А. М. Спиридонов
Федеральная служба по финансовому мониторингу (Росфинмониторинг)

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРИНЯТИИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В СФЕРЕ ФИНАНСОВОГО МОНИТОРИНГА

В статье рассматриваются понятие информационной безопасности при принятии управленческих решений (УР), специфика построения информационных систем, используемых в процессе принятия управленческих решений в сфере финансового мониторинга, возможные угрозы информационной безопасности подобных систем, а также комплексные средства по нейтрализации опасных информационных воздействий.

Введение

Управленческие решения — это выбор, который должен сделать руководитель, чтобы выполнить обязанности, обусловленные занимаемой им должностью. Целью разработки и принятия УР в сфере финансового мониторинга является осуществление контроля и надзора за выполнением юридическими и физическими лицами требований законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, привлечение к ответственности лиц, допустивших нарушение этого законодательства.

В процессе работы лица, участвующие в принятии управленческих решений, испытывают влияние объективных закономерностей и принципов, связанных с экономическими, социальными, политическими, психологическими, информационными и иными условиями и факторами современной жизни. Комплексное взаимовлияние указанных аспектов общественно-политического устройства проявляется в выборе руководством предпочтительных вариантов решения поставленных перед ним задач.

В условиях модернизации экономического, политического и социального устройства российского общества особую остроту приобрела проблема обеспечения национальной безопасности Российского государства, в том числе и в такой специфической и жизненно важной сфере, как информационная. Такой подход нашел свое отражение в Концепции национальной безопасности, утвержденной Указом Президента Российской Федерации от 10 января 2000 г., а также в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 9 сентября 2000 г.

Согласно определению, приведенному в Руководящем документе Гостехкомиссии РФ «Защита от несанкционированного доступа к информации», под информационной безопасностью понимается «состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз».

Информационная безопасность — это комплекс мероприятий, направленных на обеспечение защиты информации. На практике под этим понимается поддержание целостности, доступности и, если необходимо, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных. Комплексный характер проблемы защиты говорит о том, что для ее решения необходимо сочетание законодательных, организационных и программно-технических мер.

1. Информационная безопасность при принятии управленческих решений

Системный подход к информационной безопасности требует определения источников опасности, субъектов, средств и объектов, принципов обеспечения, направленности опасных информационных потоков.

Источники информационных опасностей могут быть естественными (объективными) и умышленными. Первые возникают в результате непреднамеренных ошибок и неисправностей, случайных факторов, стихийных бедствий и др. Умышленные информационные воздействия

осуществляются сознательно и целенаправленно. При этом часто используются средства массовой информации, специальные программные средства для компьютеров.

Субъектами информационной безопасности следует считать те органы и структуры, которые занимаются ее обеспечением. Это могут быть в первую очередь управления безопасности и защиты информации федеральных и региональных органов исполнительной, законодательной, судебной власти, органов местного самоуправления. В коммерческих структурах это, как правило, службы внутреннего контроля банков, страховых компаний и других субъектов финансового рынка.

Объектами опасного информационного воздействия и, следовательно, информационной безопасности могут быть прежде всего информационно-технические системы различного масштаба, используемые в процессе принятия решений. И, хотя в вопросах информационной безопасности важное место занимают также случаи опасного информационного воздействия в отношении так называемых социальных объектов информационной безопасности (руководители, непосредственно участвующие в принятии управленческих решений, персонал организации), все же наибольшее распространение получили информационные атаки именно на технические средства.

При анализе рисков, связанных с информационной безопасностью, необходимо принять во внимание тот факт, что компьютеры во внутренних сетях организаций редко бывают достаточно защищены, чтобы противостоять атакам или регистрировать факты нарушения информационной безопасности. Так, тесты Агентства защиты информационных систем (США) показали, что 88 % компьютеров имеют слабые места с точки зрения информационной безопасности, которые могут активно использоваться для получения несанкционированного доступа. При этом в среднем только каждый двенадцатый администратор обнаруживает, что указанный инцидент произошел в управляемой им системе.

2. Современные информационные системы организационного управления

Информационные системы организационного управления в сфере финансового мониторинга предназначены для оказания помощи специалистам, руководителям, принимающим решения, в получении ими своевременной и достоверной информации. В условиях электронной обработки данных преобладают операции, производимые автоматически на машинах и устройствах, которые считывают данные и выполняют операции по заданной программе в автоматическом режиме без участия человека или сохраняя за пользователем функции контроля, анализа и регулирования. Особое значение в таких системах придается защите информации при ее передаче и обработке.

Наибольшее распространение при защите экономической информации получили аппаратно-программные способы, в частности использование системы связи, выбранной по защитным свойствам и качеству обслуживания, гарантирующим сохранность информации в процессе передачи и доставки ее адресату; шифрование и дешифрование данных абонентами сетей общего пользования (телефонных, телеграфных) при договоренности пользователей об общих технических средствах, алгоритмах шифрования и т. п.

Реализация принципа сбора, интеграции, хранения и систематической обработки информации об операциях с денежными средствами или иным имуществом, в соответствии с законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, закладывается на стадии создания системы. Учитывается, что пользователями информации будут не только специалисты конкретной проблемной области управленческой деятельности (учета, планирования, менеджмента, маркетинга и т. п.), но и программисты, занимающиеся созданием и эксплуатацией программных средств. Поэтому в процессе проектирования и ведения базы данных в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма ведется тщательное разностороннее исследование

предметной области, ее элементов, взаимосвязи между ними, а также выявляются особенности циркулирующих в ней данных как особо важного ресурса. Создается общая структурная схема баз данных в виде многоуровневых моделей, формируются условия и осуществляется выбор системы управления базами данных (СУБД). При этом разрабатываются способы фильтрации ошибочных данных, вводимых в систему; устанавливаются необходимые разграничения доступа к массивам конкретных пользователей; удовлетворяются требования независимости данных от программ и их физического расположения и т. п. Все перечисленное учитывается среди прочих факторов при выборе или создании СУБД.

Повышение требований к оперативности информационного обмена и управления, а следовательно, к срочности обработки информации привело к созданию многоуровневых систем организационного управления объектами, какими являются, например, банковские, налоговые, снабженческие, статистические и другие службы. Их информационное обеспечение поддерживают сети автоматизированных банков данных, которые строятся с учетом организационно-функциональной структуры соответствующего многоуровневого экономического объекта, машинного ведения информационных массивов. Эту проблему в новых информационных технологиях решают распределенные системы обработки данных с использованием каналов связи для обмена информацией между базами данных различных уровней. За счет усложнения программных средств управления базами данных повышаются скорость, обеспечиваются защита и достоверность информации при выполнении экономических расчетов и выработке управленческих решений.

Возникает необходимость в накоплении фактов, опыта, знаний в каждой конкретной области управленческой деятельности. На первый план выдвигается заинтересованность в тщательном исследовании конкретных экономических, коммерческих, производственных ситуаций с целью принятия в оперативном порядке экономически обоснованных и наиболее приемлемых решений. Эта задача решается в результате дальнейшего совершенствования интегрированной обработки информации, когда новая информационная технология начинает включать в работу базы знаний. Под базой знаний понимается сложная, детально моделируемая структура информационных совокупностей, описывающих все особенности предметной области, включая факты (фактические знания), правила (знания условий для принятия решений) и метазнания (знания о знаниях), т. е. знания, касающиеся способов использования знаний и их свойств. База знаний — важнейший элемент создаваемой на рабочем месте специалиста экспертной системы, выступающей в роли накопителя знаний конкретной области профессиональной деятельности и советчика специалисту при проведении исследования экономических ситуаций и выработке управляющих воздействий.

3. Угрозы информационной безопасности при принятии управленческих решений в сфере финансового мониторинга и средства их нейтрализации

Можно выделить несколько видов опасных информационных воздействий, серьезно угрожающих информационной безопасности организации, осуществляющей контроль и надзор за выполнением юридическими и физическими лицами требований законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки приводят к прямому ущербу (неправильно введенные данные, ошибка в программе, вызвавшая остановку или разрушение системы). Иногда они создают слабые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). Согласно данным Национального института стандартов и технологий США (NIST), 65 % случаев нарушения безопасности ИС — следствие непреднамеренных ошибок.

На втором месте по размерам ущерба располагаются кражи и подлоги. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Наличие мощного информационного канала связи с глобальными сетями может, при отсутствии должного контроля за его работой, дополнительно способствовать такой деятельности.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались.

Преднамеренные попытки получения несанкционированного доступа через внешние коммуникации занимают в настоящее время около 10 % всех возможных нарушений. Хотя эта величина кажется не столь значительной, опыт работы в Интернете показывает, что почти каждый крупный веб-сервер по нескольку раз в день подвергается попыткам проникновения извне. Кроме того, необходимо иметь в виду динамику развития рисков этого типа: по данным Группы изучения компьютерных рисков (CERT), проводившей исследование различных информационных систем, контролируемых правительствами ведущих стран мира, если в 1990 г. зарегистрировано 130 удачных попыток несанкционированного доступа к компьютерным ресурсам через Интернет, то в 1994 г. эта цифра составила 2300.

Еще один вид опасных информационных воздействий связан с утратой ценной информации. Если объектами такого воздействия являются лица, непосредственно участвующие в принятии управленческих решений, то речь идет о разглашении государственных тайн, вербовке агентов, специальных мерах и средствах для подслушивания, использовании детекторов лжи, медикаментозных, химических и других воздействиях на психику человека с целью заставить его выдать определенную информацию или забыть ее.

Безопасность от информационного воздействия данного вида обеспечивают органы цензуры, контрразведки и другие субъекты информационной безопасности. Если же источником информации служат технические системы, то речь идет уже о технической разведке, или шпионаже (перехват телефонных разговоров, радиограмм, сигналов других систем коммуникации), проникновении в компьютерные сети, банки данных. Деятельностью подобного рода занимается, например, Агентство национальной безопасности США, затрачивая на это около 15 млрд долларов в год. Противодействуют технической разведке органы контрразведки, а также структуры, занимающиеся защитой компьютерных средств и систем связи.

Важный вид информационного воздействия связан с внедрением негативной информации, что может не только привести к опасным ошибочным решениям, но и заставить действовать во вред.

Информационную безопасность этого вида должны обеспечивать специальные структуры информационно-технической борьбы. Они нейтрализуют акции дезинформации, пресекают манипулирование общественным мнением, ликвидируют последствия компьютерных атак.

В завершение обзора опасных информационных воздействий рассмотрим наиболее распространенные угрозы, которым подвержены современные технические средства, используемые в процессе принятия решений. Знание возможных угроз, а также уязвимых мест информационной системы необходимо для того, чтобы выбирать наиболее эффективные средства обеспечения безопасности. Угрозами безопасности информационных и телекоммуникационных средств и систем могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

• разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

• уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

• воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

• компрометация ключей и средств криптографической защиты информации;

• утечка информации по техническим каналам;

• внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций;

• уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

• перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

• использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

• несанкционированный доступ к информации, находящейся в банках и базах данных;

• нарушение законных ограничений на распространение информации.

4. Комплексное обеспечение информационной безопасности: политика безопасности организации

Ключевым этапом для обеспечения режима хранения и защиты информационной системы в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма является выработка политики безопасности. Под политикой информационной безопасности понимается совокупность документированных управленческих решений и разработанных превентивных мер, направленных на защиту информационных ресурсов. С практической точки зрения политику безопасности целесообразно разделить на три уровня:

• Решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации.

• Вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией.

• Конкретные сервисы информационной системы.

Третий уровень включает в себя два аспекта — цели (политики безопасности) и правила их достижения, поэтому его порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, третий должен быть гораздо детальнее. У отдельных сервисов есть много свойств, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти свойства настолько важны для обеспечения режима безопасности, что решения, относящиеся к ним, должны приниматься на управленческом, а не техническом уровне.

Начать составление политики следует с анализа рисков. Анализ рисков состоит из двух основных этапов: инвентаризация и классификация технических ресурсов.

Инвентаризация технических ресурсов поможет в определении степени необходимой защиты, контроле защищенности, а также будет полезна в других областях, как-то: охрана труда и техника безопасности, страхование, финансы. В качестве технических ресурсов могут выступать:

• информационные ресурсы: файловые хранилища, базы данных, документация, учебные пособия, документы процедурного уровня (инструкции и т. д.);

• программные ресурсы: прикладное и системное программное обеспечение, утилиты и т. д.;

• физические ресурсы: вычислительное и коммуникационное оборудование, носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения;

• сервисы: отопление, освещение, энергоснабжение, кондиционирование воздуха.

После инвентаризации производится классификация ресурсов. Ценность каждого ресурса обычно представляется как функция нескольких дискретных переменных.

Приведем пример классификации информационного ресурса. В качестве основной переменной обычно выбирают степень конфиденциальности информации со следующими значениями:

• информация, содержащая государственную тайну;

• информация, содержащая коммерческую тайну;

• конфиденциальная информация (информация, не представляющая собой государственную или коммерческую тайну, хотя огласка ее нежелательна);

• иная информация.

Далее производится собственно анализ рисков. Для каждого из информационных ресурсов определяется его суммарная ценность и возможные угрозы. Каждая из угроз оценивается с точки зрения ее применимости к данному ресурсу, вероятности возникновения и возможного ущерба. На основе результатов этого анализа составляется классификационный раздел политики информационной безопасности.

Далее формируется штатный раздел, направленный на уменьшение риска ошибок персонала, краж, мошенничества или незаконного использования ресурсов. В дальнейшем этот раздел используется для составления должностных инструкций пользователей и руководящих документов для отделов и служб информационной безопасности. В документ желательно включить следующие разделы:

• правила проверки принимаемого на работу персонала;

• обязанности и права пользователей по отношению к информационным ресурсам;

• обучение пользователей и порядок допуска к работам с информационными ресурсами;

• права и обязанности администраторов;

• порядок реагирования на события, несущие угрозу информационной безопасности;

• порядок наложения взысканий.

В первый пункт включаются правила подачи заявлений о приеме, необходимые документы, форма резюме, рекомендаций и т. д. Кроме того, определяются необходимость, форма и порядок проведения собеседования с работниками различных категорий. Здесь же описываются различные обязательства о неразглашении.

Во втором пункте описываются обязанности пользователей по обслуживанию своего рабочего места, а также при работе с информационными ресурсами. Этот пункт тесно связан с третьим пунктом, поскольку определяет необходимые знания пользователей.

Третий пункт определяет знания, необходимые для различных категорий работников, периодичность и порядок проведения инструктажа по пользованию информационными ресурсами. Требуется четкое знание пользователями всех процедурных вопросов (идентификация в системе, смена пароля, обновление антивирусных баз, работа с пакетами программ и т. д.). Кроме того, описывается порядок подключения пользователя к информационным ресурсам (необходимые документы, согласующие лица и подразделения).

Для нормального функционирования системы администраторы информационной безопасности должны обладать достаточными правами. Отключение от сети или информационного ресурса рабочей станции, являющейся носителем вируса, — необходимость, а не нарушение технологического процесса.

Для своевременной реакции на угрозы безопасности системы следует четко определить формальные процедуры уведомления и реагирования. Все пользователи должны быть обязаны сообщать заранее опреленным лицам об инцидентах и слабых местах в системе безопасности, сбоях в работе программного и аппаратного обеспечения. Необходимо определить и довести до сведения пользователей методы фиксации симптомов сбоев оборудования.

Последний раздел содержит описание процедуры наложения взысканий за нарушения установленных в организации правил информационной безопасности. Карательные меры и степень ответственности необходимо закрепить документально.

В зависимости от типа предприятия меры физической защиты могут варьироваться в широком диапазоне. Исходя из анализа рисков для каждой организации необходимо жестко описать типы помещений и треюующиеся для них меры безопасности. К мерам безопасности относятся установка решеток, замков, порядок допуска в помещения, средства электромагнитной защиты и т. д. Кроме того, необходимо установить правила использования рабочего стола и способы утилизации материалов (различных магнитных носителей, бумажных документов, агрегатов), правила выноса программного и аппаратного обеспечения за пределы организации.

Разделы управления, посвященные подходам к управлению компьютерами и сетями передачи данных и порядку разработки и внедрения систем, описывают порядок выполнения стандартных процедур оперирования данными, правила ввода систем в эксплуатацию (приемка систем), аудита их работы. Кроме того, в данном разделе указывается порядок защиты информационных ресурсов организации от вредоносного программного обеспечения (регламент работы антивирусной системы, в частности). Определяются порядок аудита работоспособности систем и резервное копирование. Описывается стандартное программное обеспечение, разрешенное к работе на предприятии. Здесь же описываются системы защиты электронной почты, системы электронной цифровой подписи и другие криптографические системы и системы аутентификации, работающие на предприятии. Это немаловажно, поскольку эта область жестко регулируется российским законодательством.

Права доступа к системам должны быть документированы, а порядок их предоставления определен нормативными документами. Должны быть указаны должности лиц, производящих согласование заявок на предоставление прав доступа, а также осуществляющих раздачу прав. Кроме того, в организациях с серьезными требованиями к информационной безопасности определяются порядок проверок прав доступа к системам и лица, его осуществляющие. В этом же разделе описываются правила (политика) пользовательских паролей.

Итак, политика информационной безопасности предприятия представляет собой документ, на основе которого строится система обеспечения безопасности. В свою очередь, политика строится на анализе рисков, и чем полнее будет произведен анализ, тем эффективнее будет документ. Анализу подвергаются все основные ресурсы, включая материальную базу и человеческие ресурсы. Политика безопасности строится в соответствии со спецификой предприятия и законодательной базой государства.

Заключение

В статье рассмотрены основные проблемы информационной безопасности при принятии управленческих решений; при этом подчеркивается комплексный характер этих проблем, поскольку информация в сфере финансового мониторинга может составлять государственную, служебную,

банковскую, налоговую, коммерческую тайну. Были выделены источники информационной опасности, субъекты, средства и объекты, принципы обеспечения информационной безопасности, направленности опасных информационных потоков.

Атаки на технические средства организации, как наиболее распространенные, требуют рассмотрения специфики построения информационных систем, используемых в процессе принятия управленческих решений в сфере финансового мониторинга. Для решения стоящих перед информационной безопасностью задач необходимо сочетание законодательных, организационных и программно-технических мер. Ключевым этапом для обеспечения режима хранения и защиты информационной системы в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма является выработка политики безопасности как совокупности документированных управленческих решений и разработанных превентивных мер, направленных на защиту информационных ресурсов организации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Зубков В. А., Осипов С. К.* Российская Федерация в международной системе противодействия легализации (отмыванию) преступных доходов и финансированию терроризма. М.: Издательский дом «Городец», 2006.
2. *Бушуева Л. И.* Теоретические подходы к формированию системы информационного обеспечения управленческих решений. URL: http://www.syktsu.ru/vestnik/2006/2006-3/1.htm.
3. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Энергоатом-издат, 1994.
4. *Баззел Р. Д., Кокс Д. Ф., Браун Р. В.* Информация и риск в маркетинге. М.: Финстатинформ, 1993.
5. Вычислительные машины, системы и сети / Под ред. А. П. Пятибратова. М.: Финансы и статистика, 1991.
6. *Гордейчик С. В.* Политика информационной безопасности предприятия. URL: http://www.economer.khv.ru/content/n038/45it.
7. *Астахов А.* Разработка эффективных политик информационной безопасности. URL: http://www.morepc.ru/informatisation/inf200220041.html.
8. *Пеньков И. А.* Информационная безопасность Российской Федерации (политологический анализ). URL: http://www.cir.ru/docs/http/www.budgetrf.ru/Publications/Magazines/VestnikSF/2005/VSF_NEW200701241350/VSF_NEW200701241350_p_001.htm.