне. СОИБ представлена в качестве совокупности аппаратно-программных, организационных и технических защитных мер, которые функционируют под управлением СМИБ, а также процессов, направленных на поддержку деятельности по менеджменту информационной безопасности (ИБ).

Желание обладать СОИБ, которая бы соответствовала и обеспечивала выполнение целей ИБ, обеспечивая при этом доступность, конфиденциальность и целостность информационных активов, приведет к необходимости совершенствования СОИБ, которое будет возможно лишь при условии знания состояний характеристики, а также параметров, используемых защитных мер, процессов менеджмента и осознания степени соответствия ИБ планируемым результатам.

Для понимания данных аспектов необходимо воспользоваться результатами ИБ предприятия, которые были получены за счет модели оценки ИБ на базе свидетельств оценки, а также оценочных критериев, учитывая контекст оценки.

Под критериями оценки понимается то, что позволит устанавливать значение оценки для ее объекта. В виде критериев оценки ИБ могут быть использованы требования и процедуры ИБ, наряду с сочетанием уровня инвестиций и затрат на ИБ.

Записи, изложение фактов и прочая информация, относящаяся к критериям оценки ИБ, выступают в качестве свидетельств информационной безопасности и могут быть проверены. Ими могут быть доказательства выполняемой или уже выполненной деятельности, связанной с обеспечением информационной безопасности в качестве нормативных, распорядительных, отчетных документов, а также результатов от наблюдений и опросов.

В контексте оценки ИБ объединены назначение и цели оценки, ее вид (самооценка или независимая оценка), а также объект и основные области ИБ, ограничения ее роли.

В общем виде оценка информационной безопасности может быть представлена в качестве основных компонентов данного процесса (рис. 1): контекст, критерии и модель оценки, свидетельства – все то, что является необходимым для реализации оценочного процесса.

Суть оценки ИБ состоит в том, чтобы выработать оценочное суждение касательно пригодности процессов обеспечения ИБ, вместе с адекватностью использованных защитных мер и целесообразности затрат, инвестиций для того, чтобы обеспечить необходимый уровень информационной безопасности на основании измерения и оценки критических элементов объекта оценки [1].

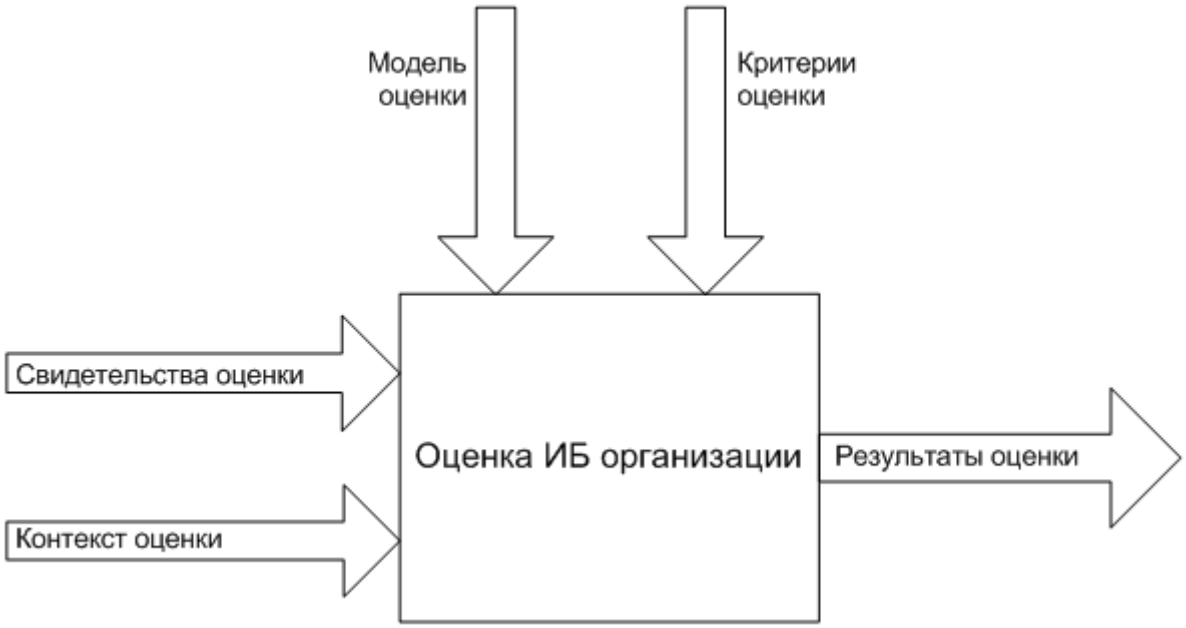

Рисунок 1 – Общий вид процесса оценки ИБ организации

Вместе с важным назначением оценки информационной безопасности, представленным в качестве создания информационной потребности для того, чтобы совершенствовать ИБ, существуют и другие цели проведения оценки информационной безопасности [2]:

1. Определить степень соответствия установленным критериям в отдельных областях обеспечения информационной безопасности, а также обеспечить защитные меры ИБ.

2. Выявить влияние критических элементов, а также их сочетание с ИБ предприятия.

3. Сравнить «зрелость» разных процессов обеспечения, а также разные защитные меры установленным требованиям.

Полученные результаты оценки информационной безопасности могут быть использованы заинтересованными лицами для того, чтобы сравнить уровень информационной безопасности предприятий в одной бизнес-сфере и в сопоставимом масштабе.

Несмотря на то, что системы управления информационной безопасностью на данном этапе получили широкое развитие, многие из них не являются

совершенными, что можно выявить в ходе оценки. При выборе наиболее подходящей системы безопасности, необходимо учитывать ряд требований и руководствоваться лучшими мировыми стандартами и практикой.

Система информационной безопасности должна охватывать все предприятие, все его горизонтальные, вертикальные и кросс-функциональные организационные структуры, куда входят люди, производства, товары, политики, процедуры, технологии, сети, системы и информация.

Информационная безопасность современного предприятия должна быть рассмотрена в качестве основного бизнес-требования, которое будет оказывать непосредственное влияние на выполнение стратегических целей, тактических задач, планов управления рисками и соблюдение требований регуляторов. Каждый менеджер должен понимать, почему информационная безопасность – это важное условие для существования бизнеса.

Информационная безопасность в современном мире – это стоимость ведения инвестиций и бизнеса, но не расход или произвольная бюджетная статья. Политику информационной безопасности разрабатывают на верхнем управленческом уровне, а значит, у сотрудников нет права на то, чтобы в одностороннем порядке принять решение а том, сколько именно информационной безопасности им необходимо. При этом гибкие исключения из правил позволят выполнять нужные для бизнеса процессы, а руководство будет обеспечено средствами для своевременного контроля.

Информационная безопасность должна быть обеспечена с учетом рисков, поскольку, оценка уровня защищенности основывается на расчете допустимой степени информационного риска, вместе с рисками нарушения требования регуляторов, сбоями в текущей работе, а также репутационным ущербом и финансовыми потерями.

Кроме того, существует необходимость изучения влияния, как внутренних, так и внешних рисков на основании чего будут пересчитаны при необходимости допустимые уровни информационной безопасности.

Важная роль отводится определению зон ответственности, ведь, на руководящих должностях в области информационной безопасности назначается квалифицированной персонал. У каждой должности существуют собственные четко ограниченные обязательства и отчетность.

Важным требованием со стороны бизнеса также является гибкость и современность политики информационной безопасности. Это легко объяснить за счет того, что требования к информационной безопасности должны точно и четко реализовываться именно за счет грамотно сформулированной политики информационной безопасности, которая будет поддерживаться со стороны персонала. Кроме того, она должна быть обеспечена за счет организационных и технических мероприятий [5].

Соблюдение требования достаточного финансирования и выделения средств для информационной безопасности вряд ли когда-то потеряет свою актуальность. ИБ должна находиться в требуемом состоянии, ведь, как известно для принятия управленческого решения важно иметь как можно больше достоверной информации о внешней и внутренней среде конкурентов, деловых партнеров и всевозможных теневых процессах. Любой хозяйствующий субъект окружен различными факторами риска, способными в один момент превратить ни во что материальные и финансовые ресурсы. При условии, что средства информационной безопасности не будут поддерживаться в требуемом состоянии, не будут обновляться, такие риски будут возрастать. Поэтому любой современный бизнесмен должен четко осознавать, что существует необходимость осуществления адекватного и устойчивого финансирования и выделения ресурсов на информационную безопасность.

Нельзя не коснуться и вопроса о безопасности жизненного цикла программного обеспечения. Как известно, предъявляемые к безопасности требования будут выполняться на протяжении всего жизненного цикла программного обеспечения, начиная от его приобретения, включая процесс проектирования, разработки, тестирования, эксплуатации, технического обслуживания и логически заканчивая списанием [5].

Безопасность – это неотъемлемая часть стратегического, финансового и оперативного планирования. В области информационной безопасности у компаний имеются достижимые, измеримые цели, интегрированные в стратегические и оперативные планы. Реализация данных целей должна контролироваться с использованием метрик. Аудит существующих планов позволит определить слабые места системы информационной безопасности, требования непрерывности бизнес-процессов и выполнение запланированного.

Уровень информационной безопасности бизнеса – это один из главных показателей работы менеджеров, поэтому его всегда следует учитывать при запуске новых проектов, во взаимоотношениях с другими участниками рынка, а также в ходе текущего управления проектами.

Кроме того для обеспечения высокого уровня информационной безопасности необходимо проводить регулярный аудит, а в случае необходимости даже пересмотреть корпоративную систему информационной безопасности, что позволит поддерживать желаемый уровень информационной безопасности на предприятии.

Список использованной литературы:

1. Асаул, А.Н. Организация предпринимательской деятельности / А.Н. Асаул. – М. 2012.
2. Грязнов, Е.С. Безопасность локальных сетей / Е.С. Грязнов, С.А. Панасенко. – М. : Вузовский учебник, 2012.
3. Козлачков, П.С. Основные направления развития систем информационной безопасности / П.С. Козлачков. – М.: финансы и статистика, 2013.
4. Леваков, Г.Н. Анатомия информационной безопасности / Г.Н. Леваков. – М. : ТК Велби, издательство Проспект, 2011. – 256 с.
5. Концепция информационной безопасности Российской Федерации [Электронный ресурс]. – Режим доступа. – URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/4d900a096c2bf5b9c325763f0045a87f (дата обращения 25.05.2014).