## Тема: *Стратегия применения средств обеспечения информационной безопасности*

Стратегия определяет структуру, приоритеты и методы принятия решений при организации и обеспечении соответствующего вида деятельности. Разработка стратегии направлена на то, чтобы наиболее важные цели соответствующей деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Процесс выработки стратегии обеспечения информационной безопасности баз данных в самом общем виде может быть определен как поиск компромисса между уровнем обеспечения информационной безопасности и необходимыми для достижения этих целей ресурсами.

Необходимый уровень информационной безопасности определяется собственником информационного ресурса или уполномоченным им лицом и учитывает, прежде всего, важность информационного ресурса для обеспечения соответствующего вида деятельности. Диапазон вариантов чрезвычайно широк: от ситуации, когда разрушение информационного ресурса приводит к прекращению бизнеса (например, утрата состояния счетов клиентов банка), до ситуации, когда произошла досадная, но мелкая неприятность (случайно стерты копии руководств по информационной безопасности, переписанные вчера из сети Интернет).

Размер средств, выделяемых на обеспечение безопасности информационного ресурса, всегда ограничен. Из соображений здравого смысла, стоимость средств, выделенных на обеспечение информационной безопасности ресурса, не может превышать ценность самого ресурса. В реальности, стоимость средств, выделяемых на обеспечение информационной безопасности ресурса, не превышает 1 % его стоимости (обычно заметно меньше). Размер средств, выделяемых на проектирование или сопровождение системы защиты информации баз данных, может определяться соответствующими позициями бюджета организации, зачастую непосредственно не связанными с ценностью информационных ресурсов организации. В этом случае стратегия расходования выделенных средств состоит в получении максимального эффективной системы обеспечения информационной безопасности при ограничениях, заданных на доступные средства.

С формальной точки зрения, сформулированные задачи являются оптимизационными задачами. Точнее, речь идет о паре двойственных задач. Несмотря на ясность содержательной сути поставленной задачи, осуществить формальную постановку задачи защиты информации баз данных в форме задач линейного или нелинейного программирования обычно не удается. Существует несколько проблем, затрудняющих формальную постановку пары двойственных задач:

     определение ценности информационных ресурсов и оценка ущерба от конкретных действий или событий часто может быть выполнена только на качественном уровне;

     эффективность методов и средств обеспечения информационной безопасности зависит от большого числа случайных и трудно предсказуемых факторов, таких как поведение злоумышленника, воздействие природных явлений, случайные сбои и необнаруженные ошибки в системе обработки информации и т. п.;

     организационные меры по обеспечению информационной безопасности связанны с действиями людей, эффективность которых также трудно оценить количественно.

В реальной практике обычно используются качественные оценки или оценки в ранговых шкалах. Например, можно рассмотреть проектные решения, которые обеспечат требуемый уровень защиты:

     от наиболее опасных из известных угроз;

     от всех идентифицированных угроз;

     от всех потенциально возможных угроз.

ВО многих случаях системы обработки данных создаются не «с нуля», а развивают имеющиеся системы обеспечения бизнес-процессов организации с возможной автоматизацией некоторых процессов. При разработке средств обеспечения информационной безопасности баз данных проектные решения в значительной степени зависят от возможностей по изменению элементов существующих систем. Можно выделить несколько вариантов, в значительной степени определяющих существо возможных проектных решений:

     никакое вмешательство в информационную систему не допускается (требование предъявляется к функционирующим системам обработки информации, остановка или модификация которых недопустима);

     допускается частичное изменение архитектуры информационной системы (возможна временная остановка процессов функционирования и модификация используемых технологий для встраивания некоторых механизмов защиты);

     требования, обусловленные необходимостью обеспечения информационной безопасности, принимаются в полном объеме при проектировании и эксплуатации системы обработки информации. На основе представленных классификаций можно предложить три стратегии обеспечения информационной безопасности, представленные в таблице 1.

***Таблица 1.***

**Стратегии обеспечения информационной безопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| Учитываемые угрозы | Влияние на информационные системы | | |
| отсутствует | частичное | существенное |
| Наиболее опасные | Оборонительная стратегия |  |  |
| Все идентифицированные угрозы |  | Наступательная стратегия |  |
| Все потенциально возможные |  |  | Упреждающая стратегия |

Выбирая оборонительную стратегию, проектировщик должен четко понимать и грамотно объяснить руководству, что если исключить вмешательство в процесс функционирования информационной системы, то можно нейтрализовать лишь наиболее опасные угрозы. Обычно это достигается построением «защитной оболочки», включающей разработку дополнительных организационных мер, создание программных средств допуска к ресурсам информационной системы в целом, использованию технических средств контроля помещений, в которых расположено терминальное и серверное оборудование.

Наступательная стратегия предусматривает активное противодействие известным угрозам, влияющим на информационную безопасность системы. Наступательная стратегия может включать установку дополнительных программно-аппаратных средств аутентификации пользователей, внедрение более совершенных технологий разгрузки и восстановления данных, повышение доступности системы с использованием горячего и холодного резервирования.

Упреждающая стратегия предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы. Важной частью упреждающей стратегии является оперативный анализ информации центров изучения проблем информационной безопасности, изучение отечественного и мирового передового опыта, проведение независимого аудита уровня обеспечения безопасности информационных ресурсов организации.

***Контрольные вопросы:***

1.       Сформулируйте определение политики безопасности.

2.       Какова цель формализации политики безопасности?

3.       Объясните необходимость нескольких вариантов документального оформления политики безопасности для различных уровней управления.

4.       Сформулируйте примерный перечень разделов документа, описывающего политику безопасности.

5.       Выполнение каких условий необходимо обеспечить для эффективной реализации политики безопасности?

6.       Сформулируйте типовой перечень документов, представляющий основные решения организации по реализации политики безопасности.

7.       Приведите известные вам примеры применения принципа открытого проектирования для конкретных систем обработки данных. Имеются ли исключения, когда применение данного принципа является неоправданным?

8.       Приведите известные вам примеры применения принципа минимально возможных привилегий. Поясните, почему применение данного принципа иногда входит в противоречие с принципом психологической приемлемости?

9.       Приведите известные вам примеры ситуаций, когда отказ или сбой аппаратных средств или программного обеспечения приводил к раскрытию конфиденциальных данных.

10.  Каким образом и кем должна определяться ценность информационного ресурса?

11.  Попытайтесь для какого-нибудь простейшего случая сформулировать задачу проектирования системы защиты информации баз данных как пару двойственных задач (например, линейного программирования).

12.  Сформулируйте характерные черты и области использования оборонительной, наступательной и упреждающей стратегий обеспечения безопасности информационных ресурсов организации.