УДК 657.6

Организация аудита информационной безопасности

СИТНОВ АЛЕКСЕЙ АЛЕКСАНДРОВИЧ,
доктор экономических наук, профессор Департамента учета, анализа и аудита,
Финансовый университет, Москва, Россия
55st@mail.ru

Аннотация

В предлагаемой статье отражены и систематизированы взгляды на аудит информационной безопасности экономических субъектов. В результате проведенного исследования автор обобщил современное состояние указанной предметной области аудита и обозначил свою точку зрения на возможности его применения при перманентном влиянии внутренней среды и внешнего окружения на экономические субъекты, раскрыл его существенные преимущества для системы управления этим субъектом.

В статье автором обозначены основные этапы организации процесса проведения аудита информационной безопасности в рамках аудита бизнеса как современной концепции на аудит в целом. Раскрыты особенности каждого из обозначенных этапов, и даны рекомендации по их осуществлению.

Результатом предложенного автором подхода к аудиту информационной безопасности является комплексная модель аудиторского цикла в рамках аудита бизнеса, позволяющая осуществлять исследования указанной предметной области, что служит основой подготовки информации для принятия оптимальных управленческих решений.

Ключевые слова: оценка ресурсов; анализ угроз; анализ уязвимостей; оценка эффективности контрмер; анализ рисков; экономический субъект; бизнес-системы.

The Organization of Auditing of Information Security

SITNOV A. A.,
Doctor of Economics, Professor, Department of Accounting, Analysis and Auditing,
Financial University, Moscow, Russia
55st@mail.ru

Abstract

The article generalizes and systematizes the views of the auditing of information security of the economic subjects. As a result of this research, the author summarized the contemporary condition of the specified subject areas of the auditing and outlined his views regarding the possibility of its application in the condition of permanent influence of the internal environment and the external surroundings on the economic entities, discovered its significant advantages for the system management of this entity.

In the article the author outlines the main organizational stages of the processes of information security auditing within the auditing of the business as a modern concept of auditing in general. The features of each of the above mentioned stages as well as the recommendations for their implementation are discovered in the article.

The result of the proposed by the author industry approach to the information security auditing is a comprehensive model of the auditing cycle within the auditing of the business which in turn allows to carry

out the research of this subject area, which serves as the basis for the preparation of the information for making best and optimal management decisions.

Keywords: assets and resources evaluation; threat assessment; vulnerability assessment; control evaluation; counter-measures efficiency evaluation; risk assessment; the economic subject; business-systems.

Информационные технологии становятся одним из основных инструментов обеспечения адаптивности и конкурентоспособности современных экономических субъектов. При этом трансформация всей структуры мировой рыночной системы в XXI в. обусловлена изменением роли высокотехнологического сектора экономики и переходом его к информационному обществу. В то же время мировая рыночная система характеризуется высокой неопределенностью и все возрастающей динамикой постоянных изменений в бизнес-среде экономических субъектов. Экономические субъекты в этих условиях становятся все более сложными и динамичными бизнес-системами. При этом усложняется как сама структура управления ими, так и обработка, и передача надлежащей информации, которая становится существенной частью их бизнес-процессов.

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 информационной системой экономических субъектов, стабильность и эффективность ее функционирования, а также ее защищенность от перманентных внутренних и главным образом 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 в особенности ее безопасностью в настоящее время считаются ключевыми элементами корпоративного управления. Ценность информации, связанные с ней риски и контроль определяют суть корпоративного управления не только в текущем времени, но и долгосрочной перспективе.

В свою очередь, исследования показывают, что наиболее совершенным и многофункциональным инструментарием оценки существующих и вероятных рисков, а также разносторонних проблемных ситуаций, сопряженных с бизнесом в целом и информационными системами в частности, и является аудит [1].

Развитие наук, направленных на совершенствование современных бизнес-систем, — процесс практически непрерывный и бесконечный, свидетельствующий о перманентности совершенствования аудита и, как следствие, определения его сущности и предметных областей. Можно с уверенностью констатировать: в настоящее время сложилось утвердившееся представление, что современный аудит следует рассматривать как аудит в широком смысле слова, под которым в эпоху информационного общества необходимо понимать не столько аудит отчетности, сколько аудит всего бизнеса, т.е. он должен охватывать все разнообразие типов и целей аудиторских исследований бизнес-систем (экономических субъектов) и их бизнес-среды [2].

Аудит в современных условиях становится практически незаменимым инструментарием осуществления разностороннего исследования и оценки информации, принятия управленческих решений, прогнозирования развития всего бизнеса и его 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 аудиту должны подвергаться не только вся совокупность бизнес-процессов экономического субъекта, но и ИТ-процессы, а также именно та информация, которая подготовлена с помощью современных информационных технологий [1].

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 экономическим субъектам необходима объективная оценка уровня безопасности их информационных систем, которую может предоставить современный аудит, реализуемый как отдельное направление аудита бизнеса, т.е. непосредственно 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 информацией и самой поддерживающей ее информационной системе [3].

Понятие аудита информационной безопасности в настоящее время еще не устоялось, но в данном контексте его можно представить как процесс аудиторского исследования 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. Существует множество случаев, когда целесообразно проводить аудит информационной безопасности, например при подготовке технического задания на проектирование и разработку системы защиты информации, а после внедрения системы безопасности — для оценки уровня ее эффективности.

Независимо от размера экономического субъекта и специфики его информационной инфраструктуры, мероприятия, направленные на обеспечение информационной безопасности для любого бизнеса, обычно содержат этапы, приведенные на *рис. 1*.

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

- определить используемые нормативно-правовые документы, руководства и стандарты в области информационной безопасности, а также основные положения политики;
- определить подходы к управлению рисками;
- структурировать контрмеры по уровням и пр.

При определении границ системы управления информационной безопасностью и постановке целей ее создания руководству экономическим субъектом необходимо сформировать документ, отражающий границы охвата системой информационной безопасности, ресурсы, подлежащие защите, и систему критериев оценки их ценности.

На этапе оценки и управления рисками необходимо прежде всего 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 руководством экономического субъекта 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:

- уменьшение риска посредством простейших контрмер (смена паролей, снижающая несанкционированный доступ к информации);
- уклонение от риска, например посредством вынесения Web-сервера экономического субъекта за пределы локальной сети;
- изменение характера риска, например путем страхования оборудования от стихийных бедствий и пр.;
- принятие риска (риск-аппетит), который остается после принятия контрмер.

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

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

Рис. 1. **Основные этапы мероприятий, направленных на обеспечение информационной безопасности**

Однако применение аудита только при исследовании контрмер сужает его высокопрофессиональные возможности. Следует отметить, что надлежащий эффект может дать только комплексный и системный подход к аудиту информационной системы. При этом аудит информационной безопасности может являться лишь элементом аудита бизнеса. Основными целевыми установками указанного аудита являются:

- исследование и анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационных технологий;
- оценка текущего уровня защищенности информационной инфраструктуры экономического субъекта;
- локализация узких мест в системе защиты;
- оценка соответствия информационной инфраструктуры существующим требованиям стандартов в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов информационной безопасности.

Организуя проведение аудита информационной безопасности, следует учитывать, что аудиторский цикл исследования указанной предметной области предполагает прохождение пяти основополагающих этапов (*рис. 2*) [3].

Особенностью организации аудита информационной безопасности является несколько иная точка зрения на сбор и обработку сведений об информационной инфраструктуре экономического субъекта, чем при аудите состояния информационных систем. Так, например, при определении границ предстоящего аудита аудитору необходимо учесть:

- перечень обследуемых физических, программных и информационных ресурсов;
- помещения, попадающие в границы обследования;
- организационные (нормативно-правовые, административные и процедурные),

физические, аппаратно-программные и прочие аспекты обеспечения информационной безопасности и их приоритеты.

Принимая задание на проведение аудита информационной безопасности, аудитор должен обозначить именно те проблемы, которые имеют наибольшее значение для данного конкретного экономического субъекта. С этой целью важно осуществить подготовительный этап, т.е. определить и согласовать с руководством этого субъекта конкретные цели и направления предстоящего аудиторского процесса. При этом основная роль руководства экономического субъекта как заинтересованного в результатах аудита информационной безопасности 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 предстоящего детального аудиторского исследования.

Исходя из этого, указанный этап должен завершиться наиболее точной формулировкой основных проблем, стоящих перед экономическим субъектом в отношении его информационной безопасности и требующих обязательного решения, а также заключением договора (контракта) на проведение указанного аудита согласно принимаемому аудитором заданию. Таким образом, цель этого этапа — обеспечение единства в понимании предстоящего процесса аудита как аудитором, так и клиентом.

Осуществляя сбор сведений об информационной системе экономического субъекта, аудитору необходимо помнить, что компетентные выводы относительно положения дел в субъекте с информационной безопасностью, а тем более адекватные рекомендации по ее оптимизации

Рис. 2. **Основные этапы аудита информационной безопасности**

могут быть осуществлены только при условии наличия всего массива надлежащих исходных данных для анализа и оценки.

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

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

- о владельцах информации;
- о пользователях (потребителях) информации;
- о провайдерах услуг;
- о характере и путях предоставления услуг конечным потребителям;
- об основных видах функционирующих приложений;
- о количестве и видах пользователей, использующих те или иные приложения;
- о существующих компонентах (элементах) информационной инфраструктуры;
- о функциональности отдельных компонент;
- о масштабе и границе информационной инфраструктуры;
- о входах в информационную систему (ИТ-процессы);
- о взаимодействии с другими системами (в частности, с системой внутреннего контроля);
- о каналах связи при взаимодействии с другими системами экономического субъекта;
- о каналах связи между компонентами информационной инфраструктуры;
- о протоколах взаимодействия;
- об аппаратно-программных платформах, используемых в информационной инфраструктуре.

Кроме перечисленных сведений, аудитору необходимо получить от экономического субъекта:

- структурные и функциональные схемы;
- схемы информационных потоков;
- описание комплекса аппаратных средств информационной инфраструктуры;
- описание автоматизированных функций;
- описание основных технических решений;
- проектную и рабочую документацию на информационную инфраструктуру;
- описание структуры программного обеспечения.

Получение знаний по указанным выше аспектам не должно заканчиваться и при проведении аудита по существу проблем информационной безопасности.

После подготовки информационной базы для исследования аудиторы переходят к анализу собранных сведений.

Подготовительный этап следует завершить письмом согласования задания, подробно раскрывающим все аспекты предстоящего аудита информационной безопасности. При этом следует учитывать, что если аудитор принимает задание от руководства экономического субъекта впервые, то указанное письмо должно быть особенно подробным. Если между субъектами уже существуют долгосрочные отношения по решению тех или иных проблем и реализации тех или иных заданий, то достаточно составить короткое письмо, охватывающее лишь только ключевые аспекты, которые будут решены в процессе предстоящего конкретного аудиторского исследования.

В общем виде письмо согласования задания может иметь произвольный характер. Однако в нем необходимо отразить:

- понимание аудитором проблем информационной безопасности экономического субъекта;
- цель и содержание аудита;
- предметные области и объекты предстоящего исследования;
- общие методические подходы к предстоящему аудиту;
- форму отчетных документов;
- ответственность сторон;
- требования свободного доступа к любой информации, необходимой для проведения аудита;
- требуемые ресурсы;
- краткое изложение ожидаемых результатов от выполнения задания.

Кроме того, в письмо согласования задания допустимо включать стратегические установки

и проект общего плана предстоящего аудита информационной безопасности.

Так как указанное письмо является основой договора (контракта) между аудитором и экономическим субъектом, то, кроме указанных аспектов, в нем необходимо в краткой форме дополнительно раскрыть следующие, не менее важные вопросы:

• ресурсы, которые обеспечивают экономический субъект (в том числе выделение специалистов по тем или иным предметным областям при возникновении в процессе аудита необходимости);

• приблизительный график выполнения работ и ориентировочную продолжительность аудиторского цикла в целом, а также по отдельным этапам;

• общие принципы оплаты выполненных работ.

В то же время следует учитывать, что некоторые из указанных аспектов могут пересматриваться и корректироваться в ходе планирования, а также в ходе аудита по существу аудиторского задания. При этом любые корректировки и иные изменения необходимо оформлять документально по мере их возникновения, например в информационном письме руководству экономического субъекта, подтверждающем внесенные изменения.

Этап заключения договора (контракта) на проведение аудита информационной безопасности, в свою очередь, требует достижения понимания сторонами предстоящего детального аудиторского исследования таких аспектов, как:

• сроки аудиторского исследования (в целом и по этапам);

• предметные области и объекты аудиторского исследования;

• условия конфиденциальности;

• количественный состав аудиторской группы с правом доступа к любой релевантной информации;

• количественный состав группы специалистов-экспертов;

• преемственность аудита (при выполнении работ не впервые);

• состав, сроки и порядок представления экономическому субъекту информации;

• состав, сроки, порядок и форма представления экономическому субъекту как промежуточной аудиторской информации, так и результатов аудита;

• сроки внедрения управленческих рекомендаций, полученных по результатам аудиторского исследования;

• условия мониторинга результатов реализации управленческих решений, выработанных на основе аудиторских рекомендаций;

• условия оплаты работ (в целом и по этапам);

• условия пересмотра договорной цены в ходе проведения аудита (в случаях непредвиденных обстоятельств и дополнительно выявленных аспектов);

• условия расторжения договора (контракта) по желанию одной из сторон;

• прочие вопросы, включая дополнительные пожелания руководства экономического субъекта.

На этапе подготовки проекта договора (контракта) необходимо установить трудоемкость работ, а также график их выполнения на долгосрочную перспективу.

Проект договора (контракта), подготовленный аудитором, направляется руководству экономического субъекта и оформляется аналогично договору (контракту) на проведение аудита финансовой отчетности и оказание сопутствующих аудиту услуг.

После подписания указанного документа, перед тем как будут выдвинуты начальные гипотезы и стратегические установки, а исследуемая проблема будет подвергнута декомпозиции на отдельные компоненты, что, в свою очередь, позволит определить наиболее значимые для них факторы, аудитор должен расширить свои знания о бизнес-системе и ее внешнем окружении.

После подготовки информационной базы для исследования по существу аудиторского задания аудитору необходимо осуществить анализ собранных сведений.

С этой целью международная практика и многолетний опыт рекомендуют три подхода, которые некоторым образом отличаются друг от друга [1, 3].

Это, во-первых, подход, основанный 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 стандартов ISO/IEC 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 экономического субъекта, его информационной инфраструктуры, среды ее функционирования и существующие, а также потенциальные угрозы безопасности. Данный подход является наиболее трудоемким и требует от аудитора привлечения к исследованию наиболее компетентных в этой области аудиторов и экспертов.

Наконец, третий подход — комбинированный, предполагающий использование базового набора требований безопасности, определяемого вышеуказанными стандартами, 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.

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

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

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

В свою очередь, ценность (важность) ресурса, как правило, определяется величиной ущерба, наносимого в случае нарушения информационной безопасности.

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

- удаленные или локальные атаки на ИТ-ресурсы;
- стихийные бедствия;
- ошибки, искажения или преднамеренные действия ИТ-персонала;
- сбои в работе при использовании информационных технологий, вызванные в программном обеспечении или неисправностями аппаратных средств.

Сама оценка рисков может быть дана с использованием как качественных, так и количественных шкал. В этом случае аудитору необходимо правильно их идентифицировать и проранжировать в соответствии со степенью их критичности для конкретного экономического 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 установленным критериям.

Логическим завершением любого цикла аудиторского исследования информационной безопасности является подготовка и предоставление заинтересованным пользователям отчета о проделанной работе и соответствующих, надлежащим образом обоснованных рекомендаций. С этой целью 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 должны быть раскрыты цель и задачи аудиторского исследования, описаны элементы информационной инфраструктуры, которые подвергались аудиторскому исследованию.

Кроме того, в отчете необходимо указать то, что аудит осуществлялся на основе требований стандартов или соответствующих норм.

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

В заключение следует подчеркнуть то, что аудит информационной безопасности в современных условиях является одним из наиболее эффективных инструментов получения независимой и объективной оценки текущего уровня защищенности любого экономического субъекта как от существующих, так и потенциальных угроз. Результаты аудита информационной безопасности позволяют сформировать стратегические установки развития отвечающей современным вызовам системы обеспечения информационной безопасности для указанного 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.

Литература

1. *Ситнов А.А., Уринцов А.И.* Аудит информационных систем: монография для магистров. М.: Юнити-Дана, 2014. 239 с.
2. *Булыга Р.П., Мельник М.В.* Аудит бизнеса. Практика и проблемы развития: монография / под ред. Р.П. Булыги. М.: Юнити-Дана, 2013. 263 с.
3. *Ситнов А.А.* Особенности аудита информационной безопасности бизнес-систем // Аудитор. 2015. № 9 (247). С. 14–22.

References

1. Sitnov A.A., Urintsov A.I. *Audit informatsionnykh sistem*: monografiia dlia magistrov [The auditing of information systems: a monograph for masters]. Moscow, Iuniti-Dana — Yuniti-Dana, 2014, 239 p. (in Russ.).
2. Bulyga R.P., Mel'nik M.V. *Audit biznesa. Praktika i problemy razvitiia*: monografiia / pod red. R.P. Bulygi [The auditing of the business. Practice and the problems of development: a monograph, under the editorship of R.P. Bulyga]. Moscow, Iuniti-Dana — Yuniti-Dana, 2013, 263 p. (in Russ.).
3. Sitnov A.A. Osobennosti audita informatsionnoi bezopasnosti biznes-sistem [The special features of the auditing of information security of business-systems]. *Auditor — Auditor*, 2015, no. 9 (247), pp. 14–22 (in Russ.).