Приложение 0. Термины и определения в области управления информационными рисками

написано Александр Астахов | 11 июня, 2023

В данной книге используются термины и определения, приведенные в русских редакциях стандартов ISO 27001, ISO 27002, ISO 27005 и BS 7799-3, а также перечисленные ниже.

Актив (ресурс)– все, что имеет ценность для организации [ISO/IEC 13335-1:2004].

Конфиденциальность– свойство, заключающееся в недоступности информации или нераскрытии ее содержания для неавторизованных лиц, субъектов или процессов [ISO/IEC 13335-1:2004].

Целостность– свойство, заключающееся в обеспечении точности и полноты ресурсов [ISO/IEC 13335-1:2004].

Доступность– свойство, заключающееся в доступности и применимости для авторизованных субъектов, когда потребуется [ISO/IEC 13335-1:2004].

Информационная безопасность– обеспечение конфиденциальности, целостности и доступности информации; дополнительно также могут подразумеваться другие свойства, такие как аутентичность, подотчетность, неотказуемость и надежность [ISO/IEC 17799:2005].

Событие информационной безопасности– идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности [ISO/IECTR18044:2004].

Инцидент информационной безопасности– одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес-операций или представляющих угрозу для информационной безопасности [ISO/IECTR18044:2004].

Угроза– потенциальная причина инцидента, который может нанести ущерб системе или организации [ISO/IEC 13335-1:2004].

Уязвимость– слабость ресурса или группы ресурсов, которая может использоваться при реализации одной или более угроз [ISO/IEC 13335-1:2004].

Воздействие– неблагоприятное изменение уровня достижения целей бизнеса.

Риск– комбинация вероятности события и его последствий[ISO Guide 73:2002].

Риск информационной безопасности– потенциальная возможность использования определенной угрозой уязвимостей актива или группы активов для причинения вреда организации.

ПРИМЕЧАНИЕ. Определяется в терминах комбинации вероятности события и его последствий.

Остаточный риск– риск, остающийся после обработки риска[ISO Guide 73:2002].

Идентификация риска– процесс, направленный на нахождение, перечисление и описание элементов риска [ISO/IECGuide73:2002].

Анализ риска– систематическое использование информации для идентификации источников и оценки величины риска[ISO Guide 73:2002].

ПРИМЕЧАНИЕ 1. Анализ рисков служит основой для оценивания рисков, обработки рисков и принятия рисков.

ПРИМЕЧАНИЕ 2. Информация может включать в себя исторические

данные, теоретический анализ, компетентные мнения и интересы владельцев бизнеса.

Расчет риска– процесс присвоения значений вероятности и последствиям риска [ISO/IECGuide73:2002].

ПРИМЕЧАНИЕ В ISO 27005 при описании расчета рисков для обозначения термина «вероятность» в английской версии используется термин «likelihood» вместо математического термина «probability».

Оценивание риска– процесс сравнения оценочной величины риска с установленным критерием риска с целью определения уровня значимости риска [ISO Guide 73:2002].

Оценка риска– общий процесс анализа и оценивания риска [ISO Guide 73:2002].

Обработка риска– процесс выбора и реализации мер по модификации риска [ISO Guide 73:2002].

ПРИМЕЧАНИЕ 1. Термин «обработка риска» иногда используется для обозначения самих мер.

ПРИМЕЧАНИЕ 2. Меры по обработке риска могут включать в себя избежание, уменьшение, передачу или сохранение риска.

ПРИМЕЧАНИЕ 3. В BS 7799-3 термин «механизм контроля» используется в качестве синонима для термина «мера».

Избежание риска – решение не принимать участия в ситуации, сопряженной с риском, или действие, направленное на выход из нее [ISO Guide 73:2002].

ПРИМЕЧАНИЕ. Решение может быть принято на основании результатов оценивания риска.

Уменьшение риска – меры, принимаемые для снижения вероятности или негативных последствий, связанных с риском, или того и другого [ISO/IECGuide73:2002].

ПРИМЕЧАНИЕ. В ISO 27005 при описании расчета рисков для обозначения термина «вероятность» в английской версии используется термин «likelihoo»” вместо математического термина «probability».

Сохранение (принятие) риска– принятие бремени убытка или извлекаемой выгоды от конкретного риска [ISO/IECGuide73:2002].

ПРИМЕЧАНИЕ. В контексте рисков информационной безопасности при описании сохранения риска учитываются только негативные последствия (убытки).

Передача риска– разделение с другой стороной бремени убытка или извлекаемой выгоды, связанной с риском [ISO/IECGuide73:2002].

ПРИМЕЧАНИЕ 1. В контексте рисков информационной безопасности при описании передачи риска учитываются только негативные последствия (убытки).

ПРИМЕЧАНИЕ 2. Требования законодательства или нормативной базы могут ограничивать, запрещать или предписывать передачу определенного риска.

ПРИМЕЧАНИЕ 3. Передача риска может осуществляться путем заключения договоров страхования или других договоров.

ПРИМЕЧАНИЕ 4. Передача риска может порождать другие риски или модифицировать существующий риск.

ПРИМЕЧАНИЕ 5. Перемещение источника не является передачей риска.

Контроль риска– действия, реализующие решения по управлению риском [ISO Guide 73:2002].

ПРИМЕЧАНИЕ. Контроль риска может включать в себя мониторинг, повторное оценивание и исполнение принятых решений.

Критерии риска– показатели, при помощи которых оценивается

значимость риска [ISO Guide 73:2002].

ПРИМЕЧАНИЕ. Критерии риска могут включать в себя связанные с ним расходы и извлекаемые выгоды, требования законодательства и нормативной базы, социально-экономические аспекты и аспекты, связанные с окружающей средой, интересы владельцев бизнеса, приоритеты и другие входные данные для оценки.

Управление риском– скоординированные действия по управлению и контролю организации в отношении риска [ISO Guide 73:2002].

ПРИМЕЧАНИЕ. Управление риском обычно включает в себя оценку риска, обработку риска, принятие риска и сообщение о риске.

Система управления рисками– набор элементов системы управления организацией, предназначенных для управления рисками [ISO Guide 73:2002].

ПРИМЕЧАНИЕ 1. Элементы системы управления могут включать в себя стратегическое планирование, принятие решений и другие процессы, имеющие дело с рисками.

ПРИМЕЧАНИЕ 2. Культура организации отражается в ее системе управления рисками.

Коммуникация риска– обмен или совместное использование информации о риске между лицом, принимающим решения, и другими заинтересованными сторонами [ISO/IECGuide73:2002].

ПРИМЕЧАНИЕ: Информация может относиться к существованию, природе, форме, вероятности, опасности, приемлемости, обработке или другим аспектам риска.

Система управления информационной безопасностью (СУИБ)– та часть общей системы управления, основанной на оценке бизнес рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

ПРИМЕЧАНИЕ: Система управления включает в себя организационную

структуру, политики, действия по планированию, распределение ответственности, практики, процедуры, процессы и ресурсы.

Декларация о применимости– документированное заявление, описывающее цели и механизмы контроля, которые имеют отношение и применимы к СУИБ организации.

ПРИМЕЧАНИЕ: Цели и механизмы контроля базируются на результатах и выводах, полученных в процессе оценки рисков и обработки рисков, законодательных требованиях и требованиях нормативной базы, договорных обязательствах и бизнес-требованиях организации к информационной безопасности.