КРАТКИЕ СООБЩЕНИЯ

УДК 621.391.25

ПРОФИЛИ БЕЗОПАСНОСТИ ОБЪЕКТОВ РАЗЛИЧНЫХ ФОРМ СОБСТВЕННОСТИ

В.В. МАЛИКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь.

Поступила в редакцию 3 ноября 2008

Предложен новый принцип формирования профилей безопасности объектов. Приводится классификация профилей по категориям безопасности.

Ключевые слова: безопасность объектов, профиль безопасности объекта, категории безопасности.

В настоящее время разработка комплексных систем безопасности для объектов различных категорий является актуальной проблемой. Важным этапом в данном процессе является оценка эффективности разработанной системы безопасности существующим угрозам, что реализуется в процессе анализа рисков. Ошибки в анализе рисков [1] приводят к не адекватному определению:

– перечня сил и средств защиты, необходимых для обеспечения гарантированной безопасности объекта;

– соотношению задействованных сил и средств защиты реальным угрозам безопасности, расстановки приоритетов в реализации алгоритмов противодействия;

– возможного экономического ущерба.

Целью настоящей работы являлась разработка профилей безопасности объектов и их классификация по категориям безопасности, для применения при проектировании систем комплексной безопасности объектов различных форм собственности.

Под безопасностью объекта будем понимать свойство, выражающееся в способности противодействовать нанесению ущерба при различных (преднамеренных и стихийных) воздействиях на него, а также ликвидации последствий таких воздействий [2].

Профиль безопасности объекта - совокупность требований для объекта определенной категории, реализация которых гарантирует противодействие соответствующим им угрозам.

Для формирования профилей безопасности объектов необходимо провести классификацию последних по категориям безопасности, для чего целесообразно использовать положения стандарта США "Критерии оценки гарантированно защищенных вычислительных систем" (Trasted Computer Systems Evaluation Criteria — TCSEC) [3].

В соответствии с требованиями TCSEC автоматизированные системы защищаемого объекта, разделены на группы:

1. D — минимальная защита;
2. C — индивидуальная защита;
3. B — мандатная защита;
4. A — верифицированная защита.

Группы систем делятся на классы, причем все системы, относимые к группе D, образуют один класс D, к группе C — два класса C1 и C2, к группе B - три класса B1, B2 и B3, к группе A — один класс A1 с выделением части систем вне класса.

Следует отметить, что стандарт TCSEC описывает только безопасность систем, которая регулируется механизмами разграничения доступа к информации (чтение, запись, создание или удаление информации).

Согласно требованиям международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (Evaluation criteria for IT security) [4–6] определены семь упорядоченных по возрастанию оценочных уровней доверия безопасности, содержащих рассчитанные на многократное применение комбинации требований доверия (не более одного компонента из каждого семейства) [6]. Наличие такой шкалы дает возможность сбалансировать получаемый уровень доверия со сложностью, сроками, стоимостью и самой возможностью его достижения.

Для проведения классификации объектов по категориям физической безопасности возможно использование положений РД 28/3.006-2005 МВД Республики Беларусь [7]. В соответствие с которым, в зависимости от значимости и концентрации материальных, художественных, исторических, культурных ценностей, размещенных на охраняемом объекте, последствий от возможных преступных посягательств на них, все объекты, их помещения и территории подразделяются на две группы (категории): А и Б. Ввиду большого разнообразия разнородных объектов в каждой группе, они дополнительно подразделяются на две подгруппы каждая: А I и А II, Б I и Б II.

Объекты подгрупп А I и А II — это особо важные объекты жизнеобеспечения повышенной опасности, противоправные действия (кража, грабеж, разбой, терроризм и другие), на которых могут привести к крупному, особокрупному экономическому или социальному ущербу государству, обществу, предприятию, экологии или иному владельцу имущества.

Объекты подгрупп Б I и Б II – это объекты, хищения на которых в соответствии с уголовным законодательством Республики Беларусь могут привести к ущербу в размере до 250 базовых величин и свыше 250 соответственно.

В зависимости от технической укрепленности объектов, находящихся в них ценностей, расположения в здании, удаленности от постов охраны, они могут блокироваться системами охранной сигнализации со следующими уровнями защиты [7]:

1. Низкий уровень защиты.
2. Средний уровень защиты.
3. Повышенный уровень защиты.
4. Высокий уровень защиты.

На основании вышеизложенного, для осуществления комплексной классификации объектов по признакам физической и информационной безопасности с учетом особенностей доступа, введем следующие категории безопасности.

1. Организационная структура управления объектом – в качестве базовой предлагается система уровневой классификации объектов по признаку государственных приоритетов системы национальной безопасности:

– республиканский уровень административного управления (Совет министров, Совет национальной безопасности и т.д.);

– региональный уровень административного управления (областные органы управления и власти);

– местный уровень административного управления (городские/районные органы управления и власти).

2. Функционально-экономического построения процесса организации деятельности объекта — в качестве базовой предлагается система уровневой классификации объектов по признаку функционально-экономической организации деятельности и регулирования со стороны государства:

– частная собственность с участием только иностранного капитала (деятельность не регулируется государством);

– частная собственность с участием смешанного (государственного/иностранного) капитала (деятельность частично регулируется государством);

– государственная собственность (деятельность регулируется государством).

3. Оценка риска.

Суммарная критичность ресурсов объекта определяется системой критериев:

– ущерб репутации организации;
– безопасность персонала;
– разглашение коммерческих сведений;
– финансовые потери и др.

Проведение расчета по оценке риска [3] может быть выполнено по формуле (1):

$$R = HP, \quad (1)$$

где R — оценка риска в денежном эквиваленте, руб.; H — оценка ущерба в результате инцидента в денежном эквиваленте, руб.; P — вероятность инцидента.

Возможно использование альтернативного эмпирического метода, разработанного специалистами фирмы IBM [3]. Зависимость ожидаемых потерь от i-й угрозы информации рассчитывается по формулам (2).

$$R_i = 10^{S_i = V_i - 4}, \quad (2)$$

где S_i — коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы; V_i — коэффициент, характеризующий значение возможного ущерба при его возникновении.

Суммарная величина потерь R определяется формулой:

$$R = \sum_{\forall i} R_i . \quad (3)$$

Под общей оценкой риска (risk assessment) будем понимать процесс, в который входят: идентификация, анализ и оценка риска [8, 9].

В качестве критериев значимости возможного уровня экономического ущерба можно использовать следующую классификацию [10, 11]:

1. особокрупный — ущерб на сумму более 1000 базовых величин.
2. крупный — от 250 до 1000 базовых величин.
3. значительный — от 40 до 250 базовых величин.
4. средний — от 10 до 40 базовых величин.
5. мелкий — менее 10 базовых величин.

С учетом вышеизложенного, предлагается введение новой классификации объектов, учитывая особенности доступа к ним.

1. Упрощенный доступ:

– контроль доступа к ресурсам объекта осуществляется региональными и местными органами административного управления;

– объекты, несанкционированный доступ к ресурсам которых может привести к мелкому (до 10 базовых величин) или среднему (от 10 до 40 базовых величин) экономическому ущербу.

2. Ограниченный доступ.

– контроль доступа к ресурсам объекта осуществляется региональными и местными органами административного управления;

– объекты, несанкционированный доступ к ресурсам которых может привести к значительному (от 40 до 250 базовых величин) экономическому ущербу.

3. Важный доступ.

– контроль доступа к ресурсам объекта осуществляется республиканскими и региональными органами административного управления;

– особо важные объекты жизнеобеспечения [7], включенные в Перечень объектов, подлежащих обязательной охране Департаментом охраны МВД Республики Беларусь, определенный в соответствии с требованиями [12] несанкционированный доступ к ресурсам [13] которых может привести к крупному (от 250 до 1000 базовых величин) экономическому ущербу.

4. Доступ с расширенной защитой:

– контроль доступа к ресурсам объекта осуществляется республиканскими органами административного управления;

– деятельность объекта напрямую регулируется государством не в полном объеме или деятельность объекта напрямую не регулируется государством;

– особо важные объекты жизнеобеспечения [7], включенные в Перечень объектов, подлежащих обязательной охране Департаментом охраны МВД Республики Беларусь, определенный в соответствии с требованиями [12] несанкционированный доступ к ресурсам [13] которых может привести к особокрупному (более 1000 базовых величин) экономическому ущербу.

5. Доступ с максимальной защитой:

– контроль доступа к ресурсам объекта осуществляется республиканскими органами административного управления;

– деятельность объекта регулируется государством;

– особо важные объекты жизнеобеспечения [7], включенные в Перечень объектов, подлежащих обязательной охране Департаментом охраны МВД Республики Беларусь [12], противоправные действия на которых могут привести к особокрупному (более 1000 базовых величин) экономическому ущербу.

Вводимая классификация объектов согласована с требованиями международного стандарта ISO/IEC 15408:1999 [4–6]:

1. функциональные требования, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;

2. требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

Процесс обеспечения безопасности в ISO/IEC 15408:1999 рассматривается не статично, а в соответствии с жизненным циклом объекта оценки, который предстает в контексте среды безопасности, характеризующейся определенными условиями и угрозами [4–6].

Согласно требованиям ISO/IEC 15408:1999 происходит формирование двух базовых видов нормативных документов:

1. Профиль защиты — представляет собой типовой набор требований, которым должны удовлетворять аппаратно-программные средства и/или системы определенного класса.

2. Задание по безопасности — содержит совокупность требований к конкретной разработке, их выполнение позволит решить поставленные задачи по обеспечению безопасности.

С учетом вышеизложенного предлагается введение новой структуры профиля безопасности объекта в следующем составе.

1. Политика безопасности объекта — совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

2. Уровень безопасности объекта — совокупность нормативно-правовых, программно-технических и физических средств / систем защиты объекта, обеспечивающих противодействие угрозам несанкционированного доступа.

3. Аудит безопасности объекта — независимая оценка состояния системы безопасности объекта, устанавливающая уровень ее соответствия определенным критериям и предоставление результатов в виде рекомендаций.

Политику безопасности объекта предлагается формировать в соответствии со следующими этапами:

1. Проведение формализованного описания защищаемого объекта с оценкой текущего уровня безопасности на основе имеющейся информации о структуре / ресурсах объекта, а также установленных средствах защиты.

2. Составление перечня угроз и сценариев атак по этапам жизненного цикла системы.

3. Формирование и корректировка политики безопасности с учетом типовых рекомендаций нормативно-правовых документов (ISO/IEC 15408:1999, BS 7799:1995 и др. [4–6, 8, 9]) и перечнем угроз и сценариев атак по этапам жизненного цикла системы.

Результатом формирования политики безопасности объекта будет являться итоговый нормативный документ, который описывает и структуризирует основные направления в области защиты организации (предприятия), определяет методику реагирования на инциденты безопасности.

Основной задачей практической реализации заданного уровня безопасности объекта будет являться выполнение установленного нормативными документами минимального набора

требований к защите объекта, обеспечиваемого введенными средствами и системами защиты с учетом:

1. статистических данных по вопросам информационной и физической безопасности, имущественных преступлений;

2. классификации угроз и сценариев атак по этапам жизненного цикла системы. Основные элементы классификации: нормативно-правовые, программно-технические, физические угрозы;

3. специализированных сигнатурных баз, построенных по алгоритму масштабирования и позволяющих определить базовый перечень средств безопасности для защищаемого объекта. Исходная полнота сигнатурной базы должна соответствовать современному уровню угроз и сценарию атак;

4. модульной конструкторско-технологической структуры построения системы безопасности объектов в зависимости от заданного/анализируемого уровня угроз. При функционировании системы должен осуществляется контроль всех функциональных модулей объекта.

Результатом проведения аудита безопасности объекта будет являться экспертная оценка надежности обеспечения защиты объекта с учетом профиля безопасности, носящая разовый / постоянный характер проведения и выполняемая:

– штатными специалистами организации (предприятия);

– специалистами сторонних организаций.

Предложенная методика классификации объектов позволяет учесть особенности доступа на объект, его организационную структуру управления, функционально-экономическую организацию процесса обеспечения функционирования объекта, и выполнить оценку риска. Введенные категории безопасности позволяют провести детализированную оценку значимости ресурсов объекта. Предложенная структура профиля безопасности объекта включает нормативные требования и правила по обеспечению безопасности объекта, комплекс средств и систем защиты, методику проведения итоговой экспертной оценки, что позволяет упростить процесс проектирования и обеспечить гарантированную защиту объектов различных форм собственности.

OBJECTS SECURITY PROFILES OF VARIOUS FORMS OF PROPERTY

V.V. MALIKOV

Abstract

The new principle of the security profiles formation for proteted objects is offered. Classification of profiles by security categories is resulted.

Литература

1. Recommended Security Controls for Federal Information Systems. NIST Special Publication SP 800-53, Second Public Draft. — U.S. Department of Commerce, NIST, September, 2004.

2. *Маликов В.В.* // Материалы 12-й Междунар. НТК Современные средства связи. Минск, 24–28 сентября 2007 г. Минск, ВГКС, 2007. С. 107–108.

3. *Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.* Основы информационной безопасности. М., 2006.

4. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO/IEC 15408-1: 1999.

5. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. – ISO/IEC 15408-2: 1999.

6. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. – ISO/IEC 15408-3: 1999.

7. РД 28/3.006-2005 МВД Республики Беларусь. Технические средства и системы охраны. Тактика применения технических средств охранной сигнализации.

8. British Standard. Code of practice for information security management British Standards Institution, BS 7799:1995.

9. British Standard. Information security management systems Specification with guidance for use British Standards Institution, BS 7799-2: 2002.
10. Кодекс Республики Беларусь об административных правонарушениях от 21 апреля 2003 г. № 194-З [Электрон. ресурс]. Режим доступа: http://www.pravo.by/webnpa/ text.asp?start =1&RN= Hk0300194.
11. Уголовный кодекс Республики Беларусь от 09 июля 1999 г. № 275-З [Электрон. ресурс]. Режим доступа: http://www.pravo.by/webnpa/text.asp?start=1&RN=HK9900275.
12. *Зегжда Д. П., Ивашко А.П.* Основы безопасности информационных систем. М., 2000. 425 с.
13. Указ Президента Республики Беларусь от 25 октября 2007 года № 534 "О мерах по совершенствованию охранной деятельности".