# Уменьшение риска

написано Александр Астахов | 11 июня, 2023
Если риск неприемлем, то обычно в первую очередь рассматривается вопрос о его уменьшении до уровня, который был определен как максимально допустимый, путем применения соответствующих механизмов контроля.

Одним из наиболее авторитетных источников для выбора механизмов контроля служат международные стандарты ISO 27001 (Приложение A) и ISO 27002, предоставляющие описание и руководство по внедрению для каждого механизма контроля. В стандарте ISO 15408 «Общие критерии оценки безопасности информационных технологий» и разработанных на его основе профилях защиты можно найти соответствующие требования и подобрать спецификацию практически для любых программно-технических механизмов контроля. Заслуживает также внимания немецкий стандарт в области ИТ безопасности BSI/IT Baseline Protection Manual.

Список источников информации о контрмерах, применяемых для уменьшения рисков не исчерпывается названными стандартами. Подробную информацию по отдельным областям контроля можно почерпнуть из других международных стандартов, которых насчитывается несколько десятков наименований. Перечислим лишь некоторые из них:

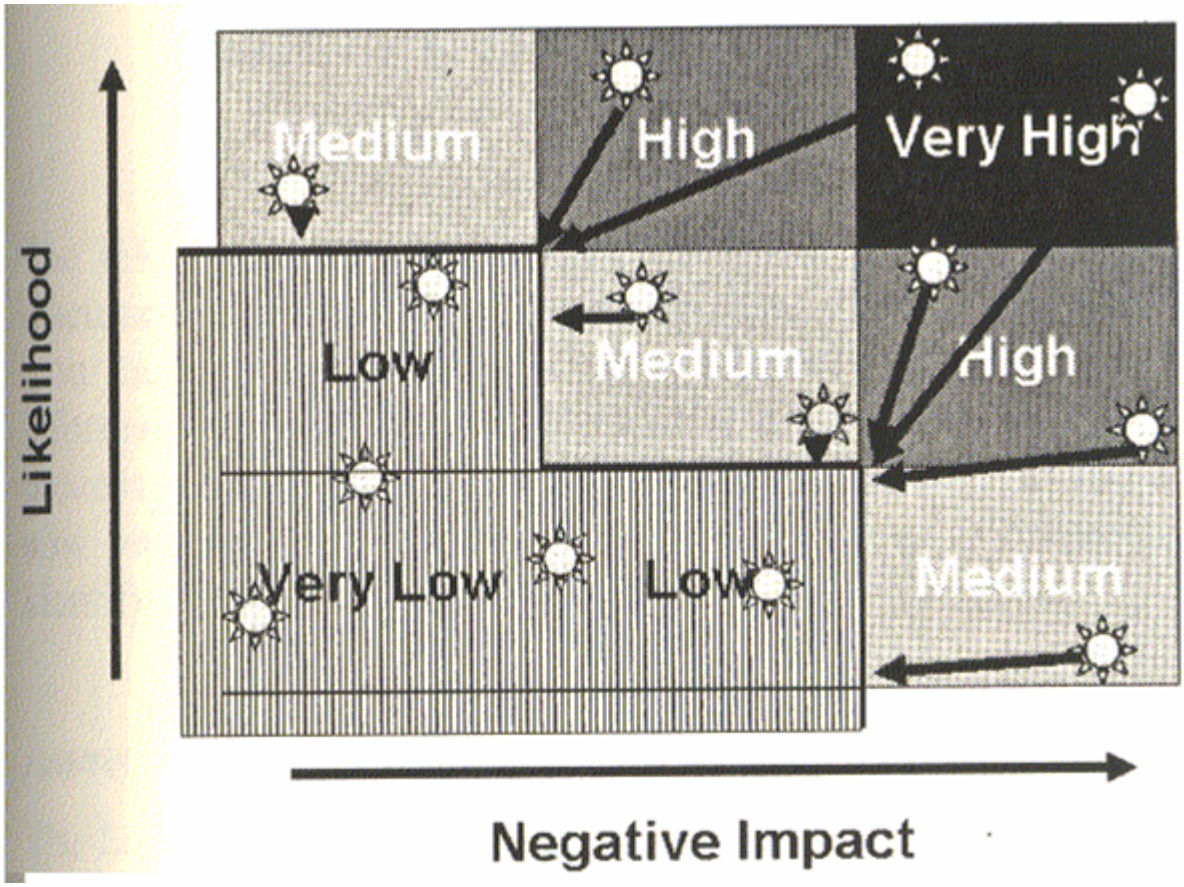
- ISO 13335 – группа стандартов «Информационные технологии. Руководство по управлению ИТ безопасностью»;
- ISO 18044 – стандарт «Информационные технологии. Методы обеспечения безопасности. Управление инцидентами информационной безопасности»;
- ISO 18043 – стандарт «Информационные технологии. Методы обеспечения безопасности. Выбор, развертывание и эксплуатация систем обнаружения вторжений»;
- ISO 13569 – стандарт «Финансовые сервисы. Руководство по обеспечению информационной безопасности»;

- ISO 13888 – группа стандартов «Методы обеспечения ИТ безопасности. Неотказуемость. Общие положения»;
- ISO 19794 – группа стандартов «Информационные технологии. Форматы обмена биометрическими данными»;
- ISO 18028 – группа стандартов «Информационные технологии. Методы обеспечения безопасности. Безопасность ИТ сетей»

---

*Международные и национальные стандарты можно приобрести в интернет-магазине shop.globaltrust.ru, являющемся официальным дистрибьютором Британского института стандартов.*

---




Механизмами контроля в международных стандартах называют любые меры, направленные на уменьшение риска. Уменьшать риски можно следующими способами:

- уменьшением вероятности воздействия угрозы на активы;

- ликвидацией имеющихся уязвимостей;
- уменьшением вероятности использования уязвимости;
- уменьшением возможного ущерба в случае осуществления риска путем обнаружения нежелательных событий, реагирования и восстановления после них.

Какой из этих способов (или их комбинацию) организация выбирает для защиты своих активов, зависит от требований бизнеса, внешней среды и обстоятельств. Выбор механизмов контроля должен быть обоснован. Основными критериями такого выбора служат его реализуемость, эффективность в достижении целей контроля и экономическая целесообразность, измеряемая коэффициентом возврата инвестиций (ROI). Каким образом определяется ROI, мы рассмотрим ниже в разделе «Оценка возврата инвестиций в информационную безопасность».

Не существует универсального или достаточно общего подхода к выбору целей и механизмов контроля. Процесс выбора, вероятно, будет включать в себя большое количество этапов принятия решения, консультации и обсуждения с представителями бизнеса и ключевыми лицами, а также анализ целей бизнеса. Процесс выбора должен базироваться на четко определенном наборе целей и задач бизнеса или его миссии и произвести результаты, которые наилучшим образом подходят для организации в терминах требований бизнеса по защите его активов и инвестиций, культуры организации и ее терпимости к риску.

Выбор механизмов контроля опирается на результаты оценки риска. Анализ уязвимости или угрозы может показать, где требуется защита и какие формы она должна принимать. Любые подобные ссылки на оценку рисков должны быть документированы с целью обоснования выбора (либо исключения) механизмов контроля. Документирование выбранных механизмов контроля, наряду с целями контроля, для достижения которых они предназначены, в декларации о применимости и в плане обработки рисков (об этих документах пойдет речь ниже) является важным условием для сертификации по стандарту ISO 27001, а также

помогает организации далее непрерывно отслеживать ход внедрения и эффективность механизмов контроля.

При выборе механизмов контроля должно учитываться большое количество других факторов, включая:

- простоту внедрения и эксплуатации механизма контроля;
- надежность и воспроизводимость механизма контроля (является ли он документированным, исполняется он вручную или запрограммирован);
- относительную силу механизмов контроля по сравнению с другими мерами;
- типы выполняемых функций (предотвращение, сдерживание, обнаружение, восстановление, исправление, мониторинг или оповещение).

На выбор механизмов контроля могут повлиять следующие ограничения:

- *время реализации*– может быть неприемлемым, например, превышать жизненный цикл процесса, для которого требуется уменьшить риск;
- *законодательные*– ограничения на использование средств шифрования;
- *кадровые*– доступность специализированного персонала;
- *этические*– не во всех организациях уместна перлюстрация почты, а сообщения о подозрительных действиях в ряде случаев могут трактоваться как доносительство;
- *культурные*– досмотр сумок можно ввести в Европе, но это недопустимо в странах Ближнего Востока. Успешность внедрения в значительной степени зависит от поддержки со стороны персонала;
- *операционные*– необходимость обеспечения непрерывной доступности системы 24 часа в сутки.