И. И. Зензин

МЕТОДИКИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Введение

Проблема обеспечения безопасности информационных систем в современном мире усложняется отсутствием единой методической базы, позволяющей проводить адекватную оценку угроз информационным ресурсам, а также степени защищенности систем в информационной сфере. Для оценки угроз и управления защищенностью зачастую используется аппарат анализа и управления рисками.

Подход на основе анализа рисков используется в различных сферах, в частности в экономике. В сфере обеспечения безопасности информационных систем анализ и управление рисками применяются сравнительно недавно. В 90-е годы прошлого века и в начале текущего десятилетия в мире были разработаны несколько стандартов, использующих управление рисками для систем обработки информации (ISO 17799, ISO 27001).

Информационная система представляет собой множество взаимодействующих компонентов, для этого множества формируется совокупность угроз безопасности. Характер взаимодействия угроз определяет общую оценку риска для системы. Проблема определения общего риска для совокупности сложных взаимодействующих угроз на данном этапе не решена в полной мере. У большинства существующих методов управления рисками есть ключевой недостаток в виде наличия следующих противоположных друг другу свойств: исключительно качественный и жестко формализованный подход к анализу рисков. Существующие методики зачастую не учитывают характер взаимодействия различных негативных факторов и дают оценку только на качественном уровне.

Принципиальная сложность проведения анализа рисков для информационных систем заключается в том, что для достижения адекватных оценок необходимо учитывать огромное количество факторов, которые находятся в сложной зависимости друг от друга. Причем зачастую достаточно трудно оценить степень достоверности полученного результата, поскольку при проведении анализа невозможно учесть все факторы.

1. Положения стандарта ISO IEC 17799 (ГОСТ Р ИСО/МЭК 17799-2005) в области управления рисками информационной безопасности

Согласно стандарту, информационная безопасность — механизм защиты, обеспечивающий [1]:

- *конфиденциальность:* доступ к информации только авторизованных пользователей;
- *целостность:* достоверность и полноту информации и методов ее обработки;
- *доступность:* доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения.

Требования к информационной безопасности определяются с помощью систематической оценки рисков. Решения о расходах на мероприятия по управлению информационной безопасностью должны приниматься исходя из возможного ущерба, нанесенного бизнесу в результате нарушений информационной безопасности.

Методы оценки риска могут применяться как для всей организации, так и для какой-либо ее части, отдельных информационных систем, определенных компонентов систем или услуг, а именно там, где это практически выполнимо и целесообразно.

Оценка риска — это систематический анализ:
- вероятного ущерба, наносимого бизнесу в результате нарушений информационной безопасности с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации и других активов;
- вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью.

Результаты этой оценки помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрению мероприятий по управлению информационной безопасностью с целью минимизации этих рисков.

Некоторые мероприятия по управлению информационной безопасностью, приведенные в настоящем стандарте, могут рассматриваться как руководящие принципы для управления безопасностью и применяться для большинства организаций [1].

Таким образом, документ определяет себе место в нормативной базе по управлению информационными рисками как основной набор средств, используя которые можно воздействовать на общий уровень риска для системы. Это отражено в первой части документа, отражающей область его применения.

Рассматриваемый стандарт предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями [1].

2. Стандарт ISO IEC 27001 (ГОСТ Р ИСО/МЭК 27001-2005) об управлении рисками информационной безопасности

Документ абстрагирован от конкретных мероприятий по защите, определяя общую стратегию управления безопасностью информации организации.

Данный международный стандарт был подготовлен для того, чтобы предоставить модель для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения Системы менеджмента защиты информации (СМЗИ). Предполагается, что принятие СМЗИ было стратегическим решением для организации.

Согласно документу, необходимо применять процессный подход к управлению защитой информации [2].

Этот международный стандарт принимает процессный подход для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения СМЗИ организации.

Организации нужно идентифицировать много видов деятельности и управлять ими для того, чтобы функционировать результативно. Любой вид деятельности, использующий ресурсы и управляемый для того, чтобы дать возможность преобразования входов в выходы, можно считать процессом. Часто выход одного процесса непосредственно образует вход следующего процесса.

Применение системы процессов в рамках организации вместе с идентификацией и взаимодействием этих процессов, а также их управлением может называться «процессный подход».

Организация должна выявить изменившиеся риски и определить требования к предупреждающим действиям, сосредоточив внимание на значительно изменившихся рисках. Приоритет предупреждающих действий должен быть определен на основе результатов оценки риска.

Стандарт ГОСТ Р ИСО/МЭК 27001-2005 и соответственно международный стандарт ISO IEC 27001:2005 устанавливают общие принципы ведения защиты организаций в информационной сфере. Вообще говоря, стандарт отходит от конкретных практических реализаций, рассматривая общие организационные моменты управления информационной

безопасностью систем. Важно отметить, что управление защищенностью организации в стандарте, который планируется как основа для серии стандартов в области информационной безопасности, является стержневым подходом для анализа и управления рисками. Документ определяет порядок проведения данного анализа, общий характер работы по обеспечению информационной безопасности организации [2].

Существенно и то, что рассмотренный ранее стандарт ГОСТ Р ИСО/МЭК 17799-2005 является дополнением этого стандарта в плане конкретизации мероприятий по управлению информационными рисками для определенных случаев. Таким образом, стандарты представляют собой связанные документы, и обеспечение информационной безопасности организации — это процесс планомерного совместного применения этих стандартов.

3. Стандарт BS 7799-3 — «Руководство по управлению информационными рисками»

Стандарт Великобритании BS 7799 посвящен управлению информационной безопасностью организации. Этот стандарт является одним из наиболее авторитетных в мире. На его базе разработаны международный стандарт ISO IEC 17799, позже эволюционировавший в ISO IEC 27002. Третья часть данного стандарта представляет особый интерес, поскольку целиком посвящена вопросам управления информационными рисками.

Стандарт BS 7799-3 содержит вводную часть, разделы по оценке рисков, обработке рисков, непрерывным действиям по управлению рисками, а также имеет приложение с примерами активов, угроз, уязвимостей, методов оценки рисков. Стандарт придерживается самого общего понятия риска, под которым понимают комбинацию вероятности события и его последствий (стоимости компрометируемого ресурса). Управление риском (risk management) сформулировано как скоординированные непрерывные действия по управлению и контролю рисков в организации.

BS 7799-3 допускает использование как количественных, так и качественных методов оценки рисков, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методологического аппарата оценки рисков ИБ.

Отличительной чертой стандарта является принцип осведомленности о процессах оценки, отработки, контроля и оптимизации рисков в организации. На каждом этапе предусмотрено информирование всех участников процесса управления безопасностью, а также фиксирование событий СУИБ.

4. Стандарт NIST 800-30 — «Руководство по управлению информационными рисками ИТ-систем»

Стандарт Национального института стандартов и технологии США NIST 800-30 был опубликован в июле 2002 г. В своем введении документ определяет важную роль управления рисками (risk management) в обеспечении безопасности информационных технологий. Основной задачей менеджмента информационных рисков в соответствии с документом является обеспечение защищенности интересов организации, причем не только в информационной сфере. Стандарт определяет роль менеджмента информационных рисков как важной части управления организацией. Под управлением информационными рисками предполагается, прежде всего, организационная деятельность, а затем уже технические аспекты обеспечения информационной безопасности.

Понятие риска в документе достаточно близко к тем, которые были рассмотрены в рамках анализа других стандартов. Риском в соответствии с рассматриваемым стандартом является комбинация вероятности события и уровня негативного воздействия на систему.

Анализ документа показывает [3], что подходы к менеджменту в области информационной безопасности в американском стандарте NIST 800-30 и британском стандарте BS 7799-3 (проекте

ISO IEC 27005) достаточно близки друг к другу. Стандарты не противоречат друг другу, и при этом налицо определенное сходство между подходами к управлению информационными рисками.

Заключение

В работе представлен краткий обзор четырех современных стандартов в области управления рисками информационной безопасности. На сегодняшний день в российской нормативной базе в области информационной безопасности отсутствует ГОСТ по управлению информационными рисками. Из трех частей стандарта BS 7799 перевод имеют лишь две – ГОСТ Р ИСО/МЭК 17799 (представлены требования к системе менеджмента информационной безопасности) и ГОСТ Р ИСО/МЭК 27001 (имеются примеры по среде и системам информационной безопасности), при этом отсутствует руководство по оценке и управлению рисками. Таким образом, при необходимости приложения на практике руководства по управлению рисками целесообразно обратиться к оригиналу третьей части британского стандарта BS 7799.

Необходимость рассмотрения различного рода современных стандартов обусловлена актуальностью проблемы поиска и разработки универсальной методики управления рисками информационной безопасности. Проблеме выбора меры риска посвящено множество исследований, в частности в области экономики. В области обеспечения информационной безопасности ситуация усложняется разнородностью исследуемых процессов. Поэтому представляется наиболее разумным ввод мер риска для информационной системы, имеющих обобщенный характер. Это позволит, используя набор данных, полученных для каждого процесса при произвольной методике оценки, собрать выходные данные по системе в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006. – 56 с.
2. ГОСТ Р ИСО/МЭК 27001-2005. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2006. – 31 с.
3. *Остапенко О. А., Карпеев Д. О., Асеев В. Н.* Риски систем: оценка и управление / Под ред. Ю. Н. Лаврухина. М.: Горячая линия–Телеком, 2007. – 247 с.