УДК 004.056.5
DOI 10.33764/2618-981X-2023-8-1-150-155

*Е. А. Овчинникова[1], А. В. Троеглазова[2]**

Анализ отдельных подходов к обеспечению информационной безопасности объекта

[1] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: troeglasovaa@mail.ru

Аннотация. В статье рассматриваются отдельные, актуальные подходы к формированию системы информационной безопасности объекта. Применение данных подходов позволяет обеспечить эффективность реализуемых мер по защите информационных активов организации.

Ключевые слова: система обеспечения информационной безопасности, актив, угроза, риск, система управления информационной безопасностью, процессный подход, управленческий подход, риск-ориентированный подход

*E. A. Ovchinnikova[1], A. V. Troeglazova [2]**

Analysis of Individual Approaches to Ensuring the Information Security of an Object

[1] Siberian State University of Telecommunications and Information Science, Novosibirsk, Russian Federation
[2] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: troeglasovaa@mail.ru

Abstract. The article describes separate, topical approaches to the formation of an object's information security system. The use of these approaches makes it possible to ensure the effectiveness of the implemented measures to protect the organization's information assets.

Keywords: information security system, asset, threat, risk, information security management system, process approach, management approach, risk-based approach

Введение

Информация, как один из наиболее значимых ресурсов организации, в зависимости от ее ценности может быть оценена и представлена в стоимостном эквиваленте, который соответствует объему доходов, полученных при ее использовании, или объему расходов, которые несет организация в случае неправомерного воздействия на информацию (ее утечки, утрате или нарушению целостности). Таким образом, целью функционирования системы обеспечения информационной безопасности (СОИБ) является предотвращение или минимизация ущерба, наносимого организации вследствие воздействия на ее информационные активы, в том числе на автоматизированную информационную систему.

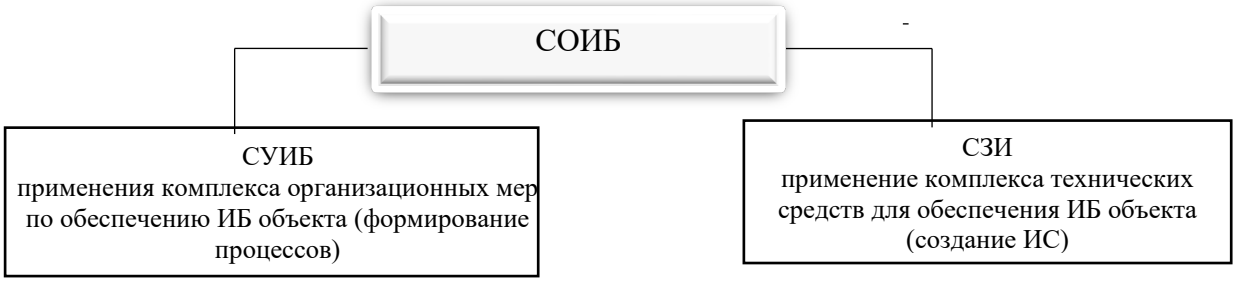

Рис. 1. Конфигурация СОИБ

Таким образом, защищенность объекта (ИС, АИС) обеспечивается посредством применения комплекса организационных мер, направленных на формирование процессов СУИБ, которые могут быть реализованы при условии применения комплекса адекватных технических средств (рис. 1).

Процессный подход

Обеспечение безопасности определенного объекта, то есть состояния защищенности его активов, может быть достигнуто посредством реализации совокупности процессов, которые и образуют систему обеспечения информационной безопасности. Так как, в силу объективных факторов, безопасность не может быть абсолютной, все усилия, в конечном итоге, могут быть направлены только на снижение вероятности реализации потенциальных угроз информационной безопасности (устранение уязвимостей, воздействие на потенциальных нарушителей) и минимизации потерь в случае их реализации.

СОИБ формируется с учетом таких составляющих, как объект и процесс, в рамках которого обеспечивается безопасность защищаемых активов. Состав и содержание процессов обеспечения информационной безопасности (ИБ) зависит от характера объекта (организации), его организационной структуры, масштабов деятельности, специфики обрабатываемой информации, состава и структуры информационной системы, особенностей нормативно-правового регулирования. При этом сформирована стандартизированная совокупность процессов, которые могут быть реализованы на объекте, независимо от его особенностей и целей обеспечения безопасности. Таким образом, деятельность по обеспечению ИБ объекта, осуществляемая посредством последовательной реализации совокупности процессов, образует наиболее востребованный в современных условиях процессный подход.

Процессный подход предполагает, что деятельность по обеспечению ИБ в целом (или большая ее часть) оформляется в логические блоки (процессы), каждый из которых имеет четкие цели реализации, ресурсы, входные и выходные активы. При этом процессы СОИБ рассматриваются как часть общего процесса управления организацией, соответственно, задействованные активы (ресурсы) могут быть использованы другими процессами. Используемый управленческий инструментарий, универсальный для любого бизнес-процесса, показан на рис. 2.

Рис. 2. Обобщенный состав процесса СОИБ

Успешное использование процессов обеспечения информационной безопасности достигается посредством реализации циклической процессной модели Деминга – Шухарта (цикл PDCA). Цикл PDCA позволяет организации эффективно управлять процессами: формировать процессы в соответствии с актуальными требованиями, задействовать адекватные активы, осуществлять управление, определять и реализовывать возможности для улучшения [2]. Достижение целей информационной безопасности и реализуемых в рамках установленных процессов задач определяется эффективностью управления.

Управленческий подход

Вместе с тем, следует учитывать, что ИБ не является основным направлением деятельности организации. Обеспечивая стабильное состояние информационных активов организации (их целостность, конфиденциальность, доступность, неотказуемость), СОИБ призвана создать условия для непрерывного и эффективного осуществления основной деятельности и, соответственно, должна быть имплементирована в общую систему управления организацией.

На рис. 3 приведены три группы процессов, обеспечивающих реализацию основной деятельности организации.

Рис. 3. Высокоуровневые процессы деятельности организации

Являясь частью вспомогательных процессов по отношению к основной деятельности организации, процессы СОИБ, призваны обеспечивать ее непрерывность, эффективность, поддержку и, соответственно, должны быть встроены в общий бизнес-процесс. Таким образом, в рамках СОИБ наряду с процессным походом применяется управленческий подход.

Разделение бизнеса на комплекс четко обозначенных и сформированных процессов повышает возможности координации между подразделениями организации, эффективность контрольных мероприятий, то есть решает системные и поведенческие проблемы.

Система управления информационной безопасностью (СУИБ или СМИБ) реализуется в соответствии с ГОСТ Р ИСО МЭК 27001-2006 в качестве встроенного элемента системы управления организацией. Таким образом, процессы, направленные на обеспечение информационной безопасности, могут быть структурированы и реализованы в контексте общей системы менеджмента качества, основанной на циклической процессной модели.

Процессный подход состоит в формировании и управлении системой процессов в целях достижения намеченных результатов, реализации поставленных задач. Управление ИБ осуществляется в соответствии с политикой информационной безопасности, согласуемой с политикой в области качества и стратегическим направлением деятельности организации [2]. Управление процессами и системой в качестве единого целого может достигаться при использовании цикла PDCA. Вместе с тем, особое внимание следует уделять риск-ориентированному подходу, нацеленному на максимальное использование возможностей ИС и предотвращение нежелательных последствий реализации имеющихся уязвимостей.

Риск-ориентированный подход

Управление информационной безопасностью осуществляется с учетом характерных особенностей ИБ, а именно, неотвратимости наступления события, нарушающего безопасность объекта (инцидента ИБ). В этой связи целями системы управления информационной безопасностью являются следующие (рис. 4):

•снижение рисков информационной безопасности до приемлемого уровня;

•минимизация ущерба вследствие реализации рисков ИБ;

•предотвращение или минимизация инцидентов ИБ.

Риск информационной безопасности – возможность того, что установленная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [2]. Процесс оценки риска включает следующие процедуры (перечень и описание элементов риска представлены в Методике оценки угроз безопасности информации ФСТЭК России (Методика)):

• идентификация риска (3 вида риска);

• описание последствий реализации риска (возможные типовые негативные последствия);

• измерение возможного ущерба вследствие реализации риска, исходя из комбинации вероятности события и его последствия (количественная оценка).

Согласно Методике, риск определяется вероятностью реализации направленной на объект угрозы и исчисляется соответственно нанесенному ущербу. Таким образом, именно величина риска ИБ указывает на уровень защищенности объекта.

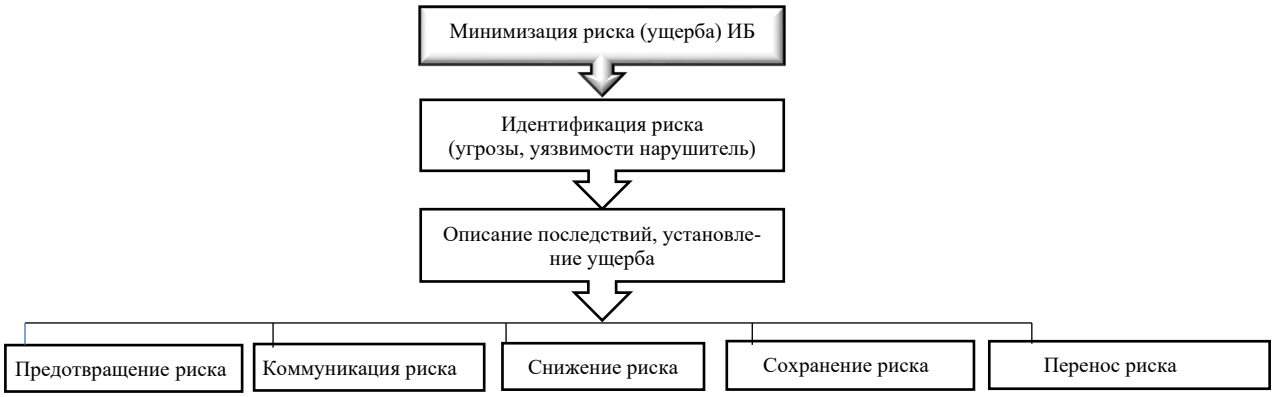

Рис. 4. Управление рисками

Результатом проведенной оценки рисков является принятое управленческое решение, которое может выражаться в следующем [2]:

• предотвращении риска, то есть принятии комплекса правовых, организационных и технических мер по невовлечению в рискованную ситуацию;

• коммуникации риска предполагает оповещение о риске заинтересованных сторон;

• снижении риска, то есть принятие мер по уменьшению вероятности реализации угрозы ИБ, минимизации негативных последствий;

• сохранении (принятие потерь) риска, которое допускается вследствие сопоставления количественного значения последствий риска и затрат на его предотвращение, принятие риска невозможно в том случае, если, согласно закону, данный конкретный вид информации подлежит обязательной защите (персональные данные);

• перенос риска предполагает разделение с другой стороной (организацией-лицензиатом) бремени потерь или выгод.

Принятия риска возможно при условии, что количественное значение его последствий (величина ущерба) ниже или соответствует затратам на предотвращение риска. Вместе с тем, соответствие количественных параметров не является решающим основанием для принятия риска. К отдельным видам информации, конфиденциальность которых, в соответствии с федеральным законом, обеспечивается в обязательном порядке, как например, персональные данные, указанное правило не применяется.

Таким образом, эффективность СОИБ по обеспечению информационной безопасности объекта определяется сравнением величин риска до применения мер ИБ и после их применения, а также уровнем вероятности реализации угроз безопасности объекта.

Процессы обеспечения информационной безопасности объекта являются циклическими, учитывают реалии современного развития информационного пространства, особенности основной деятельности организации. Эффективность мер ИБ также обеспечивается использованием различных механизмов контроля и постоянным совершенствованием реализуемых процессов.

Обсуждение

В статье приводятся наиболее востребованные на современном этапе подходы к обеспечению информационной безопасности организации. Каждый из таких подходов встроен в общую систему правовых механизмов СОИБ (в том числе посредством национальных стандартов и нормативных документов регулирующих ведомств).

• процессный подход рассматривает СОИБ как систему взаимосвязанных процессов;

• управленческий подход предполагает использование совокупности механизмов управления с целью реализации процессов СОИБ, как вспомогательного элемента системы управления организацией;

• риск-ориентированный подход основан на предположении неизбежности наступления события ИБ и, соответственно, поиске эффективных механизмов минимизации рисков (вероятности) возникновения инцидента ИБ и его последствий (ущерба).

Обозначенные подходы формируются с учетом особенностей организации и реализуются в комплексе соответственно циклу PDCA.

Заключение

Содержание приведенных в статье подходов к обеспечению информационной безопасности объекта указывает на необходимость их комплексного применения с учетом особенностей информационных активов организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»: дата введения 2011-12-01. – Режим доступа: https://docs.cntd.ru/document/1200058325 (дата обращения: 24.03.2022). – Текст электронный.