Определение ценности активов

написано Александр Астахов | 10 июня, 2023

Идентификация и определение ценности активов, исходя из потребностей бизнеса организации, являются основными факторами в оценке риска. Для того чтобы определить требуемый уровень защиты активов, необходимо оценить их ценность с точки зрения важности этих активов для бизнеса. Важно учитывать идентифицированные законодательные требования, требования бизнеса и контрактных обязательств, а также последствия нарушения конфиденциальности, целостности и доступности этих активов.

Этапы определения ценности активов:

- *Определение шкалы ценности активов.*
- *Определение критериев оценки ущерба.*
- *Получение исходных данных для оценки от владельцев и пользователей активов.*
- *Определение последствий для бизнеса в результате нарушения конфиденциальности, целостности и доступности актива.*
- *Определение ценности актива отдельно для каждого из трех свойств.*

Исходные данные для определения ценности активов могут быть предоставлены владельцами и пользователями этих активов, которые способны авторитетно рассуждать о ценности конкретной информации для организации, а также о том, каким образом активы используются для осуществления бизнес-процессов и какую роль в достижении целей бизнеса они играют. Для того чтобы единообразно определять ценность активов, должна быть определена соответствующая шкала ценности активов.

Для каждого из свойств актива, таких как конфиденциальность, целостность или доступность, должно быть определено отдельное значение ценности, так как эти значения являются независимыми и могут варьироваться для каждого из активов.

Согласно ISO 27002 (раздел 7.2) информация и другие активы организации должны быть классифицированы в соответствии с идентифицированной ценностью активов, законодательными и бизнес-требованиями и уровнем критичности. Классификация показывает потребность, приоритеты и ожидаемый уровень защиты при обращении с информацией. Определение классификации, а также ее пересмотр с целью предоставления гарантий того, что классификация остается на соответствующем уровне, входит в обязанности владельца актива.

Классификация последствий нарушения безопасности активов:

- *Последствия угроз:*

- *К – нарушение конфиденциальности;*
- *Ц – нарушение целостности;*
- *Д – нарушение доступности.*
- *Последствия нарушения требований:*

- *Т1 – нарушение требований бизнеса;*
- *Т2 – нарушение контрактных обязательств;*
- *Т3 – нарушение законодательства.*

Что касается активов, не относящихся к категории информационных (помещения, оборудование, носители информации, кадровые ресурсы и прочие материальные активы), то определение собственной ценности этих активов (без учета их влияния на

соответствующие информационные активы) при анализе информационных рисков является необязательным, т.к. множество рассматриваемых нами рисков охватывает только информационные активы. Другими словами, при выходе из строя сервера рассматривается ущерб, связанный с недоступностью и необходимостью затрат на восстановление связанных с этим сервером информационных активов, при этом стоимость замены или ремонта самого сервера может и не учитываться. Такой подход позволяет упростить оценку рисков без ущерба для ее объективности.

В большинстве случаев критичность программного обеспечения оценивается так же, как и для технических средств, в терминах его восстановления или замены. В этом случае необходимо оценить лишь финансовые потери от его разрушения. Однако в некоторых случаях программное обеспечение может иметь собственную ценность, заключающуюся, например, в обеспечении конфиденциальности и целостности исходных текстов программ, представлять собой объект интеллектуальной собственности и относиться к категории коммерческой тайны. В этих случаях критичность программного обеспечения оценивается так же, как и для информационных активов.

Вычисление суммарной ценности активов производится с учетом взаимосвязей между различными видами активов. Суммарная ценность физических активов определяется собственной ценностью, а также ценностью связанных с ними информационных активов и программного обеспечения. Суммарная ценность программного обеспечения определяется собственной ценностью, а также ценностью связанных с ним информационных активов.

Суммарная ценность каждого отдельно взятого актива может быть представлена матрицей ценности актива, где по вертикали указываются последствия воздействия угроз на актив, по горизонтали — категория требований, которые при этом нарушаются, а на пересечении — качественное либо количественное значение ценности актива.

	Требования бизнеса	Требования законодательства	Контрактные обязательства
Конфиденциальность			
Целостность			
Доступность			
Аутентичность			
Неотказуемость			

Для заполнения данной матрицы, необходимо определить качественную шкалу ценности активов и критерии оценки ущерба.