УДК 330.46

Скворцова Ирина Андреевна *студентка 4 курса специальности «Экономическая безопасность» ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва»*

Емелин Владимир Николаевич, *кандидат экономических наук доцент кафедры бухгалтерского учета, анализа и аудита ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва»*

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация: В статье раскрываются проблемы информационных систем, концептуальные подходы и методы экономической безопасности информационных систем. Отражены способы защиты информационных систем от различных угроз и проблем.

Ключевые слова: информационные системы, информационная безопасность, экономическая безопасность, острые проблемы.

Abstract: the article reveals the problems of information systems, conceptual approaches and methods of economic information systems security. Reflected ways to protect information systems from various threats and challenges.

Keywords: information systems, information security, economic security, acute problems.

Безопасность информационной системы является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю - национальном, отраслевом, корпоративном или персональном.

Если рассматривать безопасность в качестве общенаучной категории, то она может быть определена как некоторое состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой - ее функционирование не создает угроз для элементов самой системы и внешней среды. При таком определении мерой безопасности системы являются:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз - степень (уровень) сохранения системой своей структуры, технологи и эффективности функционирования при воздействии дестабилизирующих факторов;

- с точки зрения отсутствия угроз для элементов системы и внешней среды - степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам самой системы или внешней среде.

Чисто механическая интерпретация данных формулировок приводит к следующему определению безопасности информационной системы:

Безопасность информационной системы - такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Именно такое понятие «безопасность информационной системы» положено в основу «Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации», (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)

Приведенное определение представляется достаточно полным и вполне корректным. Однако, для того, чтобы служить более конкретным ориентиром в направлении поиска путей решения проблем безопасности информационной системы, оно нуждается в уточнении и детализации его основополагающих понятий.

Отсюда вытекает, то что обеспечение защищенности информативной системы в единой постановке проблемы может быть достигнуто только при взаимоувязанном постановлении 3-х составляющих вопросов:

1) охрана оказавшейся в системе информации от дестабилизирующего влияния внешних и внутренних опасностей информации;

2) охрана компонентов системы от дестабилизирующего влияния внешних и внутренних информационных опасностей;

3) охрана внешней среды от информационных опасностей со стороны

Можно отметить следующие особо значимые проблемы формирования теории и практики обеспечения информационной безопасности:

- формирование теоретических основ и развитие научно-методологического базиса, позволяющих верно характеризовать процессы в условиях существенной неопределенности и непредсказуемости проявления дестабилизирующих условий (информационных опасностей);

- создание научно аргументированных нормативно-методичных документов по обеспечению информационной безопасности на основе изучения и систематизации угроз информации и формирования стандартов требований к защите;

- стандартизация подходов к формированию систем защиты информации и совершенствование методик и строений управления защитой на объектовом, региональном и государственном уровнях.

Необходимо проанализировать одно из ключевых направлений защищенности информационных систем, это компьютерная безопасность. Её можно охарактеризовать следующим образом.

Компьютерная безопасность (сетевая защищенность, телекоммуникационная защищенность, защищенность данных) - предоставление защиты информации в её условном виде. Допустимо выделять этапы нахождения информации в среде, и согласно этим основам различать, к примеру, компьютерную (в месте формирования, хранения либо обработки данных) и сетевую (при пересылке) защищенность, однако это, в принципе, нарушает единую картину защищенности. Только одно, с чем разумно было бы выразить согласие, - это термин безопасность данных, либо точнее, безопасность данных в рамках данного приложения. Проблема в том, то, что в определенном программном комплексе форма безопасности может быть выполнена таким способом, что это потребует отдельного специалиста (либо даже службы) согласно её поддержанию. В данном случае, допустимо, разделить определения безопасность данных (конкретного приложения) и безопасность сети (всей остальной информационной среды).

При применении каждой информационной технологии необходимо концентрировать внимание на присутствие средств охраны данных, программ, компьютерных систем.

Безопасность данных содержит обеспечение достоверности данных и защиту данных и программ от неразрешенного доступа, копирования, изменения.

Достоверность данных контролируется на абсолютно всех этапах научно-технического процесса эксплуатации ЭИС. Отличают визуальные и программные способы контролирования. Визуальный надзор производится на домашинном и завершающем этапах. Программный - на внутримашинном этапе. При этом неизбежен надзор при вводе сведений, их исправлении, т.е. повсюду, где имеется вторжение пользователя в электровычислительный процесс. Надзираются отдельные реквизиты, записи, категории записей, комп.данные. Программные ресурсы контролирования достоверности сведений закладываются на стадии рабочего проектирования.

Защита сведений и программ от неразрешенного доступа, копирования, изменения реализуется программно-аппаратными способами и научно-техническими способами. К программно-аппаратным средствам охраны относят пароли, электронные ключи, электронные личные номера, электронную подпись, средства кодировки, декодирования сведений. С целью кодировки, декодирования сведений, программ и электронной подписи применяются шифровальные методы. К примеру, в США используется шифровальный стандарт, созданный группой IETF. Экспорту он никак не подлежит. Изобретены в том числе и российские электронные ключи, к примеру, Novex Key с целью охраны программ и данных в системах Windows, DOS, Netware. Средства охраны аналогичны, согласно словам экспертов, дверному замку. Замки взламываются, однако никто никак не убирает их с двери, оставив квартиру открытой.

Научно-технический контроль состоит в организации многоуровневой системы охраны программ и сведений равно как средствами проверки паролей, электронных подписей, электронных ключей, скрытых меток файла, применением программных продуктов, удовлетворяющих условиям компьютерной защищенности, таким образом и способами визуального и программного контролирования достоверности, единства, всесторонности сведений.

Безопасность обработки сведений находится в зависимости от защищенности использования компьютерных систем. Компьютерной системой называется комплекс аппаратных и программных средств, разного рода физических носителей информации, непосредственно данных, а кроме того персонала, обслуживающего приведенные компоненты.

В настоящее время в США сконструирован стандарт оценок защищенности компьютерных систем - аспекты оценок пригодности. В нем предусматриваются 4 вида условий к компьютерным системам:

-условия к проведению политики защищенности - security policy;

-ведение учета применения компьютерных систем - accounts;

-взаимодоверие к компьютерным системам;

-условия к документации.

Условия к проведению последовательной политики защищенности и ведение учета использования компьютерных систем находятся в зависимости друг от друга и поддерживаются средствами, заложенными в систему, т.е. разрешение проблем защищенности включается в программные и аппаратные средства на стадии проектирования.

Нарушение доверия к компьютерным системам, как правило, бывает обусловлено нарушением культуры разработки программ: отказом от структурного программирования, неисключением заглушек, неясным вводом и т.д. Для тестирования на доверие необходимо понимать архитектуру приложения, принципы устойчивости его укрепления, тестовый образец.

Требования к документации означают, то что пользователь обязан иметь полную информацию по абсолютно всем вопросам. При этом документация должна являться краткой и ясной.

Только уже после оценки защищенности компьютерной системы она может поступить на рынок.

В период эксплуатации ИС максимальный ущерб и потери доставляют вирусы. Защиту от вирусов возможно осуществить так же, как и защиту от неразрешенного доступа. Методика защиты считается многоуровневой и включает следующие этапы:

1. Входной контроль новейшего программного обеспечения либо дискеты, который исполняется группой специально выбранных детекторов, ревизоров и фильтров. К примеру, в состав группы можно ввести Scan, Aidstest, TPU8CLS. Возможно осуществить карантинный режим. Для этого формируется ускоренный компьютерный календарь. При любом последующем эксперименте включится новая дата и прослеживается отклонение в старом программном обеспечении. В случае если отклонения не имеется, то вирус не найден.

2. Сегментация жесткого диска. При этом отдельным разделам диска присваивается атрибут Read Only. Для сегментации можно применять, к примеру, проект Manager и др.

3. Систематическое применение резидентных, программ-ревизоров и фильтров с целью контролирования целостности данных, к примеру Check21, SBM, Antivirus2 и т.д.

4. Архивация. Ему подлежат и системные, и прикладные проекты. В случае если один ПК используется несколькими пользователями, то предпочтительно ежедневное архивирование. Для архивирования возможно применять PKZIP и др.

Существенное значение для избежания информационных угроз имеет мотивирование, финансовое стимулирование и психологическая помощь деятельности персонала, который гарантирует информационную защищенность.

Каждый из упомянутых средств способен применяться как без помощи других, так и в интеграции с другими. Это делает допустимым формирование систем информационной защиты для систем любой трудности и конфигурации, вне зависимости от применяемых платформ.

Системы кодирования дают возможность уменьшить потери в случае неразрешенного доступа к сведениям, хранящимся на жестком диске либо ином носителе, а также перехвата данных при её пересылки по электронной почте либо передаче по сетевым протоколам. Задача данного средства защиты — обеспечения конфиденциальности. Основные требования, предъявляемые к системам шифрования - высокий уровень криптостойкости и легальность использования на территории государства.

Межсетевой дисплей предполагает внешне систему или комбинацию систем, производящую между 2-мя либо более сетями предохранительный барьер, предохраняющий от неразрешенного попадания в сеть либо выхода из нее пакетов данных - проверка каждого пакета данных на соответствие входящей и исходящей IP адреса базе допустимых адресов. Подобным способом, межсетевые экраны существенно расширяют способности сегментации информационных сетей и контроля за циркулирование сведений.

Говоря о криптографии и межсетевом экране, необходимо отметить о защищенных виртуальных частных сетях (Virtual Private Network ─ VPN). Их применение дает возможность решить проблемы конфиденциальности и целостности сведений при их передаче по открытым коммуникационным каналам. Применение VPN возможно свести к решению 3-х ключевых вопросов:

1. охрана информационных потоков между разными офисами фирмы (кодирование данных выполняется только лишь на выходе во внешнюю сеть);

2. безопасный доступ удаленных пользователей сети к информационным ресурсам фирмы, как правило, исполняемый посредством Internet;

3. охрана информационных потоков между отдельными приложениями изнутри корпоративных сетей (данный подход кроме того весьма значим, так как большая часть атак исполняется из внутренних сетей).

Эффективное средство защиты от потери конфиденциальной информации - фильтрация содержимого входящей и исходящей электронной почты. Проверка почтовых сообщений на основе правил, установленных в организации, позволяет также обеспечить безопасность компании от ответственности по судебным искам и защитить их сотрудников от спама. Средства контентной фильтрации позволяют проверять файлы всех распространенных форматов, в том числе сжатые и графические. При этом пропускная способность сети практически не меняется.

Помимо этого, разработаны технологические процессы моделирования поведения, позволяющие обнаруживать вновь вирусные программы. Выявленные объекты могут подвергаться излечению, изолироваться (помещаться в карантин) либо устраняться. Охрана от вирусов может быть определено на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под почти каждой из

распространенных операционных систем (Windows, Unix-и Linux-системы, Novell) в процессорах разных видов. Фильтры спама существенно сокращают непроизводственные расходы труда, сопряженные с рассмотрением спама, уменьшают трафик и загрузку серверов, усовершенствуют общепсихологический фон в коллективе и сокращают риск вовлечения работников фирмы в мошеннические действия. Помимо этого, фильтры спама сокращают опасность инфицирования новыми вирусами, так как уведомления, содержащие вирусы (даже ещё никак не введены в базу противовирусных программ) зачастую имеют свойства спама и фильтруются. С целью противодействия природным угрозам информационной защищенности в компании должен быть сконструирован и выполнен комплект процедур по предотвращению чрезвычайных ситуаций (к примеру, по обеспечению физической охраны сведений от пожара) и минимизации потерь в том случае, если подобная ситуация все же появится. Единственный из ключевых способов защиты от потери сведений - резервное копирование с точным соблюдением определенных операций (регулярность, виды носителей, способы хранения копий и т.д.).

В РФ главным источником концентрированных государственных вложений в усиление информационной защищенности считается федеральная целевая программа «Электронная Российская федерация». В рамках данной программы до 2010 года в информатизацию государства было инвестировано в общей сложности 2.4 миллиардов $. По оценкам специалистов, от 5 вплоть до 10% от данной суммы будет израсходовано на проблемы, непосредственно связанные с информационной защищенностью.

Сегодня в Российской федерации функционируют более 100 компаний, которые специализируются на информационной защищенности, размер вложений в их развитие по различным оценкам составляет 200—250 миллионов $ в год. Замечается тенденция учащенного возникновения и формирования компаний, которые специализируются не на разработке программных и аппаратных средств защищенности, а на предоставлении услуг — консалтинга, аудита, тестирования персонала и информационных систем и т. д.

Проводимые в Российской федерации НИОКР в сфере технологий информационной защищенности вынашивают разрозненный вид и имеют необходимость в координации и приоритетной поддержке со стороны правительства.

При этом, то, что область информационной защищенности в необходимой мере коммерциализирована, стране следует обеспечивать её непрерывное формирование посредством вложений в ключевые НИОКР, создавая подобным способом рынок средств обеспечения информационной защищенности с учетом интересов национальной безопасности.

В нынешних обстоятельствах формирования рыночных взаимоотношений в экономической сфере, информация считается особого рода продуктом, который содержит значительную важную ценность. Как товар информация может пользоваться спросом, так как содержит определенную ценность, но её особенность, сопряжена с превращением человеческих знаний, формирует сложности в определении её стоимости [6]. Однако значимость информации может формироваться, исходя из её достоверности, единства и доступности. Последняя делает информацию более привлекательной, так как её конфиденциальность обусловливается определенным режимом доступа и ограничивается диапазоном лиц, которые имеют возможность владеть ею [7].

Рассматривая характерные черты информационной функции системы управления экономической безопасностью предприятия, необходимо выделить, то что только лишь комплексный подход к управлению предпринимательством и безопасностью в нем и если все без исключения сотрудники должны, особенно в кризисных, остроконфликтных и неустойчивых ситуациях, серьезно обращаться к вопросу обеспечения информационной, личной защищенности и экономической безопасности компании в целом, что повлечет позитивные результаты работы. Для этого менеджеру и специалистам службы безопасности компании следует основательно освоить и эффективно использовать основные методы управления организацией, персоналом и системой защищенности в предпринимательской деятельности. Таким образом, с целью нормального формирования собственного бизнеса, предприниматель должен не только сформировать концепцию защищенности компании, но и умело и профессионально управлять ею. Информационная безопасность обязана обеспечиваться посредством выполнения целостной государственной программы в соответствии с Конституцией и действующим законодательством РФ и норм международного права путем реализации определенных

доктрин, стратегий, концепций и проектов, касающихся государственной информационной политики РФ. Понятие информационной безопасности компании необходимо также рассматривать в контексте предоставления безопасных условий существования информационных технологий, которые содержат проблемы защиты данных, построения успешной информационной инфраструктуры, информационного рынка и формирование безопасных условий жизни и формирования информационных процессов.

Информационная безопасность является одной из главных составляющих экономической безопасности, и определяется как "состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз». Состояние защищенности — это стабильно прогнозируемое во времени состояние окружения, в котором предприятие может осуществлять свои уставные задачи без перерывов, нарушений и потери конкурентоспособности.

Библиографический список

1. Балдин, К.В. Информационные системы в экономике: Учебник / К.В. Балдин, В.Б. Уткин. - М.: Дашков и К, 2013.

2. Бодров, О.А. Предметно-ориентированные экономические информационные системы: Учебник для вузов / О.А. Бодров. - М.: Гор. линия-Телеком, 2013. - 244 с.

3. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. - М.: Форум, 2013. - 528 с.

4. Вдовин, В.М. Предметно-ориентированные экономические информационные системы: Учебное пособие / В.М. Вдовин. - М.: Дашков и К, 2013. - 388 с.

5. Основы информационной безопасности: Учебное пособие / О.А. Акулов, Д.Н. Баданин, Е.И. Жук и др. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. - 161 с.

6. Исаев, Г.Н. Информационные системы в экономике: Учебник для студентов вузов / Г.Н. Исаев. - М.: Омега-Л, 2013. - 462 с.

7. Федорова, Г.Н. Информационные системы: Учебник для студ. учреждений сред. проф. образования / Г.Н. Федорова. - М.: ИЦ Академия, 2013. - 208 с.