Приложение 4. Базовый опросник для определения степени критичности систем по методу CRAMM

написано Александр Астахов | 11 июня, 2023

Этот опросник служит для определения степени критичности обследуемой системы и глубины проводимого обследования. Он заполняется владельцем или пользователем информационной системы, представляющим себе величину ущерба, который может быть нанесен ему, организации, государству или конкретным людям в случае инцидента информационной безопасности.

Для принятия правильного решения относительно глубины проводимого обследования нужны как можно более точные и полные ответы на представленные вопросы с рассмотрением возможных сценариев нарушения информационной безопасности.

Оценка возможного ущерба от нарушений информационной безопасности дается на основе знаний о видах, объеме и степени критичности информации, хранимой и обрабатываемой в системе.

Рассматриваются следующие виды нарушений информационной безопасности:

- Несанкционированное раскрытие конфиденциальной информации.
- Нарушение целостности информации (разрушение или несанкционированное изменение).
- Потеря доступности информации в результате отказа технических средств, приложений и т.п.

Вопросы для оценки возможного ущерба:

1. Может ли в результате нарушения информационной безопасности быть причинен более-менее значительный ущерб здоровью или личности (моральный, финансовый и т.п.) одного или несколько индивидуумов?
2. Могут ли ошибки, допущенные при формулировании требований или реализации политики безопасности, нанести более-менее значительный ущерб здоровью или личности (моральный, финансовый и т. п.) одного или несколько индивидуумов?
3. Может ли отказ исполнить юридические или договорные обязательства в результате нарушения информационной безопасности повлечь предупреждение, гражданский иск или уголовное расследование или привести к финансовым потерям/штрафу для организации или ответственных лиц?
4. Может ли нарушение информационной безопасности способствовать совершению преступления или препятствовать расследованию преступления?
5. Хранятся ли в системе коммерческие или экономические данные, стоимость которых для конкурентов оценивается выше X руб.?
6. Может ли компрометация коммерческих или экономических данных привести к финансовым потерям или потери платежеспособности организации или привести к получению выгоды или конкурентных преимуществ для индивидуумов или организаций?
7. Может ли по причине упущений, допущенных при организации защиты коммерческих или экономических данных, быть нарушена конфиденциальность информации, предоставленной третьими сторонами?
8. Могут ли прямые или косвенные финансовые потери в результате нарушения информационной безопасности составить более X руб.?
9. Может ли снижение работоспособности организации в результате нарушения информационной безопасности прямо или косвенно привести к потерям больше чем X руб.?
10. Могут ли проблемы с информационной безопасностью привести к нарушению производственной дисциплины,

общественного порядка или вызвать массовые волнения?

11. Могут ли быть нарушены процессы управления организацией или бизнес-процессы в результате нарушения информационной безопасности?
12. Может ли нарушение информационной безопасности неблагоприятно повлиять на отношения с акционерами, поставщиками, органами надзора, правительством, другими организациями или общественностью и привести к антирекламе в средствах массовой информации?
13. Превышает ли стоимость ремонта или замены всех программно-технических средств системы X руб.?