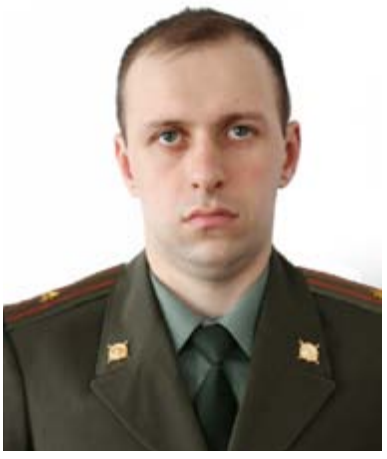
Основные вопросы по организации защиты информации в центре обработки данных



Екимов
Иван Алексеевич,
начальник группы технической защиты информации центра автоматизированной системы управления Санкт-Петербургского военного института внутренних войск МВД России, майор

Для правильной организации работы центра обработки данных[1] необходимо принять большое число решений, которые будут определять режим работы ЦОД. Многие из этих решений влияют на степень защиты информации. Поэтому их необходимо рассматривать в свете общих конечных целей функционирования ЦОД.

Организацию защиты информации в ЦОД необходимо рассматривать со следующих позиций:

- Внешнее окружение ЦОД;
- Способы контроля доступа;
- Применимость мер защиты;
- Надежность вычислительных средств и вспомогательных систем;
- Обучение пользователей.

1. Внешнее окружение ЦОД

Для ограничения числа лиц, которые получают доступ в помещение центра обработки данных, могут быть использованы: организационные меры и меры непосредственной защиты. Здесь можно выделить три основных режима организации работы ЦОД:

1. Закрытый режим. Только небольшое число операторов имеет прямой доступ в помещение ЦОД.
2. Открытый режим. Любой сотрудник может получить доступ в помещение ЦОД. Пользователь для выполнения вычислений должен сам появиться в помещении ЦОД, и в это время можно выполнить процедуры его идентификации.
3. Режим без ограничений. Доступ к средствам ЦОД осуществляется по линиям связи. При этом пользователь не должен появляться в помещении ЦОД.

2. Способы контроля доступа к информации

Защита информации в процессе функционирования системы связана в первую очередь с процессом установления полномочий. В процессе организации защиты информации необходимо ответить на следующие вопросы:

1. Кто? — Связан с необходимостью знать, *кто* хочет получить доступ к информации или изменить ее.
2. Какая? — Связан с тем, *какая* информация требуется в данном случае.
3. Что? — Связан с потребностью знать, *что* именно (какое действие) должно быть выполнено над этой информацией (например, чтение, модификация и т. п.).
4. Когда? — Обусловлен тем, *когда* (т. е. в какой отрезок времени) допускается выполнение данного действия.
5. Откуда? — Необходимость информирования, *откуда* (т. е. из какого источника) исходит требование на получение доступа к данным.
6. Зачем? — Действие принципа «пользователь должен знать только то, что ему необходимо».

Раскрывая эти вопросы, возможно рассмотреть их в такой интерпретации:

Идентификация и подтверждение подлинности (Кто?)

Для того чтобы проконтролировать, кто получает доступ, необходимо иметь возможность идентифицировать пользователя и подтверждать его подлинность. При реализации процесса подтверждения подлинности обычно используется нечто такое, что пользователь знает (например, пароль) или имеет при себе (например, жетон), или используются некоторые его физические характеристики (например, отпечатки пальцев).

Как только пользователь успешно прошел процедуру идентификации и подтверждения подлинности, его можно рассматривать как индивидуальное лицо, как исполнителя некоторой роли и как некоторую функциональную единицу.

Классификация информации (Какая?)

Проблема контроля того, какая информация может быть доступна, во многих отношениях аналогична проблеме, кто имеет доступ к информации. В частности, некоторый конкретный документ или некоторый объем информации может быть идентифицирован и на него могут быть установлены полномочия доступа либо как к конкретному документу, либо как к исполнителю некоторой роли, либо как к представителю некоторой функциональной категории.

Классификация информации может усложняться за счет действия многих факторов, например таких как детальность информации и уровень секретности.

1 Далее по тексту ЦОД

Операции над информацией (Что?)

В простейшем случае допустимы всего две операции — считывание и запись. Если некоторому лицу разрешено считывание определенной информации, то он не имеет права изменять ее. Если некоторому лицу разрешена операция записи, то он может изменять информацию. Возможны различные варианты этих двух основных операций.

3. Применимость мер защиты

Введение мер защиты может создать дополнительные трудности или неудобства для пользователей. Если эти меры слишком усложняют работу, то, вероятнее всего, эффективность их использования будет низкой. Для большинства пользователей обеспечение защиты не является основной функциональной обязанностью. Если применение мер защиты требует от пользователя затрат лишнего времени и он будет совершать некоторую лишнюю работу, которая не относится к его непосредственным обязанностям, то это косвенно побудит его найти обходные пути, которые поставят под угрозу работу механизма защиты.

Поэтому, когда разрабатывается способ установления полномочий и мер защиты, важно учесть условия работы с системой и должен быть выбран подход защиты информации, который обеспечивает простоту и удобство использования средств защиты. Такое решение может потребовать компромисса между степенью защиты системы и простотой работы с нею.

4. Надежность вычислительных средств и вспомогательных систем

По мере того как вычислительные системы увеличивают свои возможности и становятся все более выгодными по критерию стоимость-эффективность, они всё глубже проникают в различные сферы жизнедеятельности военного института и становятся неотъемлемыми частями механизма управления процессами жизнедеятельности. Также необходимо учитывать, что для обеспечения беспрерывной работы вычислительных систем на полную мощность должны работать некоторые вспомогательные системы (такие как постоянное и стабильное электропитание и кондиционирование). Это в свою очередь приводит к повышению требований к надежности систем, к их резервированию и способности восстанавливать работоспособность.

Высокая надежность систем позволяет минимизировать вероятность их выхода из строя с опасностью разрушения информации. Резервирование этих систем позволяет не допускать перерыва в предоставлении вычислительных сервисов. Кроме того, очень важно иметь эффективные процедуры восстановления, которые позволяют в возможно более короткий срок после выхода из строя вновь обеспечить нормальное функционирование вычислительных систем.

Процедуры, обеспечивающие надежность системы и защиты информации, способны к восстановлению и контролю целостности информации. Например, многие механизмы обеспечения надежности основаны на использовании дополнительных проверок и испытаний для обнаружения возможных ошибок или неисправностей в программном обеспечении или аппаратуре. Некоторые из этих испытаний или анализ их результатов могут быть непосредственно (или после незначительной модификации) использованы для проверки и обнаружения потенциальных нарушений системы защиты.

Многие же из этих механизмов основаны на введении избыточности и использовании дублирования.

Один простой способ решения этих проблем состоит в систематической проверке всех процедур, обеспечивающих защиту системы, ее надежность и способность к восстановлению.

5. Обучение пользователей

Обучение пользователей является важным предварительным условием эффективности внедрения различных процедур защиты. Знания пользователей и понимание ими проблем защиты будут углубляться за счет сообщений средств массовой информации, увеличения числа прямых контактов с вычислительной техникой, а также по мере того, как средства вычислительной техники станут все шире использоваться в процессе выполнения различных задач и будут совершенствоваться системы защиты (как в техническом плане, так и в плане повышения их качества по критерию стоимость-эффективность).

Двумя основными проблемами управления персоналом, которые особенно важны в условиях применения систем защиты, являются распределение ответственности и организация проверок и ревизий. Необходимо проведение нескольких этапов проверок и ревизий, чтобы воспрепятствовать попытке разрушить систему защиты. На любом из этих этапов попытка разрушения защиты может быть либо предотвращена, если это один из предварительных этапов, либо обнаружена. Распределение ответственности подразумевает, что разные лица несут ответственность за реализацию различных шагов. Таким образом, для нарушения системы защиты необходимо активное взаимодействие нескольких лиц. Это делает попытку разрушения системы защиты значительно более трудной и рискованной задачей и уменьшает угрозу безопасности вычислительных систем.

При рассмотрении вопросов внедрения систем защиты информации необходимо учитывать эти решения с позиций экономической выгоды вложения средств, что привычно и первично в сложившемся на настоящей момент материально-ориентированном ценностном подходе.

Основными проблемами, которые должны быть рассмотрены для определения экономических аспектов проблемы защиты, являются следующие:

а) определение ценности информации;
б) оценка вероятных угроз системе защиты информации;
в) оценка и эффективность возможных механизмов защиты.

Ниже рассмотрены некоторые аспекты этих проблем.

С позиции оценки ценности информация может быть:

1. Важная оперативная информация;
2. Персональная информация (например, данные об отдельных лицах или медицинская информация, которая хранится в файлах данных о сотрудниках) имеет значительно большую ценность для источника (т. е. для лица, к которому относится информация), чем для держателя информации);

3. Информация, используемая при выработке стратегических решений.

С позиции угроз действия злоумышленников можно отнести к следующим четырем группам:

1. Прерывание — прекращение нормального доступа к информации;
2. Кража или раскрытие — чтение или копирование информации с целью получения данных;
3. Видоизменение — искажение информации с целью дезинформации;
4. Разрушение — уничтожение информации.

Таким образом, в процессе определения ценности информации необходимо учитывать свойства самой информации, возможные угрозы и заинтересованную сторону. В частных случаях, например, могут быть использованы оценки типа «затраты держателя на защиту информации X против раскрытия» и «затраты злоумышленника на изменение информации У».

Оценка угроз проводится для того, чтобы определить затраты на выполнение определенных действий с информацией. Для разработки рационального плана защиты необходимо оценить и вероятность осуществления каждой угрозы.

Общей целью большинства предложенных стратегий оценки риска является получение его количественной оценки. В качестве наиболее приемлемого метода для этого можно предложить вычисление ожидаемой величины потерь для каждой угрозы в виде произведения Yp, где Y — денежная оценка угрозы, а p — вероятность ее осуществления. Следовательно, если оценка угрозы составляет 1 млн. руб., а вероятность ее осуществления равна 0,05, то оценка риска составляет 50 тыс. руб.

К проблемам оценки рисков относятся:

1. определение точной денежной оценки угрозы;
2. большинство людей обычно неохотно приписывают денежную оценку угрозам, которые могут оказать социальное воздействие.

Существуют также большие трудности и при определении вероятности осуществления угрозы. Определенные явления природы, например землетрясения и наводнения, пришлось изучать в течение достаточно длительных периодов времени, чтобы получить некоторые разумные вероятности их появления. Угрозы вычислительным системам слишком разнообразны, а их изучение началось не так давно, чтобы можно было собрать по этому вопросу достоверный статистический материал.

В заключение хотелось бы отметить, что для каждого типа угроз обычно можно назвать одну или большее число мер противодействия. Вследствие новизны этой области и разнообразия угроз в настоящее время невозможно полностью перечислить все возможные угрозы и соответствующие им меры противодействия.

Целью применения мер противодействия является уменьшение риска либо за счет уменьшения вероятности осуществления угрозы, либо за счет уменьшения эффекта воздействия угрозы. Так, например, вероятность потери информации может быть уменьшена благодаря введению дополнительных процедур для наблюдения за условиями хранения информации. Влияние потери информации на работу военного института может быть уменьшено либо за счет подготовки копий, дублирующих эту информацию, либо за счет подготовки заранее разработанных процедур, которые позволяют быстро и с небольшими затратами восстановить информацию.

Существуют две основные характеристики мер противодействия — эффективность и стоимость. Они служат базой для составления рационального с экономической точки зрения плана защиты. Мера противодействия считается разумной с экономической точки зрения, если ее эффективность, выраженная через уменьшение ожидаемого экономического ущерба, превышает затраты на ее реализацию.

Важной целью мер противодействия является увеличение цены нарушения системы защиты до значения, которое превышает оценки злоумышленником достигаемого им выигрыша. Таким путем достигается уменьшение риска.

Составной частью любого плана мероприятий по защите информации должно быть четкое указание целей, распределение ответственности и перечень организационных мер защиты.

Методы и процедуры подтверждения правильности и состоятельности данных важны и для уменьшения частоты непреднамеренных ошибок, и в качестве средства обнаружения или предотвращения различных форм преднамеренных нарушений доступа, как сотрудниками военного института, так и внешними злоумышленниками. С целью предотвращения данного вида событий целесообразно применять сложные проверки состоятельности данных.