разование: современные тренды: коллективная монография / гл. ред. О. Н. Широков. – Чебоксары: ЦНС «Интерактив плюс», 2015. – № VIII. – С. 471–484.

Шапиро Ольга Сергеевна
студентка 4 курса факультета информационных технологий и системного анализа
ФГБОУ ВПО «Орловский государственный институт экономики и торговли»
e-mail: oshapiro@bk.ru

Сергеева Инна Ивановна
к.э.н., доцент кафедры математики, информатики и информационных технологий
ФГБОУ ВПО «Орловский государственный институт экономики и торговли»
e-mail: inchiksergeeva@yandex.ru

УДК 657.6:321:004

Ромашова Л.В.

ОСОБЕННОСТИ ГОСУДАРСТВЕННОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-СИСТЕМ

Глобальные изменения структуры мировой рыночной системы в XXI в. обусловлены изменением роли высокотехнологического сектора экономики и переходом ее к информационному обществу. Экономические субъекты в этих условиях становятся все более сложными и динамичными бизнес-системами. Усложняется как сама структура управления ими, так и обработка и передача надлежащей информации, которая становится существенной частью их бизнес-процессов. Особую роль в этом играют современные информационные технологии.

В представленной статье систематизированы взгляды на государственный аудит информационной безопасности бизнес-систем, который в современных условиях становится практически незаменимым инструментарием разностороннего исследования и оценки информации, принятия управленческих решений.

Ключевые слова: информационная безопасность, бизнес-система, информационные процессы, государственный аудит информационной безопасности.

В настоящее время информационные технологии становятся одним из основных инструментов обеспечения адаптивности и конкурентоспособности бизнес-систем. По мере изменения требований бизнес-среды меняются требования, предъявляемые к программным продуктам и ИТ-сервисам (ИТ-услугам), что приводит к добавлению в их поддерживающую информационную инфраструктуру все новых и новых программно-аппаратных платформ. При этом все возрастающая их сложность и разнородность оказывают влияние на управляемость всей информационной системой (ИС) субъектов, стабильность и эффективность ее работы, а также ее защищенность от перманентных внутренних и в особенности внешних угроз.

В то же время потребность в уверенности относительно полезности, которую дают информационные системы, управление связанными с ними рисками и растущие требования к контролю над информацией и ее безопасностью, в настоящее время считаются ключевыми элементами корпоративного управления. Ценность, риск и контроль определяют суть корпоративного управления информационной системой не только в текущем времени, но и долго-

срочной перспективе.

В свою очередь исследования показывают, что наиболее совершенным и многофункциональным инструментарием исследования существующих и вероятных рисков, а также разносторонних проблемных ситуаций является государственный аудит. Государственный аудит в современных условиях становится практически незаменимым инструментарием осуществления разностороннего исследования и оценки информации, принятия управленческих решений, прогнозирования развития всей бизнес-системы и ее информационной системы в частности, а также инструментом поддержки управления этими системами. При этом следует учитывать, что информационная система, являясь по своей сути моделью бизнес-системы, в которой она функционирует, весьма сложное и многофункциональное образование, требующее особого, кропотливого и комплексного подхода к ее исследованию. Поэтому государственный аудит в этих условиях должен быть не аудитом в традиционном смысле, а аудитом бизнеса и, в частности, его информационной системы [1]. Государственному аудиту должна подвергаться не только вся совокупность бизнес-процессов экономического субъекта, но и ИТ-процессов, а также та информация, которая подготовлена с помощью современных информационных технологий.

Расширение использования информационных технологий, объединяемых в единую информационную систему, для получения, обработки, хранения и передачи информации всем заинтересованным в ней пользователям во главу угла ставит проблемы ее защиты, особенно в условиях глобального роста числа информационных угроз, приводящих в случае их реализации к значительным материальным и финансовым потерям. Поэтому для эффективной защиты от указанных как потенциальных, так и существующих угроз бизнес-системам необходима объективная оценка уровня безопасности их информационных систем, которую может предоставить современный аудит, реализуемый как отдельное направление аудита бизнеса, т.е. непосредственно государственный аудит информационной безопасности.

Под информационной безопасностью обычно понимается защищенность информации и поддерживающей ее информационной системы от случайных и преднамеренных воздействий естественного или искусственного характера, наносящих ущерб владельцам или пользователям этой информации и самой поддерживающей ее информационной системе [6].

В свою очередь, под аудитом информационной безопасности в данном контексте следует понимать исследование информации об информационной системе экономического субъекта с целью оценки уровня ее защищенности от перманентных внутренних и внешних угроз и разработки управленческих рекомендаций по их минимизации.

Независимо от размера экономического субъекта и специфики его информационной инфраструктуры работы по обеспечению информационной безопасности обычно включают следующие этапы:

1) формирование политики информационной безопасности;

2) определение границ (масштаба) системы управления информационной безопасностью и постановка конкретных целевых установок ее создания;

3) оценка и управление рисками;

4) выбор контрмер, обеспечивающих надлежащий режим информационной безопасности;

5) аудит системы управления информационной безопасностью.

В свою очередь, каждый из перечисленных этапов имеет свой алгоритм реализации. Так, например, при формировании политики информационной безопасности необходимо:

а) определить используемые нормативно-правовые документы, руководства и стандарты в области информационной безопасности, а также основные положения политики;

б) определить подходы к управлению рисками;

в) структурировать контрмеры по уровням и др. [4].

При определении границ системы управления информационной безопасностью и постановке целевых установок ее создания руководящее звено системы управления должно сформировать документ, отражающий границы системы информационной безопасности, ресурсы, подлежащие защите, и систему критериев оценки их ценности.

На этапе оценки и управления рисками необходимо поставить конкретные задачи их оценки и обосновать требования к самой методике этой оценки. При этом выбор той или иной методики зависит от уровня требований, предъявляемых в бизнес-системе к режиму информационной безопасности, характера принимаемых во внимание угроз и эффективности контрмер. Кроме того, необходимо разработать основополагающую стратегию управления рисками различных классов. При этом обычно используют несколько подходов:

1) уменьшение риска посредством простейших контрмер (смены паролей, снижающей несанкционированный доступ к информации);

2) уклонение от риска, например, посредством вынесения Web-сервера экономического субъекта за пределы локальной сети;

3) изменение характера риска, например, путем страхования оборудования от стихийных бедствий и др.;

4) принятие риска, который остается после принятия контрмер.

В соответствии с выбранной стратегией управления рисками необходимо определить комплекс контрмер, структурированных по уровням (организационному, аппаратно-программному и др.), а также отдельным аспектам информационной безопасности.

И наконец, аудит системы управления информационной безопасностью осуществляется с целью проверки соответствия выбранных контрмер декларированным в политике безопасности целям.

Однако применение государственного аудита только при исследовании контрмер сужает его возможности. Следует отметить, что надлежащий эффект может дать только комплексный и системный подход к аудиту информационной системы.

При этом государственный аудит информационной безопасности может являться лишь элементом системы аудита любой бизнес-системы. Основными целевыми установками указанного направления аудита являются:

1) исследование и анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационных технологий;

2) оценка текущего уровня защищенности информационной инфраструктуры экономического субъекта;

3) локализация «узких мест» в системе защиты;

4) оценка соответствия информационной инфраструктуры существующим требованиям стандартов в области информационной безопасности;

5) выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов информационной безопасности [5].

Как и при аудите состояния информационных систем, аудиторский цикл исследования информационной безопасности предполагает прохождение пяти основополагающих этапов (рис. 1).

Рисунок 1 – Цикл государственного аудита информационной безопасности (ИБ)

Отличительной особенностью выполнения государственного аудита информационной безопасности является несколько иная точка зрения на сбор и обработку сведений об информационной инфраструктуре субъекта, чем при аудите состояния информационных систем. Так, например, при определении границ (масштаба) предстоящего аудита государственному аудитору необходимо учесть:

1) перечень обследуемых физических, программных и информационных ресурсов;
2) помещения, попадающие в границы обследования;
3) организационные, физические, аппаратно-программные и прочие аспекты обеспечения информационной безопасности и их приоритеты.

Принимая задание на проведение государственного аудита информационной безопасности, аудитор должен обозначить именно те проблемы, которые имеют наибольшее значение для данного конкретного субъекта. С этой целью важно осуществить подготовительный этап, то есть определить и согласовать с руководством этого субъекта конкретные цели и направления предстоящего аудиторского процесса. При этом основная роль руководства субъекта как заинтересованного в результатах аудита лица состоит в том, чтобы оказывать всестороннюю поддержку аудитору в уточнении формулировок наиболее значимых для него проблем, а также в подготовке достаточного и надлежащего информационного обеспечения для предстоящего детального аудиторского исследования.

Исходя из этого, подготовительный этап должен завершиться наиболее точной формулировкой основных проблем, стоящих перед субъектом и требующих обязательного решения, а также заключением договора на проведение государственного аудита информационной безопасности. Таким образом, цель этого этапа - обеспечение единства в понимании предстоящего процесса государственного аудита как аудитором, так и клиентом.

Так как обеспечение информационной безопасности - это комплексный процесс, требующий четкой организации и дисциплины, он должен начинаться с определения ролей и распределения ответственности среди должностных лиц, занимающихся безопасностью. Поэтому аудитору необходимо получить знания об организационных структурах пользователей информационных технологий и обслуживающих их подразделений [3].

Осуществляя в ходе сбора исходной информации интервьюирование ответственных и наделенных руководящими полномочиями лиц экономического субъекта, аудитор должен получить следующие сведения о (об):

1) владельцах информации;

2) пользователях (потребителях) информации;
3) провайдерах услуг;
4) характере и путях предоставления услуг конечным потребителям;
5) основных видах функционирующих приложений;
6) количестве и видах пользователей, использующих те или иные приложения;
7) существующих компонентах (элементах) информационной инфраструктуры;
8) функциональности отдельных компонентов;
9) масштабе и границе информационной инфраструктуры;
10) входах в информационную систему (ИТ-процессов);
11) взаимодействии с другими системами (в частности, с системой внутреннего контроля);
12) каналах связи при взаимодействии с другими системами экономического субъекта;
13) каналах связи между компонентами информационной инфраструктуры;
14) протоколах взаимодействия;
15) аппаратно-программных платформах, используемых в информационной инфраструктуре [2].

Кроме перечисленных сведений, аудитору необходимо получить от экономического субъекта:

а) структурные и функциональные схемы;
б) схемы информационных потоков;
в) описание комплекса аппаратных средств информационной инфраструктуры;
г) описание автоматизированных функций;
д) описание основных технических решений;
е) проектную и рабочую документацию на информационную инфраструктуру;
ж) описание структуры программного обеспечения.

Некоторые аспекты, обозначенные на подготовительном этапе, могут пересматриваться и корректироваться в ходе планирования, а также в ходе аудита по существу. При этом любые корректировки и иные изменения необходимо оформлять документально по мере их возникновения, например, в информационном письме руководству субъекта, подтверждающем внесенные изменения.

После подготовки информационной базы для исследования по существу аудиторского задания государственному аудитору необходимо провести анализ собранных сведений. При этом международная практика и многолетний опыт свидетельствуют о трех подходах, которые несколько отличаются друг от друга.

Первый подход основан на использовании существующих стандартов информационной безопасности, которые определяют некий базовый набор требований для широкого класса информационных технологий и которые разрабатываются на основе передового мирового опыта в указанной области знаний, в частности ISO 17799, OCTAVE, Cobit, BS 7799-2 и др. Аудитор, опираясь на регламент указанных Стандартов и полученные сведения о субъекте, должен надлежащим образом определить адекватный набор требований, соответствие которым необходимо обеспечить для конкретной информационной системы. Указанный подход позволяет при минимальных затратах вырабатывать адекватные управленческие рекомендации по совершенствованию информационной безопасности в каждом конкретном случае. Однако основным недостатком этого подхода является отсутствие параметров, характеризующих режим информационной безопасности. При таком подходе можно упустить из поля зрения специфические для конкретной информационной системы классы потенциальных и

даже существующих угроз.

Второй подход основан на использовании в аудиторском исследовании существующих методов анализа рисков, учитывающих индивидуальность каждого субъекта, его информационной инфраструктуры, среды ее функционирования и существующие, а также потенциальные угрозы безопасности. Данный подход является наиболее трудоемким и требует привлечения к исследованию наиболее компетентных в этой области экспертов.

И наконец третий подход – комбинированный, предполагающий использование базового набора требований безопасности, определяемого вышеуказанными стандартами и дополняемого требованиями, учитываемыми при использовании метода анализа рисков. Указанный подход хотя и намного проще второго, так как основой его являются требования безопасности, определенные стандартами, но в то же время он лишен недостатка первого подхода, связанного с тем, что требования стандартов практически не учитывают индивидуальность систем конкретного экономического субъекта [5].

В том случае, когда существуют повышенные требования к информационной безопасности, наиболее приемлемым является третий подход к аудиторскому исследованию. В данном случае государственному аудитору наряду с базовыми требованиями стандартов необходимо надлежащим образом исследовать:

1) бизнес- и ИТ-процессы с позиции информационной безопасности;
2) ресурсы экономического субъекта и их ценность;
3) существующие и потенциальные угрозы информационной безопасности;
4) уязвимости, т.е. слабые места в существующей у субъекта защите информации.

При этом все ресурсы необходимо исследовать с позиции оценки угроз, то есть воздействия вероятных или спланированных действий внутренних или внешних злоумышленников, а также различных нежелательных событий естественного происхождения.

Осуществляя аудиторское исследование информационной безопасности, аудитору необходимо выяснить, может ли быть нанесен ущерб бизнес-системе в целом и ее информационной системе в частности в результате следующих видов угроз:

1) удаленных или локальных атак на ИТ-ресурсы;
2) стихийных бедствий;
3) ошибок, искажений или преднамеренных действий ИТ-персонала;
4) сбоев в работе информационных технологий, выявленных в программном обеспечении или обусловленных неисправностями аппаратных средств [1].

Сама оценка рисков может быть осуществлена с использованием как качественных, так и количественных шкал. В этом случае государственному аудитору необходимо правильно их идентифицировать и проранжировать в соответствии со степенью их критичности для конкретного субъекта. На основе проведенного исследования и оценки рисков вырабатываются адекватные им мероприятия (контрмеры) по их снижению до приемлемого уровня. В каждом конкретном случае рекомендации должны быть конкретными и применимыми к исследуемой информационной системе. Кроме того, указанные рекомендации необходимо обосновать экономически. Следует помнить, что контрмеры по защите организационного уровня должны иметь приоритет над аппаратно-программными методами защиты. В то же время обязательной составляющей цикла аудита информационной безопасности является периодическая проверка соответствия реализованного по результатам аудита режима безопасности политике безопасности и на соответствие установленным критериям.

Логическим завершением любого цикла аудиторского исследования информационной

безопасности являются подготовка и предоставление заинтересованным пользователям отчета о проделанной работе и соответствующих надлежащим образом обоснованных рекомендаций. С этой целью государственный аудитор должен всесторонне изучить и оценить выводы, сделанные на основе проведенного исследования. Структура отчета, как правило, не регламентирована, однако определенные разделы должны в нем обязательно присутствовать. Так, например, в отчете обязательно должна быть раскрыта цель и задачи аудиторского исследования, описаны элементы информационной инфраструктуры, которые подвергались аудиторскому исследованию. В частности, здесь следует раскрыть:

1) назначение и основные функции как информационной инфраструктуры в целом, так и ее отдельных элементов;
2) группы задач, решаемых информационной системой;
3) классификацию ИТ-пользователей;
4) организационную структуру обслуживающего персонала;
5) структуру и состав комплекса аппаратно-программных средств;
6) виды информационных ресурсов;
7) структуру информационных потоков;
8) характеристику каналов взаимодействия с иными системами (в частности, с системой внутреннего контроля и др.), а также входов и выходов [4].

Кроме того, в отчете необходимо указать, что государственный аудит осуществлялся на основе требований стандартов или соответствующих норм. Здесь также отражаются сведения:

1) о местах размещения аппаратно-программных средств субъекта;
2) об основных классах (группах) угроз информационной безопасности, рассмотренных в ходе аудита.

Раскрывая характер аудиторского исследования, в отчете необходимо отразить и саму примененную методику аудиторского исследования, а также критерии оценки величины вероятного ущерба, оценки критичности ИТ-ресурсов и анализа и оценки рисков.

В заключение отчета четко и аргументированно формулируются основные выводы, полученные на основании аудита, а также раскрываются рекомендуемые предложения (контрмеры) как по организационным аспектам деятельности экономического субъекта и, в частности информационной безопасности, так и аппаратно-программным средствам [6].

Подводя итог вышеизложенному, следует подчеркнуть, что государственный аудит информационной безопасности в современных условиях является одним из наиболее эффективных инструментов получения независимой и объективной оценки текущего уровня защищенности любой бизнес-системы как от существующих, так и от потенциальных угроз. Результаты аудита информационной безопасности позволяют сформировать стратегические установки развития отвечающей современным вызовам системы обеспечения информационной безопасности для любого экономического субъекта. Однако следует понимать, что применение на практике аудита информационной безопасности должно быть не эпизодическим, а регулярным, позволяющим не только выявить уже свершившиеся факты, но и предугадать потенциальные угрозы.

Список литературы:

1. Булыга Р.П., Мельник М.В. Аудит бизнеса. Практика и проблемы развития: монография / под ред. Р.П. Булыги. – М.: ЮНИТИ-ДАНА, 2013. – 263 с.

2. Ситнов А.А. Особенности аудита информационных инфраструктур // Аудитор. – 2011. – №11 (201). – С. 26-38.
3. Ситнов А.А. Стандарт Cobit: новые возможности российского аудита // Аудиторские ведомости. – 2012. – № 6. – С. 44-56.
4. Ситнов А.А. Аудит состояния информационной инфраструктуры // Аудитор. – 2012. – № 12 (214). – С. 16-21.
2. Ситнов А.А. Операционный аудит: теория и организация: учебное пособие. – М.: ФОРУМ, 2011. – 403 с.
3. Ситнов А.А., Уринцов А.И. Аудит информационных систем: монография для магистров. – М.: ЮНИТИ-ДАНА, 2014. – 358 с.

Ромашова Любовь Владимировна
студентка 1 курса факультета магистратуры и подготовки кадров высшей квалификации
ФГБОУ ВПО «Орловский государственный институт экономики и торговли»
e-mail: ivanilova30121992@mail.ru

Научный руководитель:
Музалевская Алла Анатольевна
к.п.н., доц. кафедры математики, информатики и информационных технологий
ФГБОУ ВПО «Орловский государственный институт экономики и торговли»
e-mail: maa_orel@yahoo.com

УДК 004.9:005

Нечаева М.А., Зимина Л.В.

ОСОБЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЯ С КЛИЕНТАМИ

За минувшие годы управление взаимоотношениями с клиентами (CRM) стало одной из наиболее известных и обсуждаемых управленческих технологий, а построенные в основе данной концепции CRM-системы являются одними из наиболее популярных на рынке программного обеспечения с целью управления предприятиями.

Многие отделения компании, работая с внешней средой, разобщены между собой. Это ведет к тому, что фирма утрачивает массу способностей увеличения продаж и повышения уровня лояльности клиентов, причем это на сегодняшний день является важным условием стабильности конкурентных преимуществ. Интегрирование покупателя внутрь фирмы, обеспечение ему настоящего персонального обслуживания – вот цель, которую стремится разрешить мировое бизнес-сообщество.

Ключевые слова: CRM-системы, работа с клиентами, управление предприятием.

CRM-система – это набор приложений, позволяющих собирать и сохранять сведения о клиентах, исследовать их и осуществлять конкретные выводы, предоставлять данные сведения сотрудникам в подходящем варианте.

Целью CRM-систем считается приобретение на основе накапливаемых сведений информации, которую возможно применять напрямую с целью увеличения прибыльности и эффективности ведения бизнеса, создавая на основе данных сведений новейшие и вспомогательные услуги для разных групп потребителей. Применение CRM дает возможность продавать покупателю больше товаров и услуг, опираясь на познания того, что он на самом деле