СОЗДАНИЕ И АТТЕСТАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

О.К. Барановский

Государственное предприятие «НИИ ТЗИ», испытательная лаборатория
ул. Первомайская, 26/2, г. Минск, Республика Беларусь
телефон(ы): + (37517) 2940171; факс(ы): + (37517) 2853186; e-mail: obar@niitzi.by
web: www.niitzi.by

Рассматриваются вопросы безопасности информации в информационных системах. Приводятся особенности установления требований безопасности при создании системы защиты информации. Обрисовываются цели и мероприятия при аттестации систем защиты информации. Обсуждается проблема выбора методического подхода к оценке эффективности системы защиты информации.

Ключевые слова – информационная система, система защиты информации, аттестация, безопасность информации

ВВЕДЕНИЕ

Автоматизация процессов поиска, получения, передачи, обработки, накопления, хранения, распространения и (или) предоставления, пользования информацией осуществляется путем создания информационных систем (ИС). Устойчивое выполнение ИС своей миссии обеспечивается поддержанием состояния защищенности информации и обслуживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, несущих угрозу нанесения ущерба владельцам или пользователям информации. Для этой цели создается система защиты информации (СЗИ) через реализацию мер, направленных на обеспечение целостности, конфиденциальности, доступности и сохранности информации (безопасности информации).

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

До создания эффективной (критерий – минимизация затрат с учетом актуальных рисков) СЗИ необходимо классифицировать по степени важности хранящиеся и обрабатываемые в ИС сведения, а также присвоить ИС класс типового объекта информатизации (ОИ). Классификация сведений по степени важности проводится по принципу идентичности по степени конфиденциальности, гарантируемому уровню целостности, доступности и сохранности. Присвоение класса типового ОИ проводится с учетом степени важности сведений, эквивалентности ИС по организации вычислительного процесса, степени безопасности предоставляемых ИС автоматизированных процессов.

Стандарт СТБ 34.101.30 позволяет классифицировать ОИ по степени конфиденциальности обрабатываемой информации и эквивалентности организации вычислительного процесса [1].

В целях получения актуализированных наборов требований безопасности необходимо также классифицировать ОИ по целостности, доступности и сохранности информации, а также по конфиденциальности, целостности и доступности предоставляемых ИС автоматизированных процессов.

Для каждого класса типовых ОИ должна быть разработана базовая модель угроз безопасности ОИ на основе полного перечня факторов, воздействующих на безопасность информации [2].

Для каждого класса типового ОИ необходимо разработать профиль защиты. Задание по безопасности (ЗБ) на конкретную ИС разрабатывается на основе профиля защиты или, при его отсутствии, модели угроз безопасности.

После оценки ЗБ требования безопасности должны быть реализованы в ИС. При построении СЗИ необходимо использовать технические средства защиты информации, имеющие положительное экспертное заключение, разрешающее их применять в СЗИ ИС, отнесенных к заданному набору классов типовых ОИ.

АТТЕСТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аттестация СЗИ заключается в оценке ее соответствия требованиям безопасности информации и включает: оценку корректности реализации требований ЗБ в ИС, оценку разработанной документации, проверку уровня подготовки персонала, испытания средств защиты информации (средств безопасности) и комплекса средств безопасности (КСБ) в целом в реальных условиях эксплуатации на различных этапах технологического процесса обработки защищаемой информации.

Можно выделить две цели оценки СЗИ:

1) требование соответствия нормативным правовым актам, в том числе техническим нормативным правовым актам в области защиты информации;

2) построение эффективной СЗИ, отвечающей современным угрозам и базирующейся на методике управления рисками.

В этой связи при оценке СЗИ проводят два типа испытаний:

1) проверка настройки и выполнения своих функций как отдельными средствами, так и КСБ в целом по утвержденным или согласованным установленным порядком методикам испытаний ИС;

2) испытания КСБ методом «взлома» в обход или вопреки применяемым мерам и средствам защиты по специально разработанным методикам.

При проведении испытаний необходимо оценивать эффективность выполнения функций безопасности.

Показателем эффективности является параметр или характеристика, характеризующие степень выполнения СЗИ одной или системы заданных функций. Показатель эффективности должен удовлетворять следующим требованиям [3]:

1) иметь определенный физический смысл и возможность количественной оценки;

2) эксперт должен иметь ясное представление об алгоритме оценки;

3) инструментальные средства оценки должны обеспечивать необходимую чувствительность к изменению условий испытаний.

На сегодня применяют следующие методические подходы к оценке эффективности СЗИ [3]:

1) детерминистический подход;

2) логико-вероятностные методы;

3) вероятностно-временной анализ.

Детерминистический подход заключается в задании и последующей проверке полноты выполнения обязательных формализованных требований. Результаты могут интерпретироваться на качественном уровне, либо на основании полученных данных могут конструироваться интегральные критерии, позволяющие получать количественные оценки. Однако метод не содержит критериев оценки правильности установки и настройки технических средств защиты информации, выполнения организационных мер защиты и др. Метод является экспертным (субъективным), поэтому отвечающая всем требованиям СЗИ в реальных условиях может оказаться неспособной решать поставленные перед ней задачи.

Логико-вероятностные методы позволяют определить степень риска, присутствующего в СЗИ. Составляется сценарий развития угрозы безопасности информации или ИС, представляющий собой логико-вероятностную модель функционирования СЗИ. Метод дает обоснованный количественный показатель эффективности СЗИ. Недостатком метода является достоверность вероятностей угроз и значительный объем трудоемких логико-вероятностных преобразований при анализе сложных сценариев.

Эффективность защиты в рамках вероятностно-временного анализа рассматривается как вероятность того, что СЗИ обнаружит и успеет пресечь угрозу нарушения безопасности. Объективность и достоверность результатов оценки сильно зависят от точности исходных данных по вероятностям обнаружения угроз нарушения безопасности, по времени действия угроз, преодоления или обхода СЗИ, предотвращения или устранения (снижения до приемлемого уровня) последствий реализации угроз. Метод характеризуется значительным объемом рутинных вычислительных процедур при анализе СЗИ на реальных объектах.

Ввиду множественности описания СЗИ как сложной технической системы не существует универсального определения «эффективности». Рассмотренные методы позволяют оценивать СЗИ в различных, дополняющих друг друга, плоскостях.

Анализ зарубежного опыта показывает, что разработка универсального метода оценки эффективности СЗИ является чрезвычайно сложной задачей. При этом степень сложности подходов к оценке эффективности должна постоянно наращиваться от простых к более сложным с их обязательной апробацией на практике.

ЗАКЛЮЧЕНИЕ

Эффективность создаваемой СЗИ определяется учетом требований безопасности информации на стадии проектирования ИС. Для ИС, реализующих информационные отношения в государстве и обществе, подходы к созданию и аттестации СЗИ должны обеспечивать объективную, достоверную и повторяемую оценку соответствия СЗИ установленным для нее требованиям в соответствии с процедурами, критериями и методологией, установленными в нормативных документах. Устойчивое выполнение ИС своей миссии обеспечивается перманентной актуализацией модели угроз и модернизацией СЗИ с учетом рисков.

ЛИТЕРАТУРА

[1] Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация: СТБ 34.101.30–2007. – Введ. 01.04.2008. – Минск: Госстандарт, 2007. – 7с.

[2] Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275–2006. – Введ. 01.02.2008. – Москва: Стандартинформ, 2007. – 11 с.

[3] Панин, О. Проблемы оценки эффективности функционирования систем физической защиты объектов / О. Панин // БДИ. – 2007. – № 3. – С. 23–27.