УДК 330.368

08.00.00 Экономические науки

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННОГО ПРЕДПРИЯТИЯ *

Хрусталёв Евгений Юрьевич
доктор экономических наук, профессор,
заведующий лабораторией
e-mail: stalev@cemi.rssi.ru

Елизарова Марианна Иоановна
кандидат экономических наук, старший
научный сотрудник
e-mail: melizarova@forecast.ru
Центральный экономико-математический институт РАН, 117418 Москва, Нахимовский проспект, 47

В связи с информатизацией производственной, научно-технической, социальной и общественной деятельности, становлением цифровой экономики возникает необходимость в эффективной защите секретных и конфиденциальных данных. Решение проблемы создания системы информационной безопасности становится особо актуальной и значимой, поскольку с появлением сложных автоматизированных информационных систем значительно выросли объемы сведений, хранящихся в устройствах вычислительной техники, в единых базах данных стала интегрироваться информация различного назначения, значительно расширилось число пользователей, имеющих доступ к информационным ресурсам предприятия. В статье предложены и научно обоснованы концептуальные основы и принципы построения современной системы, защищающей информационные массивы производственного предприятия, которые составляют коммерческую тайну, от порчи и несанкционированного доступа. Выявлены информационные сведения, требующие защиты от конкурентов и злоумышленников, определена инфраструктура их защиты и механизмы собственного надежного функционирования защитных систем. Показано, что объектами, подлежащими защите от потенциальных внутренних и внешних угроз и противоправных действий, являются: персонал, материальные,

UDC 330.368

Economic sciences

CONCEPTUAL FOUNDATIONS FORMATION OF INFORMATION SECURITY SYSTEM FOR A PRODUCTION ENTERPRISE

Khrustalev Evgenii Yurievich
Doctor of Economical sciences, professor,
head of the laboratory
e-mail: stalev@cemi.rssi.ru

Elizarova Marianna Ioanovna
Candidate of economical sciences, senior researcher
e-mail: melizarova@forecast.ru
Central Economics and Mathematics Institute RAS, Moscow, Russia

In connection with the informatization of production, scientific-technical, social and public activities, the emergence of the digital economy, there is a need to protect effectively sensitive and confidential data. The solution to the problem of creation of system of information security becomes particularly relevant and significant, since with the advent of complex automated information systems significantly increased the quantity of information stored in the computing device, in single databases have become integrated information for various purposes, greatly expanded the number of users having access to the information resources of the enterprise. In the article, we have proposed and scientifically based conceptual foundation and principles of construction of modern system of protecting information files to manufacturing enterprises, which constitute commercial secret, from damage and unauthorized access. We have identified the information that requires protection from competitors and intruders, identified infrastructure their protection and the mechanisms for their own reliable operation of protective systems. It is shown that the objects to be protected from potential internal and external threats and illegal acts are staff, material, financial and intellectual resources, means and systems of informatization and protection of all types of resources. The basic principles of information security production of the enterprise are the mutual responsibility of management and staff, legitimacy, cooperation with law enforcement bodies, maintenance of optimum balance of interests of the company and the individual

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований, проект № 15-06-00702-а «Формирование методологии экономической безопасности наукоемких и высокотехнологичных производств и инструментария для ее оценки и мониторинга»

финансовые и интеллектуальные ресурсы, средства и системы информатизации и охраны всех видов ресурсов. Основными принципами обеспечения информационной безопасности производственного предприятия являются взаимная ответственность руководства и персонала, законность, взаимодействие с правоохранительными органами, соблюдение оптимального баланса интересов предприятия и личности

Ключевые слова: ИНФОРМАЦИЯ, КОНЦЕПЦИЯ, БЕЗОПАСНОСТЬ, НАУКОЕМКОЕ ПРЕДПРИЯТИЕ, КОМПЛЕКСНАЯ ЗАЩИТА, ИНФОРМАЦИОННАЯ СИСТЕМА, ОРГАНИЗАЦИОННОЕ, ПРАВОВОЕ И ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, КОММЕРЧЕСКАЯ ТАЙНА, ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

Keywords: INFORMATION, CONCEPT, SECURITY, HIGH-TECH ENTERPRISE, COMPREHENSIVE PROTECTION, INFORMATION SYSTEM, INSTITUTIONAL, LEGAL AND TECHNICAL SUPPORT, TRADE SECRETS, INTELLECTUAL PROPERTY

Doi: 10.21515/1990-4665-130-007

Введение. Процессы информатизации охватили практически все страны, вышедшие на постиндустриальный этап развития, который характеризуется возрастающей ролью информации в жизни общества. На этом этапе главным ресурсом все чаще вместо вещества, энергии, капитала становится информация. Успех производственной и предпринимательской деятельности, экономическая мощь развитых государств в значительной мере стали зависеть от умения эффективно распоряжаться таким ценнейшим стратегическим ресурсом, в какой превратилась информация [3,7].

Как известно, ресурсами считаются элементы экономического потенциала, которыми располагает общество и которые используются для достижения конкретных целей хозяйственного и социального развития. Назначение традиционных видов ресурсов (материальные, финансовые, трудовые, природные и другие) и способы их применения вполне понятны. Под информационными ресурсами понимаются документы и их массивы в различных формах и видах, содержащие сведения по всем направлениям общественной деятельности. Поэтому собственность современного

предприятия – это не только машины, оборудование, сырье и т.д., но и идеи, концепции, знания, технологии (интеллектуальный потенциал), т.е. все то, что превращается в товары и услуги, направляемые на удовлетворение материальных и духовных потребностей населения.

Важнейшей характеристикой информации считается ее ценность (полезность), которая, как правило, определяется ее владельцем. Несмотря на многочисленные попытки формализовать этот процесс с помощью различных методов теории информации и исследований операций, процедура оценки пока остается достаточно субъективной. В зависимости от этой характеристики собственник решает, нужно ли держать информацию в тайне от конкурентов и как защищать ее от всевозможных посягательств. При этом важным критерием при выборе защитных средств выступает прибыль (реальная или потенциальная), приносимая используемой информацией. Для владельца ценность должна соизмеряться со стоимостью процесса защиты информации, а для конкурентов – компенсировать затраты на ее получение.

Другой значимой характеристикой информации представляется ее важность. По уровню важности можно предложить следующее распределение информации по категориям [1]:

- принципиально важная (незаменимая), наличие которой необходимо для функционирования предприятия;

- важная, которая может быть заменена или восстановлена, но эти процессы трудоемки и связаны с большими затратами;

- полезная, которую трудно восстановить, но предприятие может эффективно функционировать и без нее;

- несущественная, которая больше не нужна предприятию.

На практике процедура отнесения информации к одной из перечисленных категорий представляется достаточно сложной задачей, поскольку одна и та же информация может использоваться многими

подразделениями предприятия, каждое из которых по-разному определяет категорию важности этой информации. Категория важности, как и ценность, изменяется со временем и зависит от отношения к ней различных категорий потребителей.

На основании анализа ценности и важности определяются информационные массивы, которые составляют секреты предприятия – производственную и коммерческую тайну. Сведения из этих массивов сознательно скрываются от посторонних, поскольку они определяют истинное социально-экономическое и научно-техническое состояние предприятия.

Информационные сведения, требующие защиты. Для выявления сведений, требующих защиты, необходимо четко представлять виды информации, составляющие государственную, производственную и коммерческую тайну. В связи с тем, что вопросу зашиты государственной тайны достаточно подробно и системно рассмотрены, в рамках данной статьи внимание целесообразно сконцентрировать на информации, закрытой в интересах отдельных хозяйствующих субъектов.

Согласно существующему законодательству к производственной тайне относятся сведения технического, экономического и организационного характера, которые зависят от способа производства, технологии, организации труда, а также технологические открытия, изобретения, информация о целях и характере исследовательских работ.

Коммерческой тайной являются сведения, относящиеся к торгово-финансовой сфере деятельности предприятия. Эти сведения можно сгруппировать по тематическому принципу и с учетом отличительных особенностей каждого конкретного предприятия условно представить в виде следующего перечня:

- финансовые документы (прибыль, фонд заработной платы, финансовые отчеты и прогнозы, банковские счета и т.п.);

- информация о рынках сбыта (история, объем, тенденции производства, стратегия цен и маркетинг, планы и рыночная политика, реклама, политика и методы сбыта т.п.);

- данные о производстве и продукции (производственные мощности, номенклатура изделий, технические спецификации перспективной и существующей продукции, технический уровень и сроки создания разрабатываемых изделий и т.п.);

- сведения о поставщиках и потребителях.

Рыночные отношения способствуют усилению конкуренции не только в сфере международной торговли, но и между отдельными предприятиями, производящими однотипную продукцию. Поэтому несанкционированный доступ и использование информации, не предназначенной для распространения, уже сейчас наносит многим предприятиям значительный ущерб.

Проводимые за рубежом и российскими научно-производственными коллективами исследования убедительно показывают, что для предприятий различной формы собственности весьма актуальной и значимой становится проблема защиты информации, представляющей интерес для конкурентов или иных лиц, которые способны использовать ее в своих целях.

В условиях административно-планового народного хозяйства на предприятиях существовала хорошо организованная и эффективно действующая система охраны государственных секретов. Однако вместе с тоталитаризмом она была разрушена. Становление и развитие новых форм собственности, обвальная приватизация, направленная на разгосударствление экономики, ряд других обстоятельств привели к смене владельцев многих предприятий. К руководству пришли люди, слабо представляющие особенности рыночного производства и, в том числе, не сразу осознавшие необходимость охраны общественных и собственных

секретов. Практика функционирования экономики в переходных условиях заставила обратить самое серьезное внимание на проблемы национальной безопасности [4,10], в частности, на обеспечение безопасности в информационной сфере [2,5,9].

Прежде, чем перейти к рассмотрению собственно проблем информационной безопасности, напомним, что традиционно информационная система (ИС) определяется как организационно упорядоченная совокупность технических средств, информационных ресурсов и технологий, реализующих информационные процессы в ручном или автоматизированном режимах в целях полного, точного и оперативного удовлетворения информационных потребностей пользователей.

С появлением сложных автоматизированных информационных систем проблема обеспечения защиты информации от несанкционированного доступа становится все более актуальной по ряду причин, основными среди которых можно считать следующие [8,11,12]:

- значительный рост объемов сведений, накапливаемых, обрабатываемых и распространяемых с помощью средств и устройств вычислительной техники;

- интеграция в единых базах и банках данных сведений различного назначения;

- расширение категорий пользователей, имеющих доступ к информационным ресурсам автоматизированных систем;

- усложнение режимов работы технических средств, образующих сложные вычислительные системы (внедрение многопрограммных и многопроцессорных режимов, разделения времени и т.п.);

- увеличение количества внешних устройств и программно-технических связей в автоматизированных информационных системах.

Обеспечение безопасности ИС – это меры, предохраняющие систему от преднамеренного или случайного вмешательства в режимы ее работы. Следует подчеркнуть, что в политике информационной безопасности нет мелочей, т.к. ни одна система не является абсолютно безопасной. Не существует единого универсального решения, обеспечивающего абсолютную защиту ИС, поэтому следует адаптировать существующие методы и средства в зависимости от реальных и потенциальных угроз, размеров возможного ущерба и расходов на обеспечение приемлемой безопасности.

Необходимо отметить, что к числу особо сложных компонентов ИС любой природы относятся люди (сотрудники, продавцы, партнеры, клиенты, и т.д.), являющиеся главными источниками информации. Поэтому работа с кадрами – важнейшее направление деятельности по обеспечению сохранности конфиденциальной информации и защиты ее от несанкционированного доступа. Необходимо изучать весь состав работающих на предприятии специалистов, выделяя при этом тех, кто имеет доступ к особо ценной и важной информации. Особые категории работников – это кандидаты на вакантные должности и на увольнение. Эти люди, в большей мере, чем остальные, склонны к противоправным действиям, особенно последние. Объектом повышенной заботы должен быть персонал, осуществляющий сбыт продукции и обслуживающий запросы клиентов о возможностях улучшенных или новых моделей, планируемых к реализации. Сообщая дополнительную информацию о разрабатываемых изделиях, такие специалисты могут разгласить сведения, составляющие производственную или коммерческую тайну.

Основные положения безопасности ИС. В настоящее время сложились вполне конкретные концепции и инфраструктура защиты информации, базовыми элементами которой являются:

развитый арсенал технических и аппаратных средств защиты, создаваемых на промышленной основе;

большое количество фирм, специализирующихся на решении проблем защиты информации;

четко определенная концептуальная система взглядов на информационную безопасность.

Обширный практический опыт свидетельствует о том, что:

процесс обеспечения надежной безопасности ИС должен быть многоразовым актом, постоянно и непрерывно совершенствующийся во времени;

информационная безопасность обеспечивается только при комплексном и системном использовании всех имеющихся средств и методов защиты во всех производственных структурных элементах и на каждом технологическом этапе процедуры обработки информации и изготовления продукции;

функционирование механизмов защиты должно постоянно контролироваться, дополняться и обновляться в зависимости от изменения внутренних и внешних условий, с учетом возможных угроз различного происхождения;

без профессионального обучения пользователей и без надлежащего соблюдения ими всех установленных правил и требований сохранения конфиденциальности невозможно обеспечить требуемый уровень безопасности.

В соответствии с принципами системного подхода процесс информационной защиты должен быть:

постоянным (злоумышленники постоянно ищут малейшую возможность для того, что обойти защиту);

плановым (планирование выполняется разработкой каждым подразделением подробных планов защиты, учитывающих главную цель предприятия в целом);

централизованным (организационно-функциональная самостоятельность процедуры обеспечения безопасности должна осуществляться в рамках определенной структуры);

конкретным (защищать следует конкретные данные, потеря которых может причинить организации серьезный ущерб);

активным (информационная защита должна осуществляться целеустремленно и настойчиво);

надежным (перекрываться должны все возможные каналы и способы утечки);

целенаправленным (защищается не все подряд, а только информация, используемая в рамках некоторой конкретной цели);

универсальным (необходимо ограничиваться разумными и достаточными средствами, по возможности расширяя их возможности для решения возникающих задач);

комплексным (необходимо в полном объеме применять все виды, формы и методы обеспечения безопасности).

Система информационной безопасности (СИБ) способна снижать инвестиционные и инновационные риски предприятия [14] и должна удовлетворять следующим основным условиям, в частности:

охватывать весь технический и технологический процесс информационной деятельности каждого предприятия;

позволять проведение дополнений и изменений мер обеспечения информационной безопасности;

быть разнообразной по применяемым средствам и методам, многоуровневой с различной последовательностью доступа к информации:

быть нестандартной, оригинальной в реализации возможностей защиты;

быть удобной для технического обслуживания и простой для эксплуатации непрофессиональными пользователями.

К СИБ предъявляются следующие дополнительные требования:

четкое определение полномочий и прав пользователей к доступу на работу с определенными видами информации;

предоставление каждому пользователю минимальных инструментальных полномочий, позволяющих ему выполнить порученные работы;

сведение к минимуму количества общих для разных пользователей средств и методов защиты;

учет все попыток и случаев несанкционированного доступа к защищенной конфиденциальной информации;

обеспечение контроля за состоянием средств защиты информации и немедленное реагирование в случае выхода их из строя;

обеспечение качественной и количественной оценки уровня конфиденциальности информации.

СИБ обязана иметь надежные механизмы собственного обеспечения, на основе которых она сможет успешно и эффективно выполнить свое предназначение, в частности, в системе должны быть предусмотрены:

правовое обеспечение (правовые документы, нормативные акты, инструкции, руководства и т.п., требования, выполнение которых обязательно в рамках области их действия);

организационное обеспечение (осуществление информационной безопасности выполняется определенными структурными подразделениями, такими, как, например, служба безопасности предприятия);

информационное обеспечение (сведения, показатели, данные, параметры, используемые при решении основных задач, обеспечивающих успешное функционирование СИБ);

техническое обеспечение (аппаратные средства, предназначенные не только для защиты информации, но и для осуществления эффективной деятельности СИБ);

математическое обеспечение (методы, используемые для расчетов, позволяющих оценить опасность используемых злоумышленниками разведывательных технических средств, норм и зон необходимой защиты);

программное обеспечение (информационные, учетные, математические, статистические, когнитивные и расчетные программы, обеспечивающие оценку опасности и наличия методов несанкционированного доступа к информации и различных каналов ее утечки);

лингвистическое обеспечение (комплекс специальных языковых инструментов общения пользователей и специалистов в сфере обеспечения информационной безопасности);

нормативно-методическое и регламентное обеспечение (нормы и регламенты, формализующие деятельности органов, средств, служб, реализующих основные функции защиты информации, методики, обеспечивающие надлежащими правилами деятельность пользователей при работе с закрытой и конфиденциальной информацией).

Основной целью СИБ является предотвращение ущерба ИС и интересам отдельного предприятия, наносимому за счет хищения материально-технических и финансовых средств, нарушения процесса функционирования технических средств ИС, уничтожения ценностей и имущества, разглашения, утраты, уничтожения, утечки, искажения информации, а также физическая защита персонала [6]. Для этого СИБ должна обеспечить: защиту прав предприятия, всех его подразделений и

работающих на нем сотрудников, эффективное использование и сохранность материальных, информационных и финансовых ресурсов; повышение престижа и рост прибылей за счет обеспечения высокого качества услуг по безопасности поставщиков, партнеров и клиентов.

Основными задачами, решаемыми СИБ являются:

выявление и нейтрализация угроз безопасности, условий, причин и прочих обстоятельств, способствующих нанесению серьезного ущерба интересам предприятия, нарушению его прогрессивного инновационного развития и нормального функционирования;

отнесение информации к различным категориям ограниченного использования и доступа, к различным уровням опасности (уязвимости) и подлежащих соответствующей ситуации защите;

создание условий и методов оперативного реагирование на появляющиеся угрозы безопасности, приводящие к негативным явлениям в функционировании предприятия;

эффективное и быстрое пресечение посягательств на ресурсы предприятия и угроз персоналу;

разработка и реализация механизмов, обеспечивающих быструю локализацию опасных зон вмешательства в деятельность предприятия и максимального возмещения наносимого ущерба, ослабление негативных последствий на процесс достижения целей предприятия, возникающих вследствие нарушения безопасности.

Объектами, подлежащими защите от потенциальных внутренних и внешних угроз и противоправных действий, являются: персонал, материальные, финансовые, интеллектуальные и информационные ресурсы, средства и системы информатизации и охраны всех видов ресурсов.

Основными задачами обеспечения безопасности и надежной защиты информационных ресурсов являются:

осуществление закрытой переписки и шифровальной связи;

построение и практическая реализация системы, разрешающей работу исполнителей со сведениями и документами ограниченного доступа;

планирование и координация работ по обеспечению защиты информации, накапливаемой, систематизируемой, обрабатываемой и распространяемой средствами ИС;

обеспечение безопасности в ходе проведения конфиденциальных переговоров, совещаний и деловых встреч;

осуществление действенного контроля за сохранностью закрытых и конфиденциальных документов, за обеспечением эффективной защиты информации, собираемой и обрабатываемой средствами ИС;

организация учета, хранения и использования конфиденциальных документов и их носителей.

Основными принципами обеспечения информационной безопасности являются взаимная ответственность руководства и персонала предприятия, законность, достаточность, взаимодействие с государственными и частными правоохранительными органами, соблюдение оптимального баланса интересов предприятия и личности.

Основными направлениями обеспечения безопасности информации выступают инженерно-техническое, организационное м правовое обеспечение.

Правовое обеспечение безопасности ИС. В настоящее время вопрос о правовом обеспечении процессов информатизации активно прорабатывается как в законотворческом, так и в практическом плане. В качестве предметов правового регулирования должны рассматриваться:

правовой режим информации, средств и индустрии информатизации и систем информационных услуг, средства и формы защиты информации;

правовой статус каждого участника правоотношений в процессах производственной и социально-экономической информатизации (определение права на информацию, гарантий и защиты прав и установления ответственности в зависимости от ролей субъектов);

порядок взаимоотношений всех субъектов, участвующих в информатизации, с учетом их изменяющегося правового статуса на всех уровнях и на различных стадиях процесса функционирования ИС.

Особое значение приобретают проблемы:

экономики информатизации – выработка правовых методов и механизмов информационного обеспечения предприятия, распределения, анализа, обмена, потребления и надежной защиты информационных ресурсов;

информационной безопасности – надлежащая защита общества и личности от отрицательных последствий процессов информатизации, обеспечение правопорядка отношений в области информатизации;

информационной метрологии, стандартизации, нормативное закрепление понятийного и терминологического аппарата в области информатизации.

Законодательство, определяющее и регламентирующее информационную безопасность, является неотъемлемой частью российских законов, в том числе:

конституциональное законодательство;

общие основополагающие законы (о собственности, о налогах, правах и т.д.);

законы, связанные с организацией управления отдельными хозяйствующими структурами, с экономикой, с финансами, с государственными органам и системой, определяющей их статус;

правоохранительное законодательство;

специальные законы, относящиеся к конкретным областям отношений, процессам, отраслям хозяйства и производственным комплексам;

подзаконные и другие нормативные акты, связанные с процессами информатизации.

К правовому обеспечению следует отнести такие документы как составление трудовых договоров на проведение производственных и других работ, в том числе и по оказанию различных информационных услуг. При этом правовая гарантия определяется предусмотренными условиями ответственности в случае нарушения сторонами взятых на себя обязательств.

Стороны могут также прибегнуть к страхованию убытков. В договоре определяют, какая сторона должна заключить соответствующий договор со страховой кампанией. Обычно, страхование осуществляет исполнитель, но в этом случае страховая сумма включается в цену выполняемых работ.

Организационное обеспечение безопасности ИС. Совокупность действий или процессов, ведущих к возникновению и совершенствованию взаимоотношений (взаимосвязей) между отдельными частями единого целого, принято считать организационными мероприятиями.

К организационным мероприятиям следует отнести:

специальные действия, выполняемые при проектировании, строительстве и обустройстве производственных зданий и помещений;

подбор персонала, обучение его основам, правилам и методам работы с конфиденциальной информацией, ознакомление с ответственностью, предусмотренной за нарушение правили требований защиты информации и т.д.;

организация, поддержание и совершенствование надежного контроля за действиями посетителей и пропускного режима;

организация надежной охраны территорий и помещений;

организация использования носителей и документов конфиденциальной информации и их хранения, включая порядок учета, выдачи, исполнения и возвращения;

назначение ответственного за защиту информации, проведение систематического контроля за персоналом, работающим с конфиденциальной информаций и т.д.

Одним из основных направлений организационных мероприятий является четкая организация системы делопроизводства и документооборота. Основным организационным мероприятием является разработка перечня охраняемых сведений и проведения аттестации помещений на предмет выработки конкретных мер по защите и обеспечению безопасности конфиденциальной информации.

Важным мероприятием представляется создание на предприятии собственной службы безопасности – системы штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации. Эффективность обеспечения экономической [13] и, в частности, информационной безопасности предприятия может быть наивысшей, если работа в службе безопасности будет престижной и высоко оплачиваемой.

Интересна практика защиты информации в США. Кратко рассмотрим методологию системного подхода к организации и функционированию системы защиты конфиденциальной информации, названной методом Operation Security («Opsec»). Метод универсальный и может быть использован как для защиты технологической и коммерческой тайны, так и для обеспечения сохранности государственных секретов. Суть метода состоит в том, чтобы предотвратить, пресечь или ограничить доступ к той части информации, которая позволит конкуренту «вычислить» или узнать, какой новый инновационный товар планирует

произвести предприятие, чтобы опередить его на рынке, создав аналогичную продукцию раньше и дешевле.

Процесс защиты информации по данному методу проходит поэтапно:

начальный этап (анализ и изучение объекта защиты) заключается в определении, что следует защищать (какие виды информации требуют защиты, наиболее значимые элементы защищаемой информации, определяется жизненный цикл критической информации и т.д.);

на втором этапе осуществляется выявление потенциальных угроз (выявляется, кого может заинтересовать защищаемая информация, изучаются методы, которые используют конкуренты для ее получения, оцениваются возможные каналы утечки информации, разрабатывается система мероприятий по пресечению действий конкурентов);

на третьем этапе определяется эффективность подготовленных и постоянно действующих подсистем обеспечения безопасности;

на четвертом этапе принимаются дополнительные необходимые средства и меры по обеспечению информационной безопасности;

на пятом этапе руководителями организации изучают и оценивают представленные рекомендации для осуществления предложенных мер безопасности, выполняют расчет их стоимости и эффективности;

на шестом этапе осуществляется реализация одобренных мер безопасности в соответствии с установленными приоритетами;

заключительный этап предусмотрен для проведения контроля и доведения до персонала предприятия мер безопасности, принятых к реализации.

Для практического внедрения данного метода необходимо участие команды аналитиков, являющихся высококвалифицированными специалистами не только в области информатики, но и в тех научных областях, знания из которых используются при выполнения аналитических

исследований. Организация аналитической работы включает три основных направления: о рынке, о производстве и продукции, об организационных особенностях и финансах.

Инженерно-техническое и технологическое обеспечение безопасности ИС предприятия. Инженерно-техническая и технологическая защита – это совокупность технических средств и специальных органов, а также организационных мероприятий по их комплексному использованию в интересах обеспечения безопасности предприятия. По функциональному назначению инженерно-техническая и технологическая защита использует следующие средства:

физические, которые включают различные инженерные сооружения и средства, препятствующие проникновению злоумышленников на защищаемые объекты и осуществляющие защиту информации, материальных средств, персонала, и финансов от противоправных действий;

аппаратные, в число которых входят приборы, приспособления, устройства, а также разнообразные технические решения, начиная от телефонного аппарата и кончая самыми современными автоматизированными ИС;

программные, представляющие собой специальные программные комплексы, отдельные программы и системы разноплановой защиты информации;

криптографические – специальные алгоритмические и математические средства, основанные на применении методов шифрования. Шифрование является механизмом эффективной логической безопасности. Оно может использоваться в интересах обеспечения и целостности, и конфиденциальности как хранимой, так и передаваемой информации. Самой определяющей частью системы шифрования является генерация и передача ключей.

Физическая безопасность не сводится к безопасности только вычислительного центра, тем более, что ИС все более и более рассредоточиваются. Необходимо рассматривать взаимосвязь безопасности комплекса знаний, сооружений и оборудования. Безопасность ИС оценивается на основе использования таких мер, как идентификация, подтверждение подлинности, контроль доступа, информационные права, аудит, безаварийность и конфиденциальность. Особо следует рассмотреть систему разграничения доступа к конфиденциальной информации. Защита И в линиях связи сводится к защите содержания сообщения и защите процесса передачи данных.

Заключение. Рассмотрение проблем защиты информации с позиций системного подхода приобретает важное значение как в плане теории познания, так и с практической точки зрения.

В методологическом отношении исследование информационной безопасности предприятия как системы дает о ней прежде всего целостное представление, что, в свою очередь, позволяет с большей достоверностью и обоснованностью определять практические меры по ее обеспечению в целом и в различных конкретных условиях.

Содержание «теоретико-технологических» мероприятий информационной безопасности предприятия представляет собой обоснование объективной необходимости и определение частных и общих задач защиты; разработку соответствующих правовых, экономических, организационных, технических, социальных и других норм ее осуществления; проведение анализа правонарушений в различных информационных сферах; исследование состояния и перспектив развития средств, методов и форм организации, планирования, контроля и непосредственного осуществления защиты информации.

Исследование и анализ различных сторон практической деятельности ведущих западных и российских фирм, специальных

государственных и частных служб и других организаторов и исполнителей функций обеспечения безопасности ИС показывает, что системный подход к решению проблемы защиты информации не только полезен в реальной практической деятельности, но является единственным правильным направлением достижения надежной информационной защиты.

Литература

1. Авдонин Б.Н., Хрусталёв Е.Ю. Методология организационно-экономического развития наукоемких производств. – М.: Наука, 2010. – 367 с.

2. Астраханцева Е.А. Информационная безопасность – составляющая экономической безопасности предприятия // Ученые записки ИСГЗ, 2017, № 1, с. 43 – 47.

3. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин И.Т. Информационные системы и технологии в экономике. – М.: Финансы и статистика, 2003. – 416 с.

4. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) Система ГАРАНТ: http://base.garant.ru/182535/ #ixzz483oPf000.

5. Елизарова М.И., Крупина В.А. Методология оценки экономической безопасности наукоемкого предприятия // Модели и методы инновационной экономики / Сборник научных трудов. Выпуск 7. – М.: ЦЭМИ РАН, МАОН, 2015, с. 35-40.

6. Козунова С.С. Информационная система управления информационной безопасностью организации // Наука и Мир, 2016, том 1, № 4, с. 59 – 60.

7. Ларин С.Н., Хрусталёв Е.Ю. Использование информационных ресурсов и технологий для стимулирования инновационного развития экономики // Национальные интересы: приоритеты и безопасность, 2011, № 32, с. 2-11.

8. Лойко В.И. Алгоритмы структуры данных ЭИС. – Краснодар: КубГау, 2007. – 168 с.

9. Мингалева Ж.А., Капускина Т.В. Актуальность управления информационной безопасностью в процессе развития информационного общества // Актуальные вопросы экономических наук, 2009, № 7, с. 152 – 155.

10. Рыженкова О.Ю. Информационная безопасность: определение понятия, местов системе национальной безопасности // Закон и право, 2009, № 1, с. 50 – 52.

11. Семенов М.И., Трубилин И.Т., Лойко В.И., Барановская Т.П. Архитектура компьютерных систем и сетей. – М.: Финансы и статистика, 2003. – 256 с.

12. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ / Пер. с англ. – М.: Мир, 1982. – 436 с.

13. Хрусталёв Е.Ю. Экономическая безопасность наукоемкого предприятия: методы диагностики и оценки // Национальные интересы: приоритеты и безопасность, 2010, № 13, с. 51 – 58.

14. Хрусталёв Е.Ю., Стрельникова И.А. Методология качественного управления инвестиционными рисками на промышленных предприятиях // Экономический анализ: теория и практика, 2011, № 4, с. 16 – 23.

References

1. Avdonin B.N., Khrustalev E.Yu. Metodologija organizacionno-yekonomicheskogo razvitija naukoemkih proizvodstv. – M.: Nauka, 2010. – 367 s.

2. Astrahanceva E.A. Informacionnaja bezopasnost' – sostavljayushaja yekonomicheskoi bezopasnosti predprijatija // Uchenye zapiski ISGZ, 2017, № 1, s. 43 – 47.

3. Baranovskaja T.P., Loiko V.I., Semenov M.I., Trubilin I.T. Informacionnye sistemy i tehnologii v yekonomike. – M.: Finansy i statistika, 2003. – 416 s.

4. Doktrina informacionnoi bezopasnosti Rossiiskoi Federacii (utv. Prezidentom RF ot 9 sentjabrja 2000 g. № Pr-1895) Sistema GARANT: http://base.garant.ru/182535/ #ixzz483oPf000.

5. Elizarova M.I., Krupina V.A. Metodologija ocenki yekonomicheskoi bezopasnosti naukoemkogo predprijatija // Modeli i metody innovacionnoi yekonomiki / Sbornik nauchnyh trudov. Vypusk 7. – M.: CYeMI RAN, MAON, 2015, s. 35-40.

6. Kozunova S.S. Informacionnaja sistema upravlenija informacionnoi bezopasnost'yu organizacii // Nauka i Mir, 2016, tom 1, № 4, s. 59 – 60.

7. Larin S.N., Khrustalev E.Yu. Ispol'zovanie informacionnyh resursov i tehnologii dlja stimulirovanija innovacionnogo razvitija yekonomiki // Nacional'nye interesy: prioritety i bezopasnost', 2011, № 32, s. 2-11.

8. Loiko V.I. Algoritmy struktury dannyh YeIS. – Krasnodar: KubGau, 2007. – 168 s.

9. Mingaleva Zh.A., Kapuskina T.V. Aktual'nost' upravlenija informacionnoi bezopasnost'yu v processe razvitija informacionnogo obshestva // Aktual'nye voprosy yekonomicheskih nauk, 2009, № 7, s. 152 – 155.

10. Ryzhenkova O.YU. Informacionnaja bezopasnost': opredelenie ponjatija, mestov sisteme nacional'noi bezopasnosti // Zakon i pravo, 2009, № 1, s. 50 – 52.

11. Semenov M.I., Trubilin I.T., Loiko V.I., Baranovskaja T.P. Arhitektura komp'yuternyh sistem i setei. – M.: Finansy i statistika, 2003. – 256 s.

12. Sjao D., Kerr D., Myednik S. Zashita YeVM / Per. s angl. – M.: Mir, 1982. – 436 s.

13. Khrustalev E.Yu. Yekonomicheskaja bezopasnost' naukoemkogo predprijatija: metody diagnostiki i ocenki // Nacional'nye interesy: prioritety i bezopasnost', 2010, № 13, s. 51 – 58.

14. Khrustalev E.Yu., Strel'nikova I.A. Metodologija kachestvennogo upravlenija investicionnymi riskami na promyshlennyh predprijatijah // Yekonomicheskii analiz: teorija i praktika, 2011, № 4, s. 16 – 23.