И.В. Калиберда

Алгоритм автоматизированного определения требований для защиты информации, не составляющей государственную тайну, содержащейся в государственных и негосударственных информационных системах

Сегодня в процессе информатизации общества широко стали использоваться современные средства и методы обработки информации, что создаёт объективные предпосылки для автоматизации процессов защиты информации. Развитие вычислительной техники, увеличение производительности вычислительных машин позволяет решать всё более сложные и объёмные задачи. Если раньше, в виду сложности вычислений, такие задачи даже не пытались решать, тона современном этапе развития с успехом выполняют. Уже ни для кого не секрет, чтобы соответствовать современному уровню безопасности, необходимо использовать автоматизированные системы определения требований для защиты информации. Это позволит сократить время подбора методов и средств защиты, повысить качество принимаемых решений.

Таким образом, создание алгоритма автоматизированного определения требований для защиты информации поможет не только сохранить информацию, но и сэкономить деньги и время.

Основным документом для определения базового набора требований к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки, является Приказ ФСТЭК от 11 февраля 2013 № 17 [1] (далее Приказ). Алгоритм выбора мер защиты, с учётом требований вышеуказанного документа будет состоять из следующих программно-методических модулей:

1. Ввод исходных данных.
2. Определение перечня актуальных угроз и их типа.
3. Выбор класса информационной системы (далее ИС).
4. Определение базового набора мер.
5. Адаптация набора мер.
6. Уточнение перечня мер.
7. Дополнение требований.

Приказ [1] позволяет гибко подходить к выбору мер защиты, что отражено на схеме определения организационно-технических мер по защите информации, см. рисунок 1.

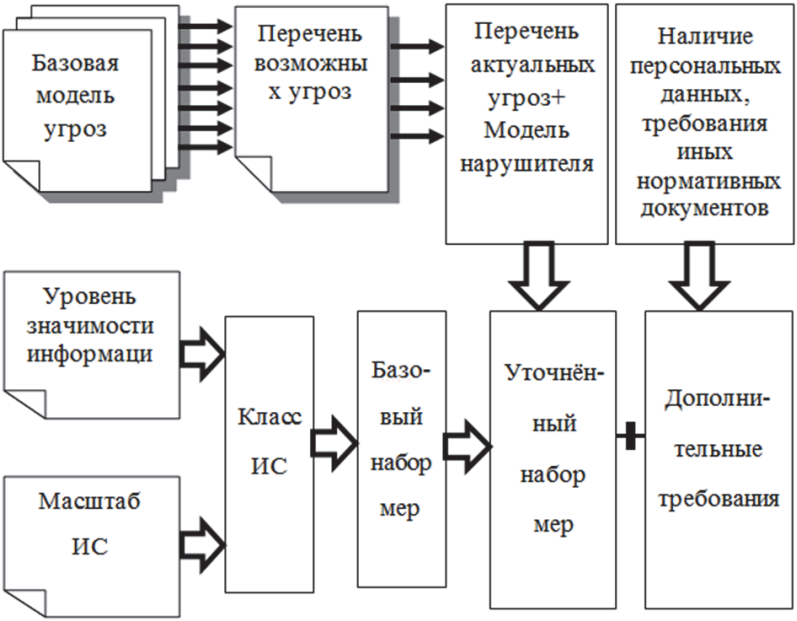

Рисунок 1. Схема определения организационно-технических мер по защите информации.

Содержание программно-методических модулей алгоритма выбора мер защиты:

- ввод исходных данных. На данном этапе собираются такие сведения ИС, как:
  - масштаб ИС;
  - уровень значимости информации;
  - перечень возможных угроз;
  - модель нарушителя;
  - требования иных нормативных документов;
  - наличие персональных данных в ИС (если есть, то указать уровень защищённости).
- определение перечня актуальных угроз и их типа. Угрозы безопасности информации определяются по результатам исследований:
  - оценка возможностей нарушителей. В данном случае учитываются потенциал, оснащенность и мотивация нарушителей;
  - анализ возможных уязвимостей ИС;
  - анализ возможных способов реализации угроз безопасности информации;

– анализ возможных последствий от нарушения свойств безопасности информации. Рассматриваются нарушения основных свойств информации: конфиденциальности, целостности, доступности.

При определении угроз безопасности информации учитываются следующие характеристики ИС:

– структура ИС;
– состав ИС;
– физические, логические, функциональные и технологические взаимосвязи между частями ИС, взаимосвязи с другими информационными системами;
– режимы обработки информации как в самой ИС, так и в её отдельных сегментах;
– применяемые информационные технологии;
– особенности функционирования ИС;
– иные характеристики ИС;

• выбор класса ИС. Классификация информационной системы производится в зависимости от двух показателей:

– значимость информации, обрабатываемой в ИС;
– масштаб ИС.

Уровень значимости информации определяется в зависимости от степени возможного ущерба от нарушения свойств информации:

– конфиденциальности (учитываются неправомерный доступ, неправомерное копирование, неправомерное предоставление или распространение информации);
– целостности (учитываются неправомерное уничтожение информации, неправомерное модифицирование информации);
– доступности (учитывается неправомерное блокирование информации).

В Приказе [1] содержится четыре класса защищенности ИС, которые определяют уровни защищенности (УЗ) содержащейся в ней информации. Самый высокий класс – первый, самый низкий – четвёртый:

– УЗ 1;
– УЗ 2;
– УЗ 3;
– УЗ 4.

Класс защищенности ИС определяется по приложению № 1, таблица 4 [1]. Если ИС состоит из отдельных сегментов, то класс защищённости определяется для каждой составной части.

Для определения масштаба ИС Приказом установлены три критерия:

- федеральный;
- региональный;
- объектовый.

• определение базового набора мер. Требования к системе защиты информации ИС определяются по приложению 2 [1] в зависимости от класса защищенности ИС. Также учитываются требования к защите информации, содержащейся в ИС, с учетом ГОСТ Р 51583 [2] и ГОСТ Р 51624 [3].

Согласно Приложению 2 [1], организационные и технические меры защиты информации, реализуемые в ИС, должны обеспечивать:

- идентификацию и аутентификацию субъектов и объектов доступа;
- управление доступом;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение вторжений;
- контроль защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту ИС, ее средств, систем связи и передачи данных.

• адаптация набора мер. В зависимости от информационной технологии могут применяться компенсирующие меры, обоснованные при оценке достаточности и адекватности мер. После определения угроз безопасности информации дополнительно могут разрабатываться рекомендации, направленные на нейтрализацию отдельных угроз безопасности информации.

• уточнение перечня мер. Предусматриваются меры по противодействию нарушителям. Выбранные и реализованные в информационной системе защиты информации меры должны обеспечивать нейтрализацию угроз безопасности информации:

- для ИС 1 класса защищенности, связанных с действиями нарушителя с высоким потенциалом;
- для ИС 2 класса защищенность, связанных с действиями нарушителя с потенциалом не ниже среднего;
- для ИС 3 и 4 классов защищенности, связанных с действиями нарушителя с низким потенциалом.

• дополнение требований. Если в ИС установлены иные нормативные правовые акты в области защиты информации, в том числе в области защиты персональных данных, то устанавливается дополнительный набор мер защиты информации.

Реализация подобного алгоритма выбора мер защиты, способного моделировать и оптимизировать инженерно-техническую защиту информационной системы, позволит:

- повысить качество проектных решений;
- оптимизировать выбор средств защиты информации;
- уменьшить время на проектирование системы защиты.

Описанный алгоритм может применяться при проектировании систем защиты информации в ИС в государственных учреждениях и коммерческих организациях.

Библиографический список

1. Приказ от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» – ФСТЭК, г. Москва.
2. ГОСТ Р 51583 «Защита информации. Порядок создания АС в защищенном исполнении. Общие положения».
3. ГОСТ Р 51624 «Защита информации. АС в защищенном исполнении. Общие требования».
4. Gizun A., Volyanska V.V., Ryndyuk V.O., Gnatyuk S.O.Main parameters for information security intruder identification // Захист інформації. 2013. Т. 1. № 58. С. 66-74.