СТРУКТУРА ПРЕДСТАВЛЕНИЯ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПРИ ФОРМИРОВАНИИ ПРОФИЛЕЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сидак А.А.

Центральный научно-исследовательский институт МО РФ
141080, г. Юбилейный, Московская область, ул. Тихонравова, 34

В настоящее время перспективным направлением является формирование требований безопасности информационных технологий в виде профилей защиты, структура которых регламентирована в международном стандарте ISO/IEC 15408-99 «Критерии оценки безопасности информационных технологий» (исторически сложившееся название – Общие критерии) /1/.

Профиль защиты (ПЗ) определяет независимо выполняемый набор требований безопасности информационной технологии (ИТ) для определенной категории объектов оценки. Такие объекты предназначены для удовлетворения потребностей многих пользователей безопасной ИТ. Пользователи могут сами формировать ПЗ или использовать имеющиеся ПЗ, чтобы сформулировать требования безопасности ИТ для конкретного объекта оценки.

Для эффективного решения проблемы обеспечения информационной безопасности при разработке ПЗ изделий ИТ необходимо выявление всех угроз активам данных изделий ИТ.

Под угрозой ИТ (фактором, воздействующим на информацию) понимается явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней /2/.

Выявление и анализ угроз безопасности играют важную роль при формировании целей и требований безопасности.

Результатом выявления угрозы безопасности является *модель угрозы*.

Модель угрозы – это формальное, полуформальное или неформальное описание жизненного цикла угрозы; направленности угрозы; источника угрозы; системы ИТ, подверженной угрозе; ИТ- и не-ИТ-среды системы ИТ; активов, требующих защиты; методов, способов и алгоритмов реализации угрозы; нежелательных событий; анализа рисков и ряда других аспектов.

В результате анализа требований Общих критериев по представлению угроз была разработана следующая структура представления моделей угроз активам систем ИТ.

▼

1. Маркировка

Ключевой символ T (от английского “Threat” - угроза)

1.1. Код угрозы T.XXX_YYY.ZZ,

где XXX – код класса угроз (определяется видом ОО);

YYY – код семейства угроз (определяется классификационным признаком угрозы);

ZZ – номер угрозы в семействе.

1.2. Наименование угрозы *

где * - произвольное количество символов (переменная μ_{14}).

2. Источник угрозы

2.1. Тип источника #

где # - цифра (цифровая символьная переменная α_{21}), определяющая тип источника по его связи с действиями человека:

1 – связан со злонамеренными действиями человека;

2 – связан с другими действиями человека;

3 – не связан с действиями человека.

2.2. Тип источника по его заинтересованности в компрометации активов * (рассматривается, если тип источника - 1)

где * - произвольное количество символов (переменная μ_{22}), определяющая источник угрозы по любым причинам.

2.3. Тип источника по уполномоченному доступу к ИТ-системе, в которой хранятся, обрабатываются и передаются активы * (рассматривается, если тип источника - 1)

где * - произвольное количество символов (переменная μ_4), определяющая источник угрозы по занимаемой должности или по его положению.

2.4. Тип источника по уровню практических навыков реализации угрозы

<#, *> (рассматривается, если тип источника - 1),

где # - цифра (цифровая символьная переменная α_{24}), определяющая уровень практических навыков реализации угрозы:

1 – низкий;

2 – средний;

3 – высокий;

4 – неопределенный;

* - произвольное количество символов (переменная μ_{24}), используемых для неформального описания практических навыков реализации угрозы.

2.5. Тип источника по наличию шансов (благоприятных возможностей) реализации угрозы <#, *> (рассматривается, если тип источника - 1)
где # - цифра (цифровая символьная переменная α_{25}), определяющая наличие шансов реализации угрозы:
1 – маловероятно;
2 – вероятно;
3 – большая вероятность;
4 – не определено;
* - произвольное количество символов (переменная μ_{25}), используемых для неформального или полу формального описания шансов реализации угрозы.
2.6. Тип источника по расположению относительно ИТ-системы #
где # - цифра (цифровая символьная переменная α_{26}), определяющая тип источника по расположению относительно ИТ-системы:
1 – внешний;
2 – внутренний.

3. Методы нападения (методы реализации угрозы)
   3.1. Потенциальные уязвимости активов *
   где * - произвольное количество символов (переменная μ_{31}), используемых для неформального описания потенциальных уязвимостей активов.
   3.2. Каналы проникновения в ИТ-систему *
   где * - произвольное количество символов (переменная μ_{32}), используемых для неформального описания каналов проникновения в ИТ-систему.
   3.3. Способы маскировки нападения (реализации угрозы) *
   где * - произвольное количество символов (переменная μ_{33}), используемых для неформального описания способов маскировки нападения.
   3.4. Способы инициализации нападения (реализации угрозы) *
   где * - произвольное количество символов (переменная μ_{34}), используемых для неформального описания способов инициализации нападения.
4. Нежелательные события
   4.1. Описание нежелательного события, от которого должны быть защищены активы *
   где * - произвольное количество символов (переменная) произвольное число элементов блок-схемы, используемых для неформального описания события, от которого должны быть защищены активы.
5. Активы, требующие защиты
   5.1. Вид актива #
   где # - цифра (цифровая символьная переменная α_{51}), определяющая тип актива:
   1 – сведения;
   2 – носители сведений.
   5.2. Владельцы актива <#, ****>
   где # - цифра (цифровая символьная переменная α_{52}), определяющая тип владельца актива:
   1 – является владельцем или ответственным лицом ИТ-системы;
   2 – является обслуживающим персоналом ИТ-системы;
   3 – не является владельцем, обслуживающим персоналом или ответственным лицом ИТ-системы;
   * - произвольное количество символов (переменная μ_{52}), описывающее владельца актива.
   5.3. Первичные активы ****
   * - произвольное количество символов (переменная μ_{53}), описывающее первичные активы, которые могут быть скомпрометированы при компрометации идентифицируемого актива.
   5.4. Тип актива #
   где # - цифра (цифровая символьная переменная α_{54}), определяющая тип актива по отношению к ОО:
   1 – внешние и расположенные вне пределов ИТ-среды ИТ-системы;
   2 – внешние, но расположенные в пределах ИТ-среды ИТ-системы;
   3 – внутренние.
   5.5. Степень секретности актива #
   (используется, если вид актива - 1)
   где # - цифра (цифровая символьная переменная α_{55}), определяющая степень секретности актива.
   5.6. Конфиденциальность актива #
   (используется, если вид актива - 1)
   где # - цифра (цифровая символьная переменная α_{56}), определяющая конфиденциальность актива.
   5.7. Гриф секретности актива #
   (используется, если вид актива - 2)
   где # - цифра (цифровая символьная переменная α_{57}), определяющая гриф секретности актива.
   5.8. Уровень важности актива для функционирования организации #

где # - цифра (цифровая символьная переменная α_{58}), определяющая уровень важности актива для функционирования организации.

5.9. Дополнительные сведения об активе *

* - произвольное количество символов (переменная μ_{59}), определяющее дополнительные сведения об активе.

6. Описание угрозы

6.1. Описание угрозы *

* - произвольное количество символов (переменная μ_{61}), определяющее неформальное описание угрозы.

7. Ответственность за противостояние угрозе

7.1. Тип источника противостояния угрозе #

где # - цифра (цифровая символьная переменная α_{71}), определяющая тип источника противостояния угрозе:

1 – ИТ-система;

2 – ИТ-среда ИТ-системы;

3 – Не-ИТ-среда ИТ-системы;

7.2. Описание источника противостояния угрозе *

* - произвольное число символов (переменная μ_{72}), определяющее неформальное описание источника противостояния угрозе.

8. Анализ рисков

8.1. Вероятность компрометации активов $p_c(y, z)$, где переменная $x \in [0,1]$, y – идентифицированный метод нападения, z – идентифицированный актив.

8.2. Последствия любого ущерба, который может быть причинен вследствие компрометации активов *

* - произвольное число символов (переменная μ_{82}), используемых для неформального описания последствий.

9. Направленность угрозы

9.1. Компрометация активов ###

где ### - цифровая символьная переменная β_{91}, определяющая направленность угрозы.

10. Описание ИТ-системы *

* - произвольное число символов (переменная μ_{100}), используемых для описание ИТ-системы.

11. Описание ИТ-среды ИТ-системы *

* - произвольное число символов (μ_{110}), используемых для описание ИТ-среды ИТ-системы.

12. Описание Не-ИТ-среды ИТ-системы *

* - произвольное число символов (переменная μ_{120}), используемых для описание Не-ИТ-среды ИТ-системы.

13. Прикладные замечания *

* - произвольное число символов (переменная μ_{130}), используемых для прикладных замечаний, относительно использования модели угрозы.

▲

Таким образом, структура представления угрозы должна включать следующие аспекты: маркировку и идентификацию угрозы; идентификацию источника угрозы; идентификацию объекта защиты; идентификацию активов (информации или ресурсов), подверженных возможности компрометации; описание угрозы; идентификацию методов реализации угрозы; описание результатов анализа рисков; описание этапов жизненного цикла угрозы (зарождения, развития, реализации и регенерации).

Литература

1. Evaluation Criteria for IT Security. ISO/IEC 15408-1: 1999.

2. ГОСТ 51275-99 «Факторы, воздействующие на информацию».

REPRESENTATION STRUCTURE OF SECURITY THREAT MODEL AT FORMATION OF INFORMATION TECHNOLOGY PROTECTION PROFILES

Sidak A.

Central research institute of DoD of Russian Federation
34 Tikhonravov street, Moscow area, Yubileyniy, 141080

Now perspective direction is the formation of the information technology (IT) security requirements as protection profiles, which structure is regulated in the international standard ISO/IEC 15408-99 "Evaluation criteria for information technology security" (historically usual name - Common criteria) /1/.

Protection Profile (PP) defines an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs. Such TOEs are intended for satisfaction of needs of many consumers. The consumers can form or use available PP to formulate the IT security requirements for any certain TOE.

For the effective decision of information security problem at IT PPs formation revealing all threats to actives of the given IT systems is necessary.

Under threat of IT (factor influencing the information) the phenomenon, action or process is understood, which result can be outflow, distortion, destruction of the protected information, blocking of access to it /2/.

Revealing and analysis of security threats play the important role at formation of security objectives and security requirements.

Result of revealing of security threat to safety is the model of threat.

The model of threat is formal, semiformal or informal description of threat life cycle; orientations of threat; a source of threat; IT systems, subject threat; IT- and non-IT-environment of IT systems; actives requiring protection; methods, ways and algorithms of attack (realization of threat); undesirable events; the risk analysis and some other aspects.

As a result of the analysis of Common Criteria the requirements on threats the following representation structure of security threat model was developed.

▼

1. Marks

Key symbol T (from English “Threat”)

1.1. Code of threat T.XXX_YYY.ZZ,

Where XXX - the code of threat class;

YYY - the code of threat family;

ZZ - number of threat in family.

1.2. Name of threat

2. Source of threat

2.1. Type of a source

1 - is connected to ill-intentioned actions of the man;

2 - is connected to other actions of the man;

3 - is not connected to actions of the man.

2.2. The type of a source on its interest in compromise of actives

2.3. A type of a source on the authorized access to IT system, in which the actives are stored, processed and transferred

2.4. Type of a source on a level of practical skills of threat realization

2.5. The type of a source on presence of chances of threat realization

2.6. Type of a source on an arrangement concerning IT system

3. Methods of an attack (methods of threat realization)

3.1. Potential vulnerability of actives

3.2. Channels of penetration in IT system

3.3. Ways of masking of an attack (realization of threat)

3.4. Ways of initialization of an attack (realization of threat)

4. Undesirable events

4.1. The description of undesirable event, from which the actives should be protected

5. Actives requiring protection

5.1. Kind of an active

1 - item of information;

2 - carriers of the items of information.

5.2. Owners of an active

5.3. Primary actives

5.4. Type of an active

1 - external and located outside of limits of IT environments of IT system;

2 - external, but located within the limits of IT environments of IT system;

3 - internal.

5.5. Degree of privacy of an active
5.6. Confidentiality of an active
5.7. Signature stamp of privacy of an active
5.8. Level of importance of an active for organization functioning
5.9. Additional items of information on an active

6. Description of threat
7. Responsibility for an opposition to threat
   7.1. Type of a source of an opposition to threat
      1 – IT system;
      2 – IT environment of IT system;
      3 - Non-IT-environment of IT system;
   7.2. Description of a source of an opposition to threat
8. The risk analysis
9. Orientation of threat
10. The description of IT system
11. The description of IT environment of IT system
12. The description of Non – IT- environment of IT system
13. The applied remarks

▲

Thus, the representation structure of threat should include the following aspects: marks and identification of threat; identification of a source of threats; identification of object of protection; identification of actives (information or resources), subject opportunity compromise; the description of threat; identification of threat realization methods; the description of risk analysis results; the description of threat life cycle stages (origin, development, realization and regeneration).

The literature

1. Evaluation Criteria for IT Security. ISO/IEC 15408-1: 1999.
2. GOST 51275-99 "The Factors influencing the information".